Teemu Korhonen

SWOT-VIITEKEHYS KYBERTURVALLISUUDEN STRATEGISEN TILANNEKUVAN MUODOSTAMISESSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Korhonen, Teemu
SWOT-viitekehys kyberturvallisuuden strategisen tilannekuvan muodostamisessa
Jyväskylä: Jyväskylän yliopisto, 2024, 50 s.
Kyberturvallisuus, pro gradu - tutkielma
Ohjaaja(t): Frantti, Tapio

Tässä tutkimuksessa tarkastellaan kyberturvallisuuden strategisen tilannekuvan muodostamista SWOT-viitekehyksen pohjalta. Tutkielmassa on tarkoituksena selvittää SWOT:n soveltuvuutta osana kyberturvallisuuden strategisen tilannekuvan muodostamista organisaatiokontekstissa. Kyberturvallisuuden strategista tilannekuvaa ei ole juurikaan tutkittu ja kyberturvallisuuden huomioiminen strategisesti on vielä vähäistä, vaikkakin kiinnostus ottaa se huomioon on kasvussa, joten tutkimuksen aihe on tärkeä.

Tutkimuksen teoreettinen tausta koostuu SWOT-analyysin, tilannekuvan ja -ymmärryksen, kybertoimintaympäristön erikoispiirteiden kuten raportoinnin, kyberuhkien ja strategisen tilannekuvan muodostamisen tarkastelusta ja määrittelystä. Tutkimuksen teoriaosuudessa taustoitetaan varsinaista tutkimusta, annetaan lukijalle riittävät perustiedot tutkimusaiheesta sekä avataan tutkimuksessa käytettävää termistöä. Tutkimusmenetelmänä tässä tutkimuksessa on hyödynnetty design science researchia eli suunnittelututkimusta. Aineistona on käytetty julkisesti saatavissa olevien kyber- ja tietoturvaan erikoistuneiden yritysten tuottamia uhkatieto- ja kyberturvallisuusraportteja.

Raporttien sisältö analysoitiin SWOT:lla ja tehtyjen havaintojen pohjalta koostettiin organisaatiotason kyberturvallisuuden strateginen tilannekuva. Analyysi ja muodostetun tilannekuvan tulokset todistivat, että SWOT-viitekehystä voi käyttää osana strategisen tilannekuvan muodostamista, mutta se ei sellaisenaan ole optimaalisin viitekehys näin spesifin aiheen analysointiin. Havaintojen teemoittelu esim. mahdollisuuksien osalta oli hankalaa tämän viitekehyksen pohjalta.

Johtopäätöksenä syntyi muokattu SWCT-viitekehys, jossa mahdollisuudet on korvattu vastatoimilla (countermeasures) ja uhat tarkennettu koskemaan kyberuhkia. SWCT-viitekehyksen lisäksi syntyi organisaatioille yleiseen hyötykäyttöön tarkoitettu strategisen tilannekuvan mallipohja. Näillä kehitysehdotuksilla voidaan paremmin vastata tarkasteltavan tilanteen havaitsemiseen, ymmärtämiseen ja vaikutuksien arviointiin organisaation tulevaisuuteen nähden.

Asiasanat: Strateginen tilannekuva, SWOT, strateginen kybertilannekuva, SWCT, kyberuhat, tilannekuva, tilanneymmärrys, kyberturvallisuus

ABSTRACT

Korhonen, Teemu
SWOT framework in formation of strategic cybersecurity situation picture
Jyväskylä: University of Jyväskylä, 2024, 50 pp.
Cybersecurity, Master's Thesis
Supervisor(s): Frantti, Tapio

This study examines the creating of strategic situation picture of cybersecurity based on a SWOT framework. The purpose of the study is to explore the applicability of SWOT as part of the strategic situation picture process in an organizational context. The strategic situation picture of cybersecurity has not been studied much and the strategic consideration of cybersecurity is still limited, although there is a growing interest in taking it into account, so the research topic is important.

The theoretical background of the study consists of a literature review and definition of SWOT analysis, situational awareness and understanding, special characteristics of the cyber environment such as reporting, cyber threats and strategic situation picture. The theoretical part of the study provides a background to the research itself, gives the reader sufficient basic information on the research topic and opens the terminology used in the study. The research method used in this study is Design Science Research. The data used in empirical part are from publicly available cyber security reports produced by cyber and information security companies, which contain threat intelligence information on the cyber environment.

The content of the reports was analyzed using SWOT and the findings were used to create a strategic situation picture of cybersecurity on organizational level. The results of the analysis and the generated situation picture proved that the SWOT framework can be used as part of the strategic situation picture, but as such it is not the most optimal framework for analyzing such a specific topic. It was difficult to thematize the findings, e.g. in terms of opportunities, in the framework.

In conclusion, a modified SWOT, named by SWCT, framework was developed, replacing opportunities with countermeasures, and specifying threats as cyber threats. In addition to the SWCT framework, a strategic situation picture template was developed for the general use of organizations'. These developments will better address the need to detect, understand and assess the implications of the situation under consideration for the future of the organization.

Keywords: Strategic situation picture, strategic situational awareness, SWOT, situational awareness. situation picture, cyber security, cyber threats, SWCT

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Viimeisen kolmen vuoden ajanjaksolle on ajoittunut useita maailmaa muuttaneita tapahtumia kuten koronapandemia, Ukrainan sota ja inflaatio. Nämä ovat tehneet lähtemättömän jäljen ihmisten elämään ja muuttaneet toimintatapojamme. Ennen kaikkea koronapandemia aiheutti lähtemättömän muutoksen erityisesti työskentelytapoihimme siirtäen niitä kohti etätyötä ja verkonvälityksellä tapahtuvaa toimintaa. Ukrainan sota vuorostaan on lisännyt valtioiden välistä informaatiovaikuttamista, joten kyberturvallisuus on etenevissä määrin noussut jokaisen huulille. Microsoft (2023) esimerkiksi raportoi omassa Ukrainaan liittyvässä raportissaan, että sodan alettua Venäjän valtion sponsoroimat hakkerit olivat kohdistaneet haittatoimiaan 74 eri maahan. Näiden kybervakoiluoperaatioiden kohteena olivat olleet Keski- ja Itä-Euroopan sekä Amerikan hallitusten ja puolustukseen liittyvät organisaatiot, kuten myös yksityiset IT-organisaatiot.

Nämä tapahtumat ovat avanneet ovia uusille uhille ja muuttanut toimintaympäristöämme erityisesti kybertoimintaympäristöämme. Kybertoimintaympäristö on ihmisten luomaa digitaalista rinnakkaistodellisuutta, joka maailmanlaajuisesti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta ihmisiä ja laitteita jopa valtiorajojen yli toisiinsa (Ulkoministeriö, 2023). Tämä verkottunut yhteiskuntamme tuo lähemmäksi ja yhdistää niin ihmisiä kuin ennen irrallaan toimineita ympäristöjä. Samalla kun tapamme olla yhteydessä niin ympäristön kuin laitteiden kautta, ovat myös uhat kuten informaatiovaikuttaminen lisääntynyt. Informaatiovaikuttamisen tapojen lisääntyessä jatkuvasti on tarpeellista lisätä varautumista kyberuhkiin ja -häiriötilanteisiin, jotka vaarantavat yhteiskunnalle välttämättömien tietoteknisten järjestelmien ja rakenteiden toimivuutta jo normaalioloissa. Ymmärrys ja tilannekuvan saaminen kyberkenttää moukaroivista kyberuhista on hyödyllistä kenelle tahansa tietotekniikan ja ennen kaikkea tietoturvan parissa työskentelevälle. Lehto (2021) korostaa informaatioteknologiassa kehityssyklien olevan usein hyvin lyhyitä ja sama trendin usein koskevan eri kyberhyökkäysmuotoja ja haittaohjelmia. Ajan tasalla pysyminen ja oman tilannetietoisuuden ylläpitäminen kybertoimintaympäristöstään ja sen uhkiin liittyen korostuu nykypäivänä.

Muuttuvassa toimintaympäristössä tilannetietoisuuden ylläpitäminen ja tulevan ennakointi korostuvat, joten monet kyberturvallisuusalan yritykset ja valtiolliset toimijat julkaisevatkin omia kyberturvallisuuskoosteita ja -raportteja. Nämä yksityisten kuin myös kansallisten organisaatioiden tuottamat tilannekuvat sekä raportit pyrkivät pitämään kyberturvasta vastaavat henkilöt ja muut asiasta kiinnostuneet tahot ajan tasalla nykyisistä ja tulevista suuntauksista. Suomessa yksityisen ja julkisen sektorin välistä tiivistä yhteistyötä kyberturvallisuuden saralla on jo tehty pitkään. Kansallisella tasolla Liikenne- ja viestintävirasto Traficomin alaisuudessa toimivalla Kyberturvallisuuskeskuksella on merkittävä rooli Suomen kyberturvallisuuden poikkeamahallinnassa sekä tilannekuvan muodostamisessa ja analysoinnissa. Kyberturvallisuuskeskus tuottaa erilaisia tilannekuvatuotteita, jakaa informaatiota ja toimii yhteyspisteenä tietoturvapoikkeamien ja -uhkien hallinnassa tarjoten apua myös näiden tutkimiseen eri tahoille (Kyberturvallisuuskeskus, 2023).

Strategisen toiminnan ja strategian muovaamisessa kyberturvallisuusraporttien merkitystä on vaikeata olla korostamatta liikaa. Hyvä tilannekuva ja -ymmärrys antavat paremmat valmiudet strategiseen johtamiseen ja strategian jalkauttamisessa organisaation toimintaan. Hyvää strategista johtamista vuorostaan tarvitaan kyberturvallisuuden yhteensovittamiseen ja koordinoimiseen, sekä yhteistoimintarakenteiden varmistamiseen erilaisten toimijoiden välillä (Lehto & Limnéll, 2021). Yrityspuolella tehdyt havainnot kuitenkin paljastavat, etteivät nykyiset strategiat vielä riittävästi edesauta digiturvallisuuden toteuttamista. Syyt tähän ovat, että kyberturvallisuutta käsitellään teknologisena haasteena ja hallinnollisena työnä ja useimmat digi- ja kyberturvallisuusjohtajat eivät osallistu yrityksen strategiseen päätöksentekoon (Huoltovarmuuskeskus, 2022). Kyberturvallisuuden implementoimisessa strategiseen tekemiseen ja johtamiseen on siis vielä paljon tehtävää.

Positiivisia merkkejä asian suhteen antaa kuitenkin Huoltovarmuuskeskus (Huoltovarmuuskeskus, 2023) julkaisemassaan selvityksessä toimialojen kyberkypsyydestä. Siinä huomattiin selkeä muutos edelliseen tutkimuskertaan erityisesti uhka- ja riskikentässä, jossa tapahtuneet muutokset ovat tuoneet kyberturvallisuuden myös niiden johtoryhmien agendalle, jotka eivät aikaisemmin käsitelleet kyberturvallisuutta ja sen tilannekuvaa säännöllisesti. Tämä on merkittävä muutos aikaisempaan ja tuskin ainakaan vähentää tilannekuvan tuottamisen tarvetta tulevaisuudessa. Tilannekuvan potentiaali päätöksenteon tukena aletaan siis pikkuhiljaa paremmin ymmärtämään. Tilannetietoisuudella ja markkina-arvon välillä on myös havaittu olevan yhteys. Berkman ym. (2018) tutkivat kyberturvallisuustietoisuutta koskevassa tutkimuksessaan tilannetietoisuuden ja markkina-arvon yhteyttä. Heidän empiiriset tuloksensa osoittavat, että kyberturvallisuustietoisuuden ja markkina-arvon välillä on positiivinen yhteys. Tämä korostaa tilannetietoisuuden hyötyä myös bisnesnäkökulmasta ja tilannekuvan paremmasta huomioinnista osana strategiaa.

Tämän pro gradun tarkoituksena on analysoida yksityisten tietoturva yritysten tuottamia uhkatieto- ja kyberturvallisuusraportteja SWOT-analyysia hyödyntäen. SWOT-viitekehys on analyysikehikko, jossa (Strengths, Weaknesses,

Opportunities, Threats - vahvuudet, heikkoudet, mahdollisuudet, uhat) yksilöidään analysoitavan kohteen hyvät ja huonot puolet, jotka liittyvät sen olemassaolon sisäisiin ja ulkoisiin olosuhteisiin (Vanek ym., 2014). Tarkoituksena on rakentaa SWOT-analyysin pohjalta viitekehys strategisen tilannekuvan arviointiin ja tuottamiseen. Tutkimuskysymys, johon pyritään tässä tutkielmassa vastaamaan SWOT-analyysin pohjalta, on seuraavanlainen:

> Voiko SWOT-analyysista rakentaa viitekehyksen strategisen tilannekuvan tuottamiseksi?

Lähdekirjallisuus teoriasuuteen on kerätty pääasiassa Google Scholarista, Jykdokista ja Web of Sciencen tietokannasta. Akateemista lähdekirjallisuutta ja aiempaa tutkimusta on näistä haettu erilaisilla hakusanoilla kuten "SWOT" AND "situation awareness", "SWOT" AND "situation picture", SWOT kyberturvallisuudessa, SWOT strategisessa tilannekuvassa, strateginen tilannekuva, SWOT, ja kyberuhat. Analysoitavat materiaalit itse tutkimusosuuteen on haettu kyberturvallisuus organisaatioiden omilta sivuilta vapaasti käytössä olevien materiaalien muodossa. Lähdekirjallisuuden ja analysoitavan aineiston osalta on valittu materiaaliksi vain tekstiä, lukuja ja erilaisia visuaalisia kuvaajia sisältäviä materiaaleja. Erilaisista poikkeamanhallintajärjestelmistä tai muista vastaavista valvontamenetelmistä saatavat kvantitatiiviset luvut ja massadata eivät kuulu tämän tutkimuksen piiriin, vaan ne ovat enemmänkin operatiiviseen tilannekuvaan hyödynnettävää dataa.

Tutkimuksen aihealue on hyvin moniulotteinen, joten kaikkia mahdollisia näkökulmia ei ole mahdollista ottaa huomioon. Tässä tutkimuksessa keskitytään käsittelemään kyberturvallisuuden tilannetietoisuuden ja tilannekuvan rakentamista strategisesta näkökulmasta. Koska kyse on strategisesta näkökulmasta ja tarkoituksena on hyödyntää SWOT-analyysia viitekehyksenä tilannekuvan tuottamiseen, jätämme tutkimuksen ulkopuolelle kybertilannekuvatoimintaan liitetyt tekniset toimenpiteet ja lähteet, kuten kybervalvonnan ja poikkeamienhallinnan. Tutkimuksen tavoitteena ei myöskään ole arvioida aihepiiriin liittyviä teknisiä menetelmiä ja ratkaisuja, joiden avulla tietoa esimerkiksi jaetaan eri toimijoiden välillä, tai toteuttaa niiden välistä vertailua.

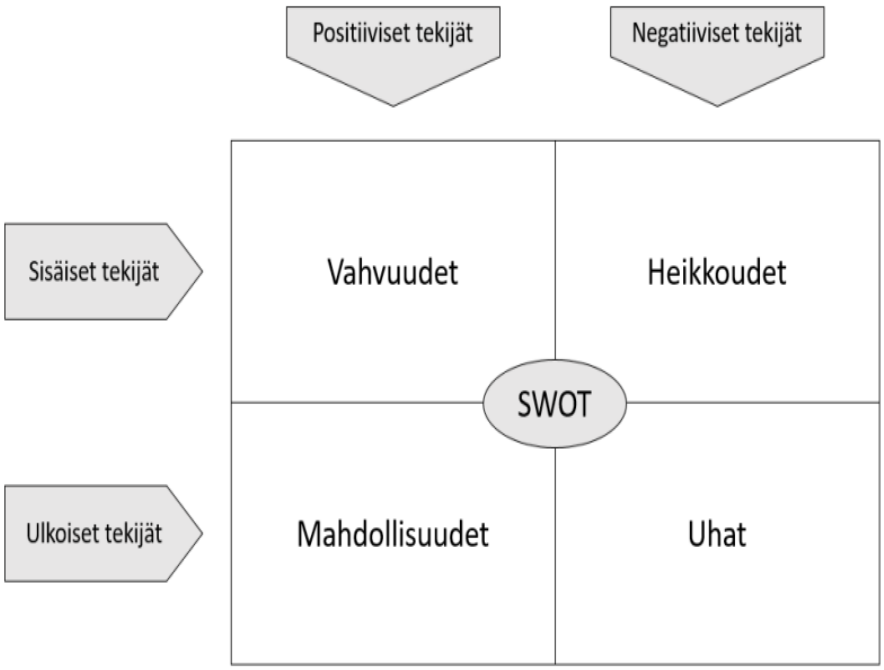
2 TEOREETTINEN KEHYS

Tässä kappaleessa on tarkoituksena avata SWOT – analyysia, kertoa mihin sitä käytetään, mitä hyötyjä ja mahdollisia heikkouksia siihen myös liittyy. Tämän jälkeen määritellään tilannekuva sekä muuta siihen olennaisesti liittyvää termistöä ennen kuin seuraavassa kappaleessa mennään kyberturvallisuus spesifeihin asioihin.

2.1 SWOT

SWOT-analyysi on Albert Humphreyn kehittämä viitekehys ja strategiatyökaluväline organisaation toimintakyvyn ja sen toimintaympäristön kokonaisuuden analysointiin. SWOT-analyysia käytetään yleisesti yrityksen strategian laatimisessa, ongelmien sekä oppimisen tunnistamisessa, ja toimintaprosessien kehittämisessä (Nyarku & Agyapong, 2011). Hyödyntämisen laajuus voi vaihdella ja analyysin kohteina voi olla esim. organisaatio koko laajuudessaan, yksittäisen tuotteen tai palvelun asema tai vaikka kilpailijoiden toiminta. SWOT-lyhenne tulee englanninkielisistä sanoista Strengths (vahvuudet), Weaknesses (heikkoudet), Opportunities (mahdollisuudet) ja Threats (uhat) (Nyarku & Agyapong, 2011).

SWOT on niin sanottu nelikenttämalli, jossa analysoitavat tekijät jaetaan neljään eri osa-alueeseen. Vahvuudet ja heikkoudet ovat sisäisiä tekijöitä, kun taas mahdollisuudet ja uhat ovat ulkoisia tekijöitä. Näiden lisäksi mallissa jaotellaan vielä osa-alueet erikseen positiivisiin ja negatiivisiin tekijöihin. Tätä nelikenttä jaottelua pyritään sitten hyödyntämään analysoitaessa esim. organisaation toimintaympäristön kokonaisuutta. Kuvio 1 demonstroi tätä nelikenttä jaottelua.



KUVIO 1 SWOT-viitekehys (Nyarku & Agyapong, 2011)

SWOT:n analysointiprosessin tavoitteena on tunnistaa sisäiset ja ulkoiset tekijät, jotka vaikuttavat organisaation liiketoiminnan suorituskykyyn.

- SWOT-analyysissä vahvuudet voidaan ajatella sisäisinä kyvykkyyksinä ja myönteisinä tekijöinä strategisen tavoitteen saavuttamiseen ja tehokkuuteen.
- Heikkoudet vuorostaan ovat sisäisiä tekijöitä tai rajoitteita, jotka saattavat estää tai haitata organisaation suorituskykyä ja toimintaa.
- Mahdollisuudet ovat positiivisia ulkoisia tekijöitä tai piirteitä, jotka voivat suosia tai helpottaa organisaation etujen hyödyntämistä organisaation ulkopuolelle ja yhteyksien luomista toimintaympäristöönsä.
- Uhkat käsittelevät yrityksen ulkopuolisia negatiivisia tekijöitä, jotka voivat estää tai viivästyttää saavutettavissa olevia tavoitteita tai pahimmillaan olla tuhoisia organisaation jatkuvuuden kannalta. (Namugenyi ym., 2019.)

SWOT-analyysi on laajalti hyödynnetty strategiatyökalu edellä mainittuihin sekä monien muiden tilanteiden analysointiin. Liiketoiminnan avainkohtien esiin nostaminen ja sovellettavuus yhdessä muiden strategiatyökalujen kanssa on syytä nostaa esiin SWOT:n vahvuuksista puhuttaessa. SWOT-analyysi onkin näistä syistä vakiintunut strategiatyön viitekehykseksi useille eri aloille (Vanek ym., 2014). Strategiatyökaluna sen vahvuudet piilevätkin strategisten

toimintojen parantamisessa. Vakiintuneesta statuksestaan huolimatta SWOT-analyysia on myös kritisoitu sen yksinkertaisuudesta johtuvan syvällisyyden puutteesta ja naiiviudesta analyysin tuloksissa. Esimerkiksi Pickton ja Wright (1998) korostavat, että SWOT-analyysi olisi nähtävä ennen kaikkea helposti sovellettavana ja dynaamisena välineenä liiketoiminnan osa-alueiden kyvykkyyksien ja kehittämistarpeiden arvioinnissa eikä välttämättä koko totuutena.

Kyberturvallisuuden piirissä SWOT- analyysi on vielä vähissä määrin hyödynnetty tai sen hyödynnettävyyttä ei ole täysin testattu. Pelkonen ym. (2016) hyödynsivät SWOT-analyysia Suomen valtioneuvostolle tekemässään selvityksessä kyberosaamisen tilasta Suomessa ja tietokartasta tulevaisuuteen. He olivat onnistuneet tunnistamaan raportissaan kyberturvallisuuteen liittyviä tekijöitä SWOT-analyysin avustuksella. Shevchenko ym. (2021) selvittivät omassa tutkimuksessaan SWOT:n käyttöä osana tietoturvariskien tunnistamista ja näiden riskien arvioimista. He pystyivätkin tutkimuksen tuloksena tunnistamaan, että erityisesti pienille- ja keskisuurille yrityksille SWOT on selkein ja helppokäyttöisin analyysityökalu tietoturvariskien tunnistamiseen ja arviointiin. Nyarku ja Agyapong (2011) selvittivät tutkimuksessaan SWOT-analyysin hyödynnettävyyttä eri aloilla ja tulivat siihen tulokseen, että yksinkertaistamalla konstruktiot ja mallit saadaan yhdistettyä SWOT-käyttäjien ja analysoijien näkemyksiä, mikä edelleen helpottaa alojen sidosryhmien, yritysten ja monikansallisten organisaatioiden analysointia alasta riippumatta. Näin ollen SWOT:n integrointi useiden eri toimialojen ja integroitujen liiketoimintaympäristöjen yhteydessä onnistuu ainakin jossain määrin.

2.2 Tilannekuva ja -tietoisuus

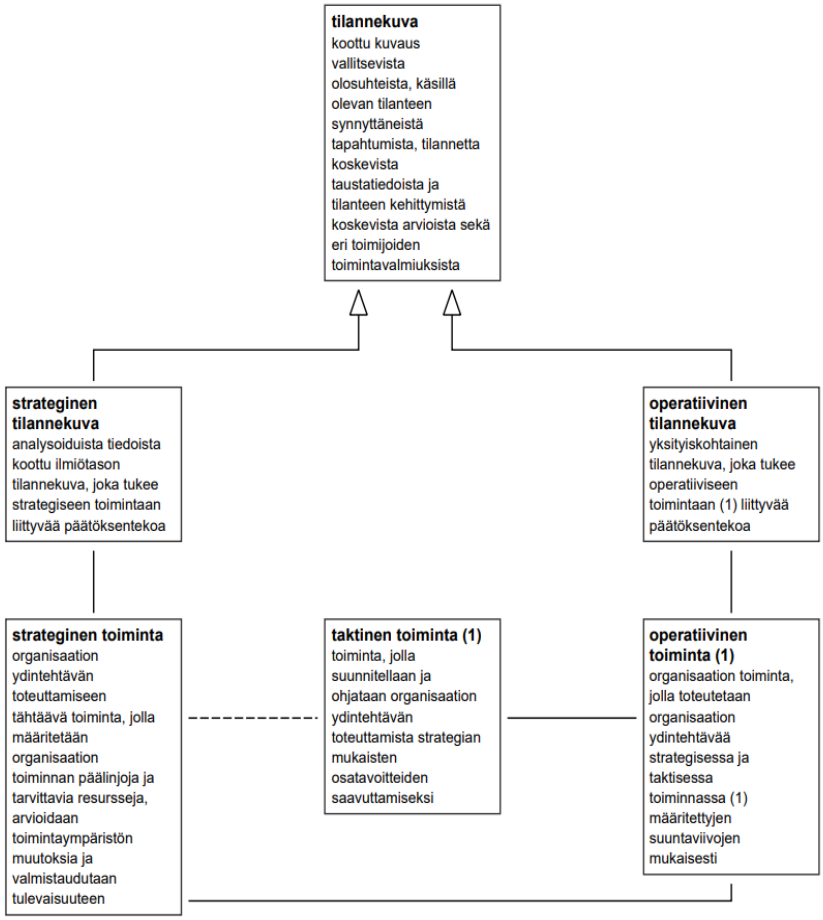
Tilannekuva (eng. situation picture) koostuu erilaisista havainnoista, arvioinneista sekö analyyseista, ja siinä voidaan käyttää myös apuna erilaisia mittareita. Sen pääsääntöinen käyttötarkoitus on toimia päätöksenteon tukena. Tilannekuvaa voisi siis kuvailla koosteeksi tai kuvaukseksi vallitsevasta tapahtumasta tai tilanteesta ja siitä saatavilla olevista taustatiedoista (Sanastokeskus, 2023). Tilannekuva ei ole pelkkää saatavilla olevan datan jakamista vaan se myös määrittelee sekä kertoo arvioita ja analyysia datan yhteyksistä ja merkityksestä sekä tilanteen kehityksestä (Horsmanheimo ym., 2017).

Periaatteet ja arvot ohjaavat organisaation tilannekuvan muodostamis- ja hyödyntämisprosessin systemaattista etenemistä. Lopullinen tilannekuvan hyödyntäminen tapahtuu vasta päätöksentekoprosessissa osana strategista johtamista. (Endsley, 1995.)

Tilannekuva voidaan määritellä käyttötarkoituksensa mukaan joko strategiseksi tai operatiiviseksi. Tämä sama jaottelu pätee myös tarkemmin kybertilannekuvasta puhuttaessa. Strateginen tilannekuva on määräajoin tuotettava yleiskatsaus tai -arvio, joka on tyypiltään kuvaileva katsaus, sisältäen analyyseja sekä mahdollisia toimenpide-ehdotuksia. Operatiivinen tilannekuva vuorostaan on

lyhyemmän aikavälin tilannekuva ja sen tavoite on hahmottaa tilannekehitystä, helpottaa päätöksenteko ja parantaa tilanteen hallintaa. (Lehto ym., 2017.)

Ajallisen hyödynnettävyyden näkökulmasta Tounsi ja Rais (2018) viittaavat yleisesti lyhyemmän ajan puitteissa tai lähes välittömästi hyödynnettävissä olevan tiedon tai tapahtuvien toimintojen olevan operatiivisella tasolla kuvaavaa, kun taas strategisella tasolla tiedon käyttöikä ja hyödynnettävyys on pidempi. Operatiivinen tilannekuva pohjautuu vahvemmin tekniseen tietoon ja dataan, jota on saatavilla esim. erilaisista SOC ja SIEM-järjestelmistä ja hyödynnettävissä kutakuinkin heti. Strateginen tilannekuva voi myös pohjautua samaiseen tietoon, mutta siinä hyödynnetään myös selkeästi hallinnollisempaa ja strategisempaa informaatiota tarkoituksena tarjota pidemmän ajankohdan tilannekuva. Päämääränä strategisella tilannekuvalla on tukea strategiseen toimintaan liittyvää päätöksentekoa. Saatavilla olevan tiedon ajallinen hyödynnettävyys vaihtelee toiminnan eri tasoilla. Toiminta ja toimintaympäristön luonne vaikuttaa koostettavassa tilannekuvassa käytettävään tietoon ja tarpeeseen vastata kohdattaviin ongelmiin. Kuviosta 2 voidaan havaita kuinka strateginen ja operatiivinen toiminta yhdessä taktisen toiminnan kanssa luovat pohjat niin operatiiviselle ja strategiselle tilannekuvalle yhdessä ja erikseen.



KUVIO 2 Tilannekuvan ja toiminnan tasojen limittyminen (Turvallisuuskomitea, 2018).

Horsmanheimo ym. (2017) omassa tutkimuksessaan koostivat kattavan listan erilaisista tilannekuvan vaatimuksista. Näiden vaatimusten pohjalta voidaan todeta tilannekuvalle olennaista olevan, että se on hallinnoitu hyvin ja sen pohjalta kyetään tekemään analyyseja ja ennen kaikkea päätöksiä. Erityisen tärkeää on myös, että tilannekuvaan koostetun tiedon tulisi olla vastaanottajille merkityksellistä, valmiiksi prosessoitua ja analysoitua, ja ymmärrettävässä muodossa. Tiedon visuaalinen esitysmuoto ja selkeys ovat myös Horsmanheimon ym. (2017) mukaan olennaisia elementtejä tilannekuvan onnistumisen kannalta, ja erityisesti strategisessa tilannekuvassa turhia teknisiä yksityiskohtia tulisi välttää. Kokonaiskuvan merkityksen korostaminen ja tulevaisuuden ennakointi onkin syytä ottaa huomioon strategisen tilannekuvan korostaminen.

Tilannekuva ei kuitenkaan itsessään ole vielä tae tilannetietoisuuden saavuttamiselle, sillä jokainen henkilö muodostaa sen itse. Tilannekuvan tuottamisella tarjotaan työkalut ja luodaan pohjat tilannetietoisuuden ja -ymmärryksen kehittymiselle. Tilannetietoisuus (engl. situation awareness) on henkilön päätöksentekoon tarvittavaa ymmärrystä tapahtuneista asioista ja olosuhteista, eri sidosryhmien tavoitteista ja mahdollisista tilanteen kehittymissuunnista (Endsley, 1995; Sanastokeskus, 2023). Tilanneymmärrys (engl. situational understanding) on kognitiivinen tulkinta vallitsevasta tilanteesta ja toimijan omasta tilannetietoisuudesta koskien kokonaisvaltaista toimintaympäristön tilannetta, johon vaikuttavat olennaisesti ihmisten yksilölliset taidot, kokemukset ja osaaminen (Kuusisto ym., 2015). Yksilölliset valmiudet yhdessä saatavilla olevan tiedon kanssa muodostavat siis tilanneymmärryksen.

Endsleyn (1995) kehittämän tilannetietoisuuden mallin ydin koostuu kolmesta peruselementistä, jotka voidaan kuvata tietoisuudentasoina. Tasot ovat havaitseminen (taso 1), tilanteen ymmärtäminen (taso 2) ja näiden vaikutuksen arviointi tulevaisuudessa (taso 3). Näiden peruselementtien kautta rakennettu tilannetietoisuus antaa perusteet johtopäätöksiin ja sitä kautta päätöksentekoon. Arvioitavan tilanteen tehtävä- sekä järjestelmäkohtaiset ominaisuudet kuin myös päätöksentekijän kyvykkyys, kokemukset ja arviointikyky vaikuttavat tilannetietoisuuden rakentumiseen Päätöksentekijöille oikeanlainen tilanneymmärrys on hyvin tärkeä, koska Madaharin ja Parishin (2016) mukaan kattava kuvaus vallitsevasta tilanteesta ja sen mahdollisesta kehityskulusta, tukee päätöksentekoa sekä antaa valmiuksia tilanteeseen liittyvien riskien ja niistä koituvien vaikutusten hallintaa. Päätöksenteko puolestaan ohjaa toimintaa, joka heijastuu takaisin havainnoitavaan toimintaympäristöön. Tilannekuvan muodostamisessa ja hyödyntämisessä Endsleyn (1995) luomaa tilannetietoisuuden mallin yleistä rakennetta onkin mahdollista soveltaa näiden tietojen pohjalta useiden eri tasojen tilannekuvien toteuttamisessa.

3 KYBERTURVALLISUUSYMPÄRISTÖN KUVAUS

Tässä luvussa käsitellään kybertoimintaympäristön tunnuspiirteitä, ominaisuuksia sekä siellä vallitsevia uhkia, jotka heijastuvat organisaatioiden kybertilannekuvan tuottamiseen. Luodaan kokonaisvaltainen käsitys uhkien ja toimintaympäristön merkityksestä organisaatioiden tilannekuvan tuottamisessa. Tämän lisäksi pohjustetaan tulevaa tutkimusosuutta ja esitellä olennainen termistöä kybertilannekuvan muodostamisen kontekstissa. Ensimmäisenä käydään läpi hieman yksityisten ja julkisten kyberturvallisuusorganisaatioiden roolia ja heidän tilannekuvatuotteitaan. Tämän jälkeen esitellään toimintaympäristön uhkatekijöitä eli kyberuhkia sekä määritellään kybertoimintaympäristö. Näiden jälkeen siirrytään strategisen tilannekuvan muodostamisen määrittelyyn.

3.1 Kyberturvallisuuden raportointi

Kyberturvallisuuden raportointi voi tapahtua monissa eri muodoissa riippuen raportoitavista tiedoista ja tietolähteistä. Sillä on myös merkitystä, kenelle raportoidaan. Kyberturvallisuusraportit ovat julkaisuja, jotka tarjoavat tietoa ja analyysiä ajankohtaisista kyberturvallisuuteen liittyvistä tapahtumista, uhkista, haavoittuvuuksista ja suosituksista. Esimerkiksi uhkatietoraportti (eng. Threat Intelligence Report) on yksi tyypillisimmistä kyberturvallisuuteen liittyvistä raporteista. Se on asiakirja, jossa yleensä kuvataan TTP:t eli tekniikat taktiikat ja proseduurit joilla voidaan järjestelmiä uhata, toimijat, kohteena olevat järjestelmä- ja tietotyypit sekä muut uhkiin liittyvät tiedot (Johnson ym., 2016). Näitä raportteja tuottavat yleensä kyberturvallisuusalan asiantuntijat, kuten kyberturvallisuusyritykset, tutkimuslaitokset ja viranomaiset.

Yksityiset ja kansalliset toimijat ovat jo hyvän tovin julkaisseet omia raportteja ja katsauksia kyberturvallisuuden tilaan liittyen. Esimerkiksi Cisco on viime vuosikymmenen aikana julkaissut runsaasti tietoturva- ja uhkatietoraportteja tietoturva-alan ammattilaisille, jotka ovat kiinnostuneita maailmanlaajuisesta

kyberturvallisuuden tilasta. Nämä kattavat raportit ovat tarjonneet yksityiskohtaisia kuvauksia uhkamaisemista ja niiden vaikutuksista organisaatioihin sekä parhaita käytäntöjä tietomurtojen haittavaikutusten torjumiseksi.

Kansallisista ja julkisista toimijoista Liikenne- ja viestintävirasto Traficomin alaisuudessa toimiva Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Näiden lisäksi sen palveluihin kuuluu kansallisen kyberturvallisuuden tilannekuvan ylläpitäminen ja kehittäminen, esimerkiksi kuukausittain julkaistavan Kybersää – tilannekuvatuotteen avulla. (Kyberturvallisuuskeskus, 2023.)

Kybersään tilannekuvan tuottamisessa on yhteyksiä ja samankaltaisuutta muihin julkisten kuin myös yksityisten organisaatioiden tuottamiin tilannekuvatuotteisiin. Luxemburgin hallituksen alaisuudessa toimiva tietoturvaloukkausten torjuntaryhmä (CSIRT) toimittaa samankaltaisen Kybersää – tilannekuvaraportin. CSIRT:n julkaisema Cyber Weather tarjoaa neljännesvuosittain tietoa kyberturvallisuutta koskevasta tilannetietoisuudesta kooten viimeaikaiset kyberturvallisuuden suuntaukset ja tapahtumat yleisölle, organisaatioiden johtajille ja teknisille asiantuntijoille (CSIRT, 2023). ENISA puolestaan on Euroopan unionin kyberturvallisuusvirasto, jonka tehtävänä on saavuttaa korkea yhteinen kyberturvallisuuden taso kaikkialla Euroopassa (ENISA, 2023). Heidän tuotteensa ENISA UHKAKUVA (ENISA – THREAT LANDSCAPE) julkaistaan vuosittain ja se pyrkii Kybersään tavoin koostamaan kybertoimintaympäristön muutoksia yhteen ja tarjoamaan tulevaisuuden näkymiä alalle.

Yksityiseltä puolelta Rapid7 ja PaloAlto Networks ovat tunnettuja pitkään tietotekniikan alalla toiminnassa olleita yrityksiä, ne julkaisevat tasaisin väliajoin tilannekuvatuotteita tietoturva-asiantuntijoille ja muille asiasta kiinnostuneille. Rapid7 esimerkiksi vuosittaisessa uhkatietoraportissaan analysoi 50:tä vuoden merkittävintä haavoittuvuutta ja hyökkäystä korostaakseen hyväksikäyttösuuntauksia ja auttaakseen tietoturva-alan ammattilaisia priorisoinnissa (Rapid7, 2022).

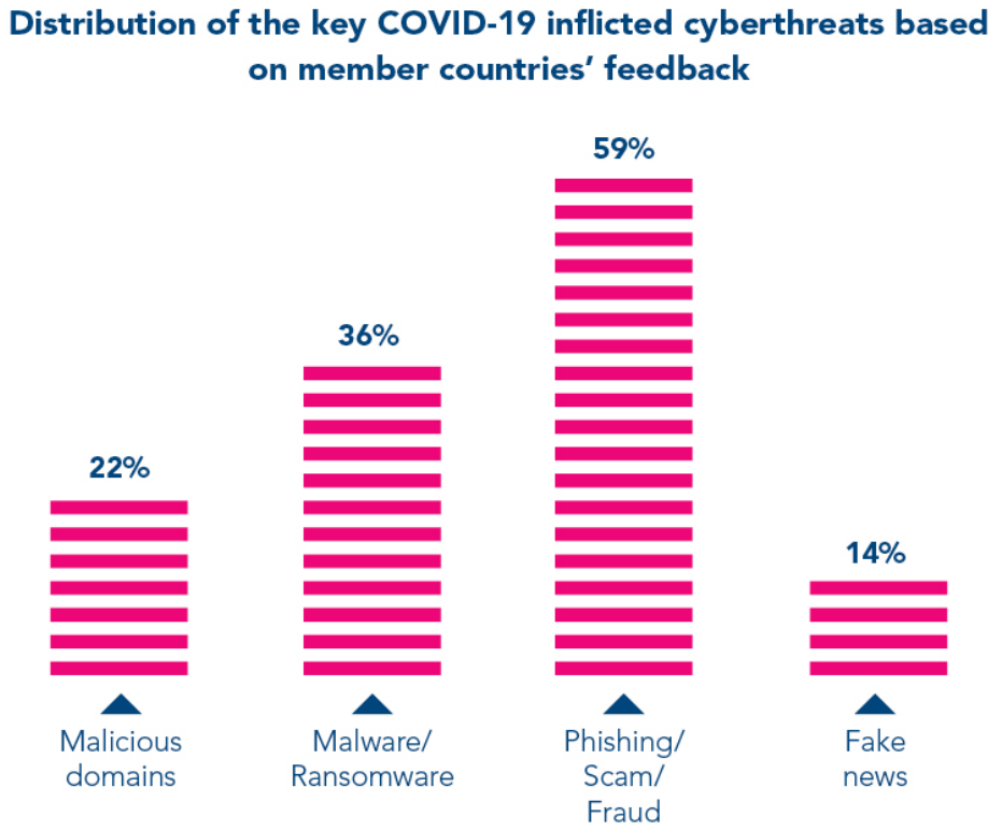
3.2 Kyberuhat

Kyberuhka (eng. cyber threat) on mahdollisesti toteutuva haitallinen kehityskulku tai tapahtuma, joka kohdistuu nimenomaan kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon (Turvallisuuskomitea, 2018). Lehdon (2017) mukaan kyberturvallisuuden kontekstissa uhat yhdessä muiden tekijöiden, kuten haavoittuvuuksien ja riskien kanssa muodostavat toisiinsa liittyvän kokonaisuuden. Lähtökohtaisesti tässä kokonaisuudessa on jokin resurssi kuten sensitiivinen data tai osaaminen, jota halutaan suojella ja turvata sen olemassaolo kaikin keinoin. Kyberuhka on siten sidoksissa näihin resursseihin, riskeihin, haavoittuvuuksiin ja uhkavakoojiin.

Kyberuhat voidaan nähdä siis yksittäisenä osana suurempaa kyberturvallisuuden kokonaisuutta. Skopik ym. (2016) jakavat julkaisussaan näkemyksen, että

luonteeltaan kybermaailmaa häiritsevät uhat ovat globaaleja ja motiivin olevan hyökkääjällä yhä useammin taloudellisen hyödyn tavoittelemisen sijaan aiheuttaa mahdollisimman paljon yhteiskunnallista ja poliittista häiriötä. Useimmat kyberuhista liittyvätkin erilaisiin rikollisjoukkioihin, terroristeihin, hakkereihin ja vihamielisiin hallituksiin, jotka ovat halukkaita tekemään kyberhyökkäyksiä nimenomaan kriittisiä infrastruktuureja vastaan (Blakemore & Awan, 2012). Pääsääntöisesti kyberuhka on jonkin ulkoisen uhkatekijän aiheuttama, vaikkakin uhri voi altistaa itsensä näille uhille tietoturvattomalla käytöksellä. Useimmiten kuitenkin kyseinen henkilö tai organisaatio valikoituu kohteeksi hallussa olevan arvokkaan resurssin tai statuksen vuoksi. Kyberuhkien suosituimpien kohteiden joukossa vuodesta toiseen keikkuvat pääasiassa kriittisen infrastruktuurin toimialat kuten terveystoimiala, valmistus ja tuotanto, pankki- ja rahoitustoimiala, julkishallinto sekä liikenne- ja kuljetustoimialat niiden yhteiskunnalla ja toimintaympäristölleen tärkeän statuksen ja arvokkaiden resurssien vuoksi (Norri-Sederholm ym., 2019).

IBM (2022) tilastoi tuottamassaan raportissa, että 97 % maailmalla jylläävistä kyberuhista oli rikollisen toiminnan aiheuttamia, vain 2 % oli valtiollisten tekijöiden ja 1 % erilaisten hakkerien aiheuttamia. Interpol tutki vuorostaan vuoden 2020 kyberrikosraportissaan COVID-19-pandemiasta aiheutuneita ja siihen liittyvien kyberuhkien ja – rikosten kasvua. Raportissa todettiin, että etätyön lisääntymisen vuoksi organisaatioiden verkot ovat entistä monimutkaisempia, hallitsemattomampia ja enemmän haavoittuvaisempia, joka on ollut omiaan kasvattamaan uhkien määrää merkittävästi (INTERPOL, 2020). Kuviosta 3 voidaankin nähdä, kuinka suurta kasvua seuraavien kyberuhkien kohdalla oli tapahtunut Interpolin jäsenvaltioissa COVID-19 jäljiltä.



KUVIO 3 Kyberuhkien lisääntyminen COVID-19 johdosta (INTERPOL, 2020)

Raportista ja kuviosta 3 on huomattavissa, että erityisesti kyberuhista haitalliset verkkotunnukset (malicious domains), haittaohjelmat/kiristysohjelmat (malmware/ransomware), kalastelu/huijaukset (phishing/scam/fraud) ja väärät uutiset (fake news) lisääntyivät merkittävästi koronapandemian kiihdyttämän etätyöhön siirtymisen takia. Nämä uhkatekijät ovat olleet omiaan lisäämään epävarmuutta kybertoimintaympäristöön ja korostavat organisaatioiden tarvetta ottaa näitä uhkia huomioon henkilökuntansa kouluttamisessa. Näitä uhkatyyppejä tavataan yhä, mutta myös uusia havainnoidaan joka vuosi.

Kyberuhille on ominaista, että ne kehittyvät hyvin nopeasti uusien hyväksikäyttömahdollisuuksien ilmetessä. Rapid7 vuoden 2022 kyberturvaraportissaan tiedotti, että hyökkääjät kehittävät ja ottavat käyttöön hyväksikäyttökohteita nopeammin kuin koskaan aikaisemmin. Jopa 56 prosenttia raportissa mainituista haavoittuvuuksista käytettiin hyväksi seitsemän päivän kuluttua niiden julkistuksesta. Tämä oli 12 % enemmän kuin vuonna 2021 ja 87 % enemmän kuin vuonna 2020. (Rapid7, 2022.)

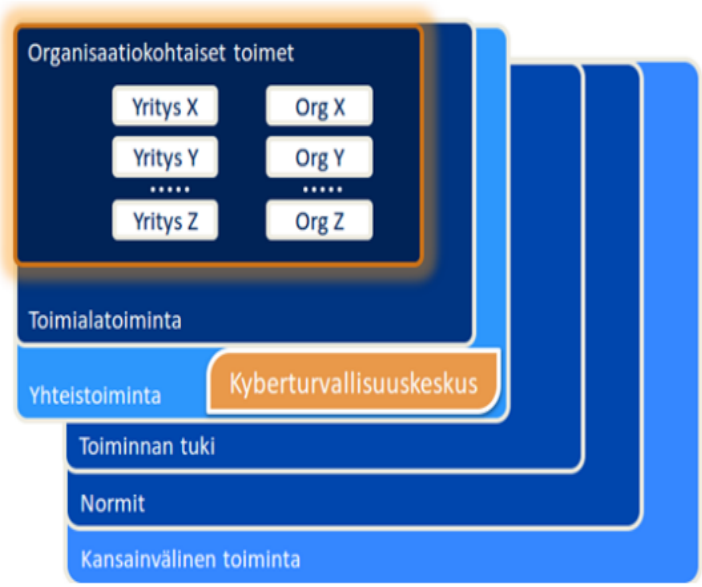
Kyberuhkia vastaan voidaan suojautua useilla eri tasoilla ja tavoilla. Lähtökohtaisesti jokaisella organisaatiolla on velvollisuus huolehtia oman toimintansa kyberturvallisuudesta ja tehdä yhteistyötä muiden toimijoiden kanssa uhkien tunnistamisessa ja torjumisessa (Norri-Sederholm ym., 2019). Organisaation jatkuvuudenhallinnalla ja tilannetietoisuudella on merkittävä rooli tässä. Pöyhönen ym. (2021) korostavatkin omassa tutkimuksessaan, että ilman ajantasaista

tilannekuvaa sekä -tietoisuutta on haastavaa tunnistaa mahdollisia uhkia ja siten toimeenpanna riittäviä hallintakeinoja. Erityisesti häiriötilanteissa ajantasaisen tilannekuvan tuottamisen tärkeys korostuu, mutta jatkuvasti ajantasaisella tilannekuvalla voidaan ehkäistä edes joutumasta mahdollisiin häiriötilanteisiin. Aina kuitenkaan hyvä varautuminen ei riitä ja kyberuhkat voivat varautumisesta huolimatta konkretisoitua hyökkäyksiksi ja tietovuodoiksi, tämän vuoksi organisaatioiden tulee pitää huoli myös sietokykynsä ja palautumisensa kehittämisestä (Norri-Sederholm ym., 2019). Strategisen tason teoilla on näin ollen iso rooli tilannekuvan ajantasaisuuden ja tulevaisuuden ennakoinnin suhteen. Tämä on kuitenkin helpommin sanottu kuin tehty jatkuvasti kehittyvien uhkien vaaniessa ja toimintaympäristön kokiessa muutoksia.

3.3 Kybertoimintaympäristö

Kybertoimintaympäristö (engl. cyber environment, cyberspace) on käsitteenä laaja ja moninainen kokonaisuus, jonka hahmottaminen ei ole usein kovin yksiselitteistä. Tyypillisesti kybertoimintatoimintaympäristö määritellään yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaksi toimintaympäristöksi. Kybertoimintaympäristölle tunnusomaista on, että elektronista ja sähkömagneettista toiminnan kirjoa käytetään datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Tähän ympäristöön kuuluvat datan ja informaation käsittelyyn liittyvät fyysiset rakenteet sekä näiden rakenteiden lisäksi kaikki toimintaympäristön toimijat. (Lehto, 2021; Turvallisuuskomitea, 2018.)

On hyvä tiedostaa, ettei kybertoimintaympäristö ole vain elektroninen irrallinen kokonaisuus vaan, että se on sekä ihmisten, organisaatioiden että fyysisten systeemien muodostama vaikutusympäristö, jossa jokaisella on oma roolinsa kyseisen ympäristön kyberturvallisuuden ylläpidossa. Kuviossa 4 on hahmoteltu kybermaailman viitekehystä. Toimialakohtaisella tasolla yritykset toimivat toimialakohtaisten säädöstensä puitteissa. Yhteistoiminta käsittää yritysten välisen toimialariippumattoman yhteistoiminnan lisäksi yhteistoiminnan sekä vuorovaikutuksen Kyberturvallisuuskeskuksen kanssa. Toiminnan tukeen liittyvät kyberturvallisuusyritysten tuottamat palvelut sekä korkeakoulujen tutkimus että koulutuksellinen tuki. Normisto koostuu sääntelyistä ja parhaista käytännöistä. Uloin kehys eli kansainvälinen toimintakenttä on koostumus kansainvälistä yhteistoimintaa, sisältäen globaalit logistiikkaverkostot ja maksuliikennejärjestelmät. (Lehto ym., 2017.)



KUVIO 4 Kyberturvallisuuden verkottunut toimintaympäristö (Lehto ym., 2017)

Esimerkiksi Ulkoministeriö (2022) Ajankohtaisselonteko turvallisuusympäristön muutoksesta – julkaisussaan korostaa yritysten ja organisaatioiden roolia Suomen kybertoimintaympäristön turvaamisessa ja kuinka varsinkin Suomessa pyritään rakentamaan vahvaa kyberturvallisuuden ekosysteemiä, joka tuo yhteen julkisen ja yksityisen sektorin toimijoita. Kyberturvallisuuskeskus on nimenomaan yksi näistä osapuolista, jotka kyberturvatuotteillaan ja -palveluillaan yrittää auttaa muita organisaatioita panostamaan kyberturvallisuuteensa ja näin ollen myös kybertoimintaympäristönsä kehittämiseen. Kuvio 4 korostaakin erinomaisesti Ulkoministeriön näkökulmaa verkottuneesta ja yhteistyötä vaativasta kybertoimintaympäristöstä, jossa organisaatiot ja yksilöt joutuvat toimimaan tänä päivänä.

Lehdon (2021) mukaan kybertoimintaympäristön ominaisuuksiin kuuluvat kehityksen suuri nopeus, tapahtumien hektisyys ja eri järjestelmien kompleksisuus. Hän myös mainitsee samaisessa julkaisussaan, että kybertoimintaympäristölle on leimallista muutosnopeus. Muutosnopeus edellyttää kaikelta toiminnalta nopeaa reagointikykyä, ketteryyttä ja kykyä varautua myös tilanteisiin, joita ei täysin kyetä ennakoimaan. Tämä korostaa ennen kaikkea useiden eri toimijoiden yhteistyökykyä ja tilannetajun tärkeyttä. Muutosnopeassa toimintaympäristössä jatkuva tilannekuvan kehittäminen ja ylläpitäminen voidaankin nähdä elinehtona kenelle tahansa toimintaympäristön toimijalle. Lehdon ja Limnéllin (2021) mukaan tiedonkeruu ja tähän tietoon perustuva päätöksenteko tapahtuu tällaisessa muutosnopeassa ympäristössä kuitenkin usein liian hitaasti suhteessa kyseisen ympäristön muutosnopeuteen, tämä vaikeuttaakin tarkan ja oikea aikaisen tilannekuvan muodostamista.

Muutosnopeuden lisäksi kybertoimintaympäristöä voisi kuvailla luonteeltaan ylikansalliseksi ja maailmanlaajuiseksi, jota ei kukaan yksinään omista ja

jossa valtion ja fyysisten rajojen ylittävä toiminta voi pahimmillaan aiheuttaa valtioiden välille suvereenisuus- ja turvallisuusristiriitoja (Laari ym., 2019; Lehto, 2021). Madahar ja Parish (2016) toteavatkin kybertoimintaympäristön olevan näistä syistä jopa mahdoton säänneltävä sekä vaikeasti määrättävä ja hallittava kokonaisuus. Jatkuvat uhkatekijät ovatkin lähempänä kuin koskaan aikaisemmin tässä ympäristössä.

Pöyhösen (2018) mukaan kybertoimintaympäristö on hyvä huomioida uhkien lisäksi myös mahdollisuutena ja voimavarana. Mikäli toimintaympäristö pystytään pitämään turvallisena helpottaa se yksilöiden sekä yritysten toiminnan suunnittelua ja toteuttamista. Turvallinen toimintaympäristö voidaan nähdä myös kilpailuetuna ja houkuttelevana investointikohteena. Esimerkiksi erilaisten organisaatioiden ja yksityisten sijoittajien silmissä Suomi nähdään todennäköisesti nyt Natoon liittymisensä jäljiltä turvallisempana toimintaympäristönä ja näin ollen houkuttelevampana sijoituskohteena kuin ennen liittymistä.

3.4 Strategisen tilannekuvan muodostaminen

Kybertoimintaympäristön kattava analysointi on olennainen edellytys kokonaisvaltaisen kyberturvallisuutta koskevan tilannekuvan aikaansaamista. Kyberturvallisuuden sanaston (2018) mukaan kyberturvallisuuden tilannekuva perustuu erilaisiin havaintoihin, analyyseihin, mittareihin, jotka voivat sisältää teknisestä lähteestä tulevaa dataa tai ihmisten esiin nostamia poikkeamia. Kyberturvallisuuden tilannekuvaa tuotetaan yhteistyössä eri toimijoiden kesken. Suomessa Kyberturvallisuuskeskuksella on suuri rooli kansallisen kyberturvallisuuden tilannekuvan kokoamisessa ja koordinoimisessa niin yksilöiden kuin organisaatioiden saataville (Kyberturvallisuuskeskus, 2023; Turvallisuuskomitea, 2018).

Strategisen kybertilannekuvan muodostamisen kannalta keskeisiä tehtäviä ovat riskianalyysi ja liiketoiminnan kannalta kriittisten varojen ja prosessien tunnistaminen (Evesti ym., 2017). Näiden kriittisten omaisuuksien, jotka liittyvät organisaation päätavoitteisiin ja liiketoimintaan, tunnistaminen ja suojaus on tapahduttava organisaation strategisella tasolla. Kriittisten omaisuuksien ja organisaation toimintaympäristön analysoinnissa aiemmin esitelty SWOT-viitekehys voikin tulla tarpeeseen.

Knerler ym., (2022) jakavat kybertilannekuvan ja sen tietoisuuden saavuttamisen kolmeen komponenttiin: informaatioon, analytiikkaan ja visualisointiin. Informaatiolla Knerler ym. (2022) viittaavat erilaisiin tietolähteisiin, joita voi olla muun muassa laite- ja järjestelmätoimittajien julkaisemat haavoittuvuustiedot. Analytiikan avulla kerättyä tietoa tulkitaan ja jalostetaan. Tämän tutkimuksen puitteissa analytiikkametodina toimii SWOT-viitekehys, jolla tulkitaan ja jalostetaan kerättyä aineistoa eli informaatiota. Visualisoinnissa aiemmin kerätystä ja jalostetusta tiedosta koostetaan esitettävä kokonaisuus päätöksenteon tueksi. Nämä kolme komponenttia toimivat apuna tilannekuvan ja tilannetietoisuuden muodostamisen tavoitteiden saavuttamisessa.

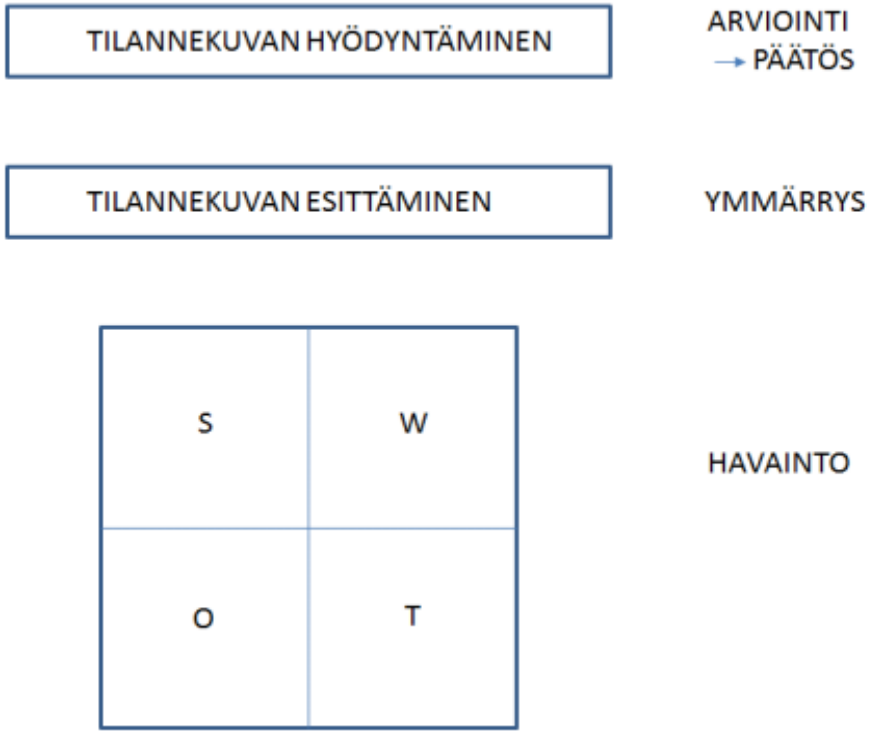
Kybertilannekuvan niin strategisen kuin operatiivisen muodostamisen perusajatus on, ettei sitä voida tuottaa samanlaisin sisällöin kaikille tarvitsijoille. Sen tarvevaatimukset ja sitä kautta myös sisältö vaihtelevat eri päätöksenteko- ja johtamistasojen sekä toimijoiden välillä. Nämä erilaiset ja uniikit tarvevaatimukset, joita eri toimijat odottavat tilannekuvatiedoiltaan on suuri vaikutus muodostuvaan uniikkiin kokonaisuuteen. (Evesti ym., 2017; Laari ym., 2019.)

Evesti ym. (2017) kuvaavatkin kybertilannekuvan muodostamisen lähtevän tavoitteesta. Tavoitteena voi olla vaikkapa liiketoiminnan resurssien heikkouksien parempi tilannetietoisuus. Määritelty tavoite voidaankin nähdä ihanneloppputuloksena, jota kyberturvallisuuden tilannekuvaa ja -tietoisuutta rakentava porukka kuin myös päätöksentekijät tietävät tavoitella toiminnallaan. Yleiseksi tavoitteeksi Evesti ym. (2017) määrittelevät, tavoitteen tuottaa tietoa päätöksenteon tueksi tietylle organisaation tasolle. Aiemmin sivuttu kenelle tilannekuvaa tehdään, päätöksenteon taso ja saatavilla olevan tiedon luonne määrittelevät pitkälti tuotettavan tilannekuvan sisältöä ja lopputulosta. Evesti ym. (2017) määrittelevät nämä kybertilannekuvan ja tilannetietoisuuden tavoitetta yksilöivät ja muokkaavat tekijät:

1. laajuudeksi (scope),
2. tasoksi (level),
3. näkökulmaksi (viewpoint)
4. päätöksenteoksi (desicion making).

Scopella viitataan siihen, että minkä tason laajuudella tilannekuvaa käsitellään. Onko kyseessä esim. kansallinen kybertilannekuva vai organisaation kybertilannekuva. Level määrittelee sen mille organisaation tasolle ja sitä kautta myös kelle on tavoitteena kybertilannekuvaa tuottaa. Aiemmin mainitut operatiivinen ja strateginen taso ovat kyseiset toimitasot. Halutun kybertilannekuvan ja tiedon luonteella on täten vaikutusta tavoitteeseen. Lopullisen päätöksentekijän asema ja tehtävä määrittelevät, minkä tyyppistä on tarvittava kybertilannekuva ja tietoisuus. Viewpoint tarkoittaa millä näkökulmalla ja mihin tarkoitukseen tilannekuvaa sovelletaan. Näkökulmia ovat liiketoiminnallinen, oikeudellinen ja tekninen näkökulma. Painotettu näkökulma vaikuttaa kybertilannekuvaan kerätyn datan luonteeseen. Oikeudellisessa näkökulmassa päätöksentekijä tarvitsee tietoa nykyisestä ja tulevasta sääntelystä ja siitä, miten ne vaikuttavat organisaatioon, kun taas tietoteknisessä näkökulmassa kerätty aineisto tulee pääsääntöisesti suoraan omista valvontajärjestelmistä teknisinä syötteinä. Viimeinen vaikuttava tekijä, decision making eli päätöksenteon malli määrittyy pitkälti aiempien tekijöiden pohjalta. Automatisoitua päätöksentekoa voidaan soveltaa operatiivisimmassa tekniseen näkökulmaan pohjaavissa kybertilannekuvan määrittelyissä, kun taas inhimillistä päätöksentekoa enemmän ihmisläheisissä kuten strategisessa liiketoiminnalliseen näkökulmaan pohjaavassa kybertilannekuvan määrittelyssä.

Tilannekuvatoiminnan tulkitsemista ja johdonmukaista analysointia varten on tärkeä valita sopiva tilannekuvan analysoinninmenetelmä. Menetelmiä on useita erilaisia ja niiden valinta riippuu organisaation tarpeista ja tavoitteista. Aiemmin esitelty SWOT-analyysi on yksi yleisimmistä strategisen analysoinnin menetelmistä ja olennainen tämän tutkimuksen tutkimuskysymyksen kannalta, joten käsittelemme sitä. Tämä auttaa organisaatiota hyödyntämään vahvuuksiaan ja mahdollisuuksiaan, samalla kun heikkoudet ja uhkat tunnistetaan ja korjataan. Kuviossa 5 on esitetty Pöyhösen (2018) SWOT-analyysiin perustuva organisaation yleinen tilannekuvaprosessi.



KUVIO 5 Organisaation yleinen tilannekuvaprosessi (Pöyhönen, 2018)

Pöyhösen (2018) mallissa kyberympäristöön kohdistetaan organisaatiokohtaisten vahvuuksien ja heikkouksien analysointi samalla arvioiden toimintaympäristön mukanaan tuomia mahdollisuuksia sekä uhkia. Nämä muodostavat pohjan havainnoille, jotka esitetään tilannekuvana, ja on mahdollista muodostaa ymmärrys SWOT:n riippuvuussuhteiden mukaisesti. Näiden pohjalta voidaan rakentaa perusteltuja arvioita vahvuuksien kehittämisestä ja mahdollisuuksien hyödyntämisestä sekä mahdollisten heikkouksen ja tunnistettujen uhkien poistamisesta, jotka voivat vahingoittaa organisaatiota.

Erilaisten analyysityökalujen tai tilannekuvaa yksilöivien tekijöiden lisäksi on hyvä muistaa, että toteutukseen vaikuttavat erityisesti ihmiset, jotka tilannekuvaa tuottavat. Kybertilannekuvan toteuttaminen tulisi nähdä tiimityönä,

koska dynaaminen ja monimuotoinen kybertoimintaympäristö voi olla yksilön kyvykkyyksien saavuttamattomissa, joten oikeanlaisen kybertilannekuvan tuottamisen kannalta tiimityöskentely antaa yksilövetoista lähestymistapaa paremmat lähtökohdat (Eldardiry & Caldwell, 2015). Pöyhönen ym. (2021) korostavatkin omassa tutkimuksessaan, ettei kybertilannetietoisuus ja -tilannekuva kehity yksilön tai pienen piirin sisällä, vaan se vaatii sidosryhmien välistä tiedon jakoa. Strategisen kybertilannekuvan näkökulmasta paras lopputulos olisikin, että mahdollisimman moni päätöksentekijä kuin myös asiantuntija pystyisi kontribuoimaan lopputulokseen. Täten itse lopputuote voi olla tarpeeksi laadukas ja ymmärrettävä, että sen voisi jalkauttaa koko organisaatiolle.

4 TUTKIMUSMENETELMÄ

Tutkimus toteutetaan kvalitatiivisena tutkimuksena, jossa päämenetelmänä sovelletaan suunnittelututkimusta eli Design Science Researchia. Aineisto tutkielmaa varten on kerätty kyberturvallisuus- ja uhkatietoraportteja toteuttavien kyberturvallisuus yritysten vapaasti käytössä olevista raporteista. Nämä raportit analysoidaan SWOT-viitekehystä hyödyntäen. Tavoitteena on tuottaa ja määritellä SWOT-analyysin pohjalta kyberturvallisuuden strateginen tilannekuva. Ensimmäiseksi tässä luvussa käydään läpi aineisto ja sen mahdolliset erityispiirteet. Tämän jälkeen esitellään Design Science Research – tutkimusmenetelmä eli suunnittelututkimus ja sen käyttö osana tätä pro gradua. Näiden pohjalta tässä pro gradussa vastataan seuraavaan tutkimuskysymykseen:

- Voiko SWOT-analyysista rakentaa viitekehyksen strategisen tilannekuvan tuottamiseksi?

4.1 Aineisto

Tutkimuksissa käytettävät aineistot on totuttu perinteisesti jakamaan kvalitatiiviseen eli laadulliseen ja kvantitatiiviseen eli määrälliseen aineistoon. Kvalitatiivisen aineiston suosiminen tarkoittaa sitä, että tutkimuksen aineistoina pääsääntöisesti käytetään erilaisia empiirisiä aineistoja, kuten tekstejä, haastatteluja, havainnointipäiväkirjoja, kuvia tai tiloja, joissa jokin toiminta tapahtuu (Juhila, 2023). Kvalitatiivisen aineiston tapauksessa aineistoja ei ensisijaisesti aleta muokkaamaan numeeriseen muotoon. Numeerinen tarkastelu ja määrään pohjaavat aineistoanalyysit ovat tyypillisempiä kvantitatiivisen tutkimuksen yhteydessä. Laadullisen tutkimuksen aineistolle on olennaista, ettei sitä ei pyritä irrottamaan kontekstistaan, vaan niitä päinvastoin tulkitaan osana kontekstia (Juhila, 2023). Tässä tutkimuksessa aineistona käytetään kyberturvallisuusorganisaatioiden julkisia kyberturvallisuus- ja uhkatietoraportteja, joita analysoidaan SWOT-

viitekehystä hyödyntäen. Kyseessä on niin sanottu luonnollinen aineisto eli aineisto, joka on syntynyt ilman että tutkija on vaikuttanut sen syntymiseen.

Aineistona käytettävät raportit ovat tuottaneet IBM (2022), Rapid7 (2022), Accenture (2021), Cisco (2022) ja Palo-Alto Networks (2023). Näistä jokainen on pitkän linjan toimija tietotekniikan alalla ja jokaiselta löytyy pitkää historiaa tietoturva- ja nykyisellään kyberturvallisuuspalveluiden ja toteutusten tarjoajina. Taulukossa 1 on esitettynä taulukoidussa formaatissa aineistona toimineiden raporttien julkaisija, raportissa käytetyn datan vuosi ja raporttityyppi.

TAULUKKO 1 Tutkimuksen aineisto

Julkaisija	**Data vuodelta**	**Raporttityyppi**
IBM	2021	Uhkatietoraportti
Rapid7	2022	Uhkatietoraportti
Accenture	2021	Uhkatietoraportti
Cisco	2022	Uhkatietoraportti
Palo-Alto Networks	2022	Uhkatietoraportti

Raporteissa käytettävä data on pääsääntöisesti ensikädentietoa eli nämä yritykset ovat keränneet datan omista järjestelmistään. Raporteissa on myös viitattu ja käytetty lähteinä muiden kyberturvallisuus organisaatioiden julkaisuja ja uutislähteitä, mutta ne ovat enemmän omaa dataa tukevassa roolissa. Raporttien julkaisuajankohdat ovat vuosilta 2021 ja 2022, joten niiden data sisältää havaintoja näiltä vuosilta. Joitain raportteja on jo julkaistu myös vuotta 2023 koskien, mutta tutkimuksen aineiston saamisen varmistamiseksi keskityttiin aiempien vuosien julkaisuihin.

4.2 Design Science Research

Design Science Research (DSR), vapaasti suomennettuna suunnittelututkimus, on tieteellisen tutkimuksen toteuttamistapa, jossa pyritään tieteellisesti kehittämään artefakteja ja legitiimiä suunnittelutietämystä, jonka päämääränä on ratkoa tunnistettuja organisatorisia ongelmia ja parantaa ihmisten tietämystä (Brocke ym., 2020; Hevner ym., 2004). Yksinkertaisimmillaan DSR voidaan ajatella tieteellisenä tutkimuksena, jonka avulla pyritään löytämään ratkaisu ongelmaan jollakin käytännön alalla. DSR on tutkimusmenetelmänä merkittävässä roolissa erityisesti sovelletuilla tieteenaloilla kuten tekniikan, arkkitehtuurin, kauppatieteiden ja tietojärjestelmiin liittyvillä tieteenaloilla, joilla luodaan uusia ratkaisuja merkityksellisiin suunnitteluongelmiin (Brocke ym., 2020).

DSR tuottaa tieto-osaamista eli niin sanottua ohjeistavaa tietämystä siitä, kuinka asioita tulee tehdä ja ongelmia ratkaista. Käytännöllisen ja soveltavamman lähestymistavan ansiosta DSR nähdään myös hyvänä ratkaisuna akateemikoille tuottaa enemmän tietämystä, josta on suoraa hyötyä myös akateemisen maailman ulkopuolella (Gregor ym., 2020) .

DSR:ssä lähtökohtaisesti pyritään tunnistamaan ongelma tai ongelmat ja suunnittelemaan artefaktit vastaamaan näihin ongelmiin. Ongelman määrittteleminen ja tunnistaminen on lähtökohta tutkimuksen motivoinnilla ja toteuttamiselle, mutta myös olennainen osa myöhempien vaiheiden toteuttamista ja lopullisten tulosten arviointia. Tutkimusprosessiin kuuluu tietojen kerääminen ja analysointi, ratkaisun suunnittelu-, kehitys- ja toteutusprosessi, jotka tapahtuvat yleensä yhdessä tai useammassa vaiheessa. DSR:ssä on vähintään yhtä tärkeää artefaktin kehittämisen lisäksi, sen arviointi ja lopullisten tulosten raportointi. Arviointi ja raportointi takaavat sen, että tutkimuksella voidaan tuottaa uutta tietämystä muille ja tätä raportoiduista tuloksista saatua tietämystä on mahdollista hyödyntää sekä jatkojalostaa mahdollisissa jatkotutkimuksissa ja artefaktien käytäntöönpanossa. On kuitenkin tärkeä huomioida se, ettei DSR:n tutkimusprosessi ole aina aivan täysin lineaarinen prosessi vaan prosessi voi elävää tutkimuksen aikana edestakaisin. Tutkimuksen kontekstilla on vaikutusta tutkimusprosessin aloitusvaiheeseen ja itse tulosten riittävyyteen. (Hevner ym., 2004; Peffers ym., 2007.)

5 TULOKSET

Tämä luku sisältää tutkielman varsinaisen analyysiosion ja tulokset. Luvussa tarkastellaan ja analysoidaan kyberturvallisuusraporteista löydettyjä tuloksia SWOT-viitekehyksen avulla tehden havaintoja, joiden pohjalta tuotetaan strateginen tilannekuva. Tulosten pohjalta haluamme saada vastauksen seuraavaan tutkimuskysymykseen: Voiko SWOT-analyysista rakentaa viitekehyksen strategisen tilannekuvan tuottamiseksi?

5.1 ANALYYSI

Tilannekuva ja strategia limittyvät analyysityössä sekä tulevan suunnittelussa. Strategisen tason kyberturvallisuuden tilannetietoisuus tuottaa pitkän aikavälin tietoa johtaville päätöksentekijöille. Sen avulla voidaan kertoa ja määritellä tulevaisuuden kehityssuunnat. Strategisen tilannekuvan avulla organisaatio pystyy suunnittelemaan mahdollisia tulevaisuuden investointeja oman liiketoimintansa tueksi.

Lehto ym. (2017) ja Pelkonen ym. (2016) olivat jo omissa tutkimuksissaan hyödyntäneet SWOT-viitekehystä tilannekuvan arviointiin ja jalostaneet sitä paremmin vastaamaan kyberturvallisuuden vaatimuksia soveltamalla esim. Suomen kyberturvallisuusstrategian strategisten linjausten kohdan 3 yritystoimintaa käsittelevää kokonaisuutta, ja ISO 9000-laatustandarin ja ISO 27000-informaatioturvallisuuden standardin keskeisimpiä pääkohtia. Tämä lähestymistapa on kuitenkin hyvin sidoksissa Suomen sisällä tapahtuvaan toimintaan ja toimii

paremmin kansallisella laajuudella, joten kansainvälisemmän lähestymistavan, lähteiden ja organisaatiotason laajuuden vuoksi ei tässä tutkimuksessa haluttu hyödyntää heidän jalostamaansa versiota vaan tehdä omat huomiot ja kehitysehdotukset perinteisen SWOT-viitekehyksen pohjalta.

Aineistona olleet uhkatieto- ja kyberturvallisuusraportteja lähdettiin analysoimaan SWOT-viitekehystä hyödyntämällä. Sen nelikenttämalli antaa selkeät raamit, kuinka teemoitella ja jakaa hyödynnettävät havainnot raporteilta. Taulukkoon 2 on listattu aineistoista löytyneitä havaintoja SWOT-viitekehyksessä analysoituna. Jokainen viitekehyksen osa-alue löydöksineen käydään vielä tarkemmin läpi alla erillisissä alaluvuissa. Raporteilta on teemoittelemalla ja ryhmittelemällä pyritty tunnistamaan oleellisimmat tiedot ja sijoitettu nämä niitä parhaiten kuvaavien SWOT-viitekehyksen osa-alueiden alle. Sisäisiin vahvuuksiin ja heikkouksiin on ryhmitelty kaikki oleelliset raporteilla esiintyneet tiedot, joilla voisi olla vaikutusta organisaation sisäisiin ominaisuuksiin. Ulkoisiin mahdollisuuksiin ja uhkiin on samaan tapaan ryhmitelty kaikki oleelliset organisaation ulkoisiin ominaisuuksiin liittyvät tiedot. Havainnot raporteilta löytyvät teemoiteltuna nelikenttämallin mukaisesti alla taulukosta 2:

TAULUKKO 2 SWOT-analyysin havainnot

	Vahvuudet	**Heikkoudet**
Sisäiset	• Riskienhallinta prosessi • Henkilökunnan osaaminen ja tietoisuus • Positiiviset kokemukset aikaisemmista tietoturvaloukkauksista • Henkilöstö ajantasaisesti koulutettu tietoturva-asioissa • Järjestelmät ja sovellukset ajan tasalle päivitetty • Oma havainnointijärjestelmä (SIEM tai SOC) • Käyttäjä- ja identifikaatioiden hallintajärjestelmät	• Järjestelmähaavoittuvuudet (nollapäivähaavoittuvuudet) • Haavoittuvuusraporttien uhat omissa järjestelmissä • Henkilöstön tietoturvakoulutuksessa aukkoja • Aikaisempien tietoturvaloukkausten vaikutukset • Käyttäjän taidoista johtuva haavoittuvuus • Havainnointijärjestelmien puute • Liian nopea pilvi-infrastruktuurin laajentaminen ja käyttöönotto • Puutteet tavanomaisissa torjuntatoimissa
	Mahdollisuudet	**Uhat**
Ulkoiset	• Hyvä valmistautuminen • Tilannetietoisuus • Uhkien kehityksen seuraaminen • Yhteistyö • Sääntelyt osaksi tekemistä • Nollaluottamus (Zero Trust Approach)	• Yleisten järjestelmien haavoittuvuudet (esim. CVE-2021-34523, CVE-2021-34473, CVE-2021-31207) • Kiristyshaittaohjelmat • Palvelunestohyökkäykset • Trendit • Kyberrikollisuus • Haktivismi • Toimintaketjuhaavoittuvuudet • Konfliktit (valtioiden, yritysten jne.)

5.1.1 Vahvuudet

Vahvuuksien osa-alueeseen on kerätty aineistoista kaikki tekijät, jotka positiivisesti vaikuttavat organisaation kyberturvallisuuteen ja sen tilannekuvan koostamiseen. Raporteista oli löydettävissä useita positiivisesti organisaation sisäisiin vahvuuksiin luettavia asioita. Ylätason huomiona, että vahvuuksiin liittyvät asiat ovat aika selkeästi enemmän tai vähemmän strategiseen johtamiseen liitoksissa olevia toteutuksia. Moni näistä liittyikin vahvasti organisaation riskienhallintaprosesseihin ja tapaan järjestää organisaation hallinnollista puolta vastaamaan vahvuuksia. Henkilöstön osaamista ja tietoisuutta kyberturvallisista toimintatavoista korostettiin joka raportissa. Sisäisten vahvuuksien näkökulmasta organisaation vahva panostus henkilöstön tietoturvaosaamiseen voidaankin nähdä jonkinlaisena tukipilarina vahvuuksien rakentamiselle. Tämän osaamisen kouluttaminen ja päivittäminen nousivat pinnalle kyseisten asioiden vanavedessä.

Teknisempiä aspekteja, jotka nousivat esille raporteista vahvuuksiin liittyen, olivat organisaation omat havainnointijärjestelmät (SIEM tai SOC). Oma havainnointikeskus, josta data on saatavilla ympäri vuorokauden, nähtiin vahvuutena. Näin pystytään itse vaikuttamaan kerättyyn dataan ja varmistetaan havaintopisteiden saaminen, milloin vain. Tämä ei kuitenkaan tarkoita, etteikö havainnointipalveluita voisi hankkia muilta toimijoilta. Jonkinlainen käyttäjien- ja identifikaatioiden hallintajärjestelmä koettiin organisaatiolle olevan hyödyksi. Vahvuuksiin oli myös luettavissa järjestelmien ja sovellusten ajan tasalla pitäminen ja päivittäminen. Näiden ajan tasalla pitäminen onkin erityisen tärkeää käyttäjien tietoturvan ja kallisarvoisen datan näkökulmasta.

5.1.2 Heikkoudet

Sisäiset heikkoudet sisältävät havaittuja negatiivisia tekijöitä. Onko kyberturvallisuus kokonaisuutena huomioitu organisaatiossa? Mitä kykyä ei ole kehitetty? Heikkouksien analysoinnissa korostuivat erityisesti omista järjestelmistä ja käytettävien sovellusten ajan tasalla pitäminen. Raporteissa esiteltyjen uhkien ja löydösten peilaaminen omiin järjestelmiin on syytä nostaa erityishuomioon, koska niin sanotut nollapäivähaavoittuvuudet (zero-day vulnerabilities) järjestelmissä nousivat selkeästi suurimmaksi heikkouteen viittaavaksi tekijäksi raporteilla.

Liian nopea pilvi-infrastruktuurin laajentaminen ja käyttöönotto oli myös ryhmiteltävissä heikkouksien joukkoon. Näiden asioiden kunnollisen implementoinnin puute altistaa organisaation hyvinkin pian ulkoisille uhkille.

Vahvuuksien yhteydessä esiin nostettu henkilöstön osaaminen ja kouluttaminen nousi esiin myös heikkouksia määriteltäessä raporteilta. Tässä yhteydessä nimenomaan puutteet näissä henkilöstön osaamisissa ilmentävät myös organisaatioiden sisäisiä heikkouksia. Aiemmin kohdattujen tietoturvaloukkausten rooli nousi myös esiin ja ennen kaikkea onko niistä otettu opiksi eli osattu vahvistaa heikkoja kohtia ja olla paremmin valmistautunut ensi kerralla. Ylipäätänsä puutteet tavoissa ottaa opiksi vanhoista virheistä ja kehittää heikkouksiaan, on

jo itsessään negatiivista vaikutusta organisaation toimintaan ja heikentäen sen toimintavalmiuksia.

5.1.3 Mahdollisuudet

Mahdollisuuksia oli selkeästi hankalinta havaita aineistoista. Koska mahdollisuudet ovat positiivisia ulkoisia tekijöitä tai piirteitä, jotka voivat suosia tai helpottaa organisaation etujen hyödyntämistä organisaation ulkopuolelle ja yhteyksien luomista toimintaympäristöönsä (Nyarku & Agyapong, 2011), oli selkein mahdollisuutena nähtävä asia yhteistyö. Yhteystyö eri sidosryhmien kanssa oli kyseessä sitten asiakas, kilpailija tai vaikka alihankkija, ja näiden kanssa tapahtuva kommunikaatio toimintaympäristön yleisistä uhista korostui raporteilla. Tämän toimintatavan näkeminen mahdollisuutena ja hyötynä tukee myös aiemmin esiteltyä näkemystä verkottuneesta kybertoimintaympäristöstä ja siellä tapahtuvasta vuorovaikutuksesta. Yhteistyö on tällä tavalla myös liitoksissa esille nousseeseen tilannetietoisuuteen, joka oli helppo myös sijoittaa mahdollisuuksien kategoriaan.

Yksi oleellisimmasta löydöistä raportteihin liittyen, joka voidaan mahdollisuudeksi tunnistaa, oli erilaisten sääntelyiden ja lakien sisällyttäminen osaksi organisaation toimintaa. Mitä aikaisemmassa vaiheessa kykenee implementoimaan uudet lakimuutokset tai sääntelyt vaikkapa tietoturvaan liittyen osaksi organisaation tekemistä, voi siitä saada selkeän kilpailuedun kilpailijoihin nähden. Joka tapauksessa kaikkien pitää samoja lakeja ja sääntelyitä noudattaa, joten aikaisessa vaiheessa niiden soveltaminen omaan toimintaan on ehdottomasti mahdollisuus. Näiden noudattamatta jättäminen aiheuttaisi vuorostaan taloudellisia uhkia sakkojen ja sanktioiden muodossa, sekä mahdollisia mainehaittoja.

IBM:n raportissa esiintynyt nollaluottamus (zero trust approach) toimintatavan käyttöönoton voisi nähdä myös mahdollisuutena. Siinä oletetaan, että tietoturvaloukkaus on jo tapahtunut. Tavoitteena on vaikeuttaa hyökkääjän liikkumista verkossa ja organisaation tietoteknisen infrastruktuurin ytimessä. Tätä kautta pyritään havainnollistamaan missä kriittiset tiedot sijaitsevat ja kenellä on pääsy näihin tietoihin, sekä vankkojen varmennustoimenpiteiden luominen koko verkkoon sen varmistamiseksi, että vain oikeat henkilöt pääsevät käsiksi näihin tietoihin oikealla tavalla (IBM, 2022).

5.1.4 Uhat

Aineistosta löydetyt uhat ovat hyvin pitkälti aiemmin kirjallisuusosuudessa läpikäytyjä uhkia. Kyberrikollisuus, haktivismi, palvelunestohyökkäykset ja kiristyshaittaohjelmat ovat yleisimmät uhista, joita organisaatiot kohtaavat aineiston mukaan. Näiden lisäksi aineistoista nousi esiin toimintaketjuhaavoittuvuudet eli erilaisissa organisaation sopimissa toimintaketjuissa voi olla haavoittuvuuksia, joihin ei pystytä itse vaikuttamaan ja näin ollen uhka aiheutua toimintaketjukumppanin heikosta kyberturvasta.

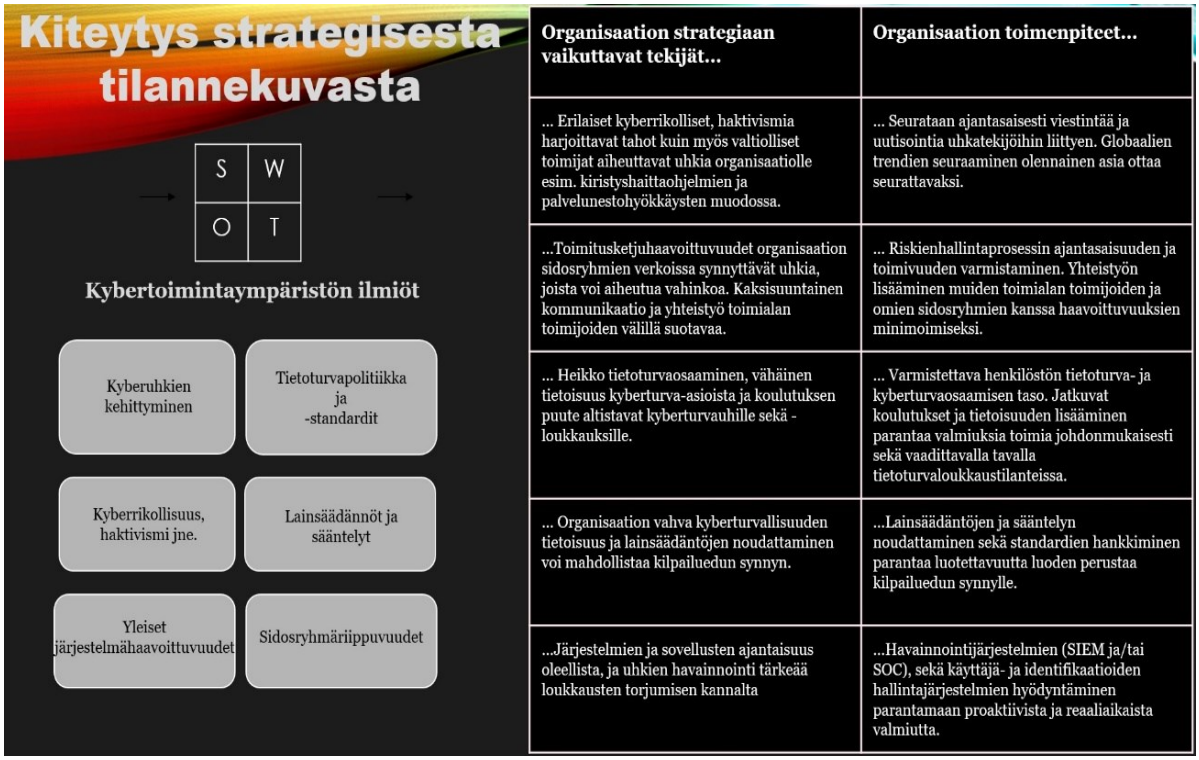
Myös kolmannelta osapuolelta hankitut järjestelmät kuten Microsoft Office – sovellukset tai Log4shell Java liitonnaisen sisältävät sovellukset ovat ulkopuolisia uhkien aiheuttajia organisaatiolle. Näistä löydetyt haavoittuvuudet raportoidaan ja ilmoitetaan yleisesti CVE-tunnisteilla, niin sanottuna julkisesti noteerattujen haavoittuvuuksien listana ja sen jälkeen ne ovat kaikkien tarkasteltavissa mukaan lukien pahantekijöiden. Näiden listojen ja tunnisteiden aktiivinen seuraaminen on siis oleellista organisaation uhkien torjunnassa ja niiltä suojautumisesta.

5.2 Strateginen tilannekuva

Kuviossa 5 esitelty Pöyhösen (2018) SWOT-analyysiin perustuvaa organisaation yleistä tilannekuvaprosessia mukaillen on SWOT-analyysin jälkeen edessä tilannekuvan koostaminen ja esittäminen. Edellä esitetyssä SWOT-analyysissa havainnoitiin aineiston pohjalta organisaation kyberturvallisuuteen positiivisesti ja negatiivisesti vaikuttavat tekijät. SWOT-analyysin havainnot toimivat perustana tilannekuvassa esiin nostettavien tekijöiden määrittelyssä ja tilannekuvan koostamisessa oikeanlaisen tilannetietoisuuden saamiseksi organisaation omasta tilanteesta osana kybertoimintaympäristöä.

SWOT nelikentän riippuvuussuhteiden mukaisten havaintojen ymmärtäminen ja kiteyttäminen esitettävään ja sidosryhmille ymmärrettävään muotoon on olennainen osa tilannekuvan muodostamista. Tässä yhteydessä onkin erityisen tärkeää kyetä arvioimaan tunnistettujen uhkien haitallisuutta omiin vahvuuksiin, ja toisaalta heikkouksien vaikutusta mahdollisuuksien hyödyntämisessä. Tilannekuvan muodostajalle on tässä vaiheessa suuri rooli, koska hän on loppukädessä päättämässä mikä on tilannekuvan arvoista tietoa ja mikä ei.

Näiden analyysista saatujen tulosten pohjalta on siis suoritettu itse tilannekuvan tuottaminen ja esittäminen alla olevassa kuvion 6 mukaisessa visuaalisessa muodossa.



KUVIO 6 Strateginen tilannekuva kybertoimintaympäristöstä

Strategiselle tilannekuvalle ei ole määritelty olemassa olevaa hyvien periaatteiden mukaista ja yleisesti hyödynnettävissä olevaa tilannekuvapohjaa tai -mallia. Koostettu tilannekuva onkin pitkälti tilannekuvan koostajan tai koostajien näkemyksestä ja tarpeista kiinni. Tutkielman tilannekuvan muodostamisessa on analysoitu analyysin tulokset ja parhaan mahdollisen osaamisen mukaisesti koostettu kyberturvallisuus kontekstin mukainen näkemyksen strategisesta tilannekuvasta.

Kuvion 6 strateginen tilannekuva kyberturvallisuusympäristöstä on syntynyt analyyttisen työn tuloksena. Kyseessä on strateginen kybertilannekuva organisaatiotasolle, jossa on pyritty esittämään kybertoimintaympäristön ilmiöt, jotka organisaation tulee ottaa huomioon toiminnassaan. Se sisältääkin analyysin organisaation vahvuuksista, heikkouksista, uhkista ja mahdollisuuksista kybertoimintaympäristössä, nostaen näiden pohjalta esille kysymyksiä kyberturvallisuuteen liittyen, joihin olisi syytä tarttua.

Tilannekuvaan on hahmoteltu organisaation strategiaan oletettavasti vaikuttavat tekijät SWOT-analyysin pohjalta ja näiden vastapainoksi tarjottu näkemys organisaation tarvittaviin toimenpiteisiin näihin liittyen. Tilannekuva perustuu aineistosta SWOT-viitekehyksen avulla koottuun tietoon kybertoimintaympäristön ilmiöistä, ilmiöiden vaikuttavuudesta organisaatiokontekstissa ja organisaatiossa huomioon otettavista asioista. Tämä tilannekuva tulisikin ymmärtää näkemyksenä kybertoimintaympäristön tekijöistä ja ilmiöistä osana organisaation kyberturvallisuuden toteuttamis- ja parantamisedellytyksiä.

Tilannekuva koostuu visuaalisesti käytännössä kolmesta eri kuviosta. SWOT-kuvio kuvastaa tilannekuvan tuottamisessa hyödynnettyä SWOT-viitekehystä ja muistuttaa teemoista tilannekuvaan nostettujen tekijöiden analysoinnin taustalla. SWOT:ssa tehdyt havainnot sisäisistä ja ulkoisista tekijöistä linkittyvät perustavanlaatuisesti tilannekuvan jälkimmäisiin kuvioihin.

Kybertoimintaympäristön ilmiöt - kuvion avulla on haluttu nostaa esille olennaisia toimintaympäristön ilmiöitä, kuten sidosryhmäriippuvuudet, lainsäädännöt ja sääntelyt, kyberuhkien kehittyminen, jotka nousivat esiin aineiston analysoinnin pohjalta. Toimintaympäristön ilmiöiden esille tuominen on olennainen osa tilannekuvan koostamista ja vallitsevan tilannekuvan ymmärtämistä, jotta voidaan paremmin perustella organisaation puutteet ja tarpeet. Kybertoimintaympäristön ilmiöt ovat vaikuttaneetkin viereiseen taulukkoon nostettuihin strategiaan vaikuttaviin tekijöihin. Nämä on tarkoitettu edistämään tilannekuvan tulkitsijan ymmärrystä viereisen taulukon johtopäätöksistä.

Kolmas kuvaaja eli taulukko Organisaation strategiaan vaikuttavista tekijöistä ja toimenpiteistä, on tarkoitettu todistamaan ja konkretisoimaan aineiston pohjalta tehdyt löydöt. Taulukon tarkoituksena on tilannekuvan hyödyntäjille todistaa nykyinen tilanne eli tuoda esiin esimerkiksi työntekijöiden heikko tietoturvaosaaminen tai tunnistetut haavoittuvuudet järjestelmissä, ja tehdä heidät tilannetietoiseksi organisaation tilasta näihin liittyen. Nykyisen tilan lisäksi taulukossa korostetaan tulevien toimenpiteiden tarpeellisuutta vaikuttaviin tekijöihin, kuten tieturvaosaamisen kohottaminen koulutusten kautta ja järjestelmähaavoittuvuuksien paikkaaminen, sekä otetaan kantaa organisaation toteuttamisedellytyksiin näihin liittyen. Organisaatiokohtaisesti tässä tilannekuvassa voitaisiin tarjota hyvinkin yksikohtaisia näkemyksiä vallitsevasta tilanteesta kuin myös korostaa selkeästi tarkemmin syy-seuraussuhteita vaikuttavien tekijöiden ja toimenpiteiden välillä. Tämän tutkimuksen konseptissa nämä havainnot joudutaan kuitenkin jättämään yleiselle tasolle.

6 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä luvussa käsitellään tutkimuksen tuloksia vastaamalla tarkemmin tutkimustehtävään ja pohditaan tutkimuksen merkitystä. Lisäksi alaluvuissa arvioidaan tutkimuksen luotettavuutta ja pohditaan edelleen mahdollisia jatkotutkimusaiheita.

Edellisessä luvussa tehtyjen havaintojen mukaan raporteista saatava informaatio on mahdollista sijoittaa SWOT-viitekehykseen ja analysoida sitä kautta, mutta SWOT:n yksinkertaiset ja joustamattomat osa-alueet hieman rajoittavat tai pakottavat tekemään kompromisseja näin spesifin tiedon analysoinnissa. Osa raporteista saatavasta informaatiosta kyberturvallisuuteen tai informaatioteknologian tietoturvaan liittyen oli vaikea teemoitella ja sijoittaa oikeaan osa-alueeseen viitekehyksen sisässä. Aiemmin Nyarku ja Agyapong (2011) tutkimuksen pohjalta esiin nostetut heikkoudet ja rajoitteet SWOT:n simppeliyden ja rakenteen joustamattomuuden vuoksi konkretisoituivatkin aineistoa analysoitaessa. Viitekehys joltain osin esim. uhkien osalta sopi hyvin analysointiin ja joiltain osin kuten mahdollisuuksien osalta ei toiminut. Paremman hyödynnettävyyden takia viitekehyksen spesifioiminen tai kehitys ei olisi pahitteeksi paremman ja luotettavamman lopputuloksen kannalta. Nykyisellä mallilla viitekehys jättää liian paljon roolia tilannekuvan koostajan kyvylle soveltaa ja analysoida analysoitavan materiaalin sisällön käytettävyyttä ja soveltuvuutta tietyiltä, kuten mahdollisuuksien osalta.

Esiin nostetuista SWOT:n heikkouksista huolimatta onnistunut tilannekuva saatiin luotua Horsmanheimon ym. (2017) korostamien hyvien tilannekuva käytänteiden mukaisesti. Tilannekuvalla valittu tiedon visuaalinen esitysmuoto tukee näitä vaatimuksia koostaen vain merkityksellisimmät tiedot SWOT-analyysista ja prosessoiden ne mahdollisimman ymmärrettävään muotoon. Lisäksi koska kyseessä on strateginen tilannekuva organisaatiotasolle, niin kokonaiskuva merkitsee teknisiä nyansseja ja pikkutarkkoja lukuja enemmän. Horsmanheimo ym. (2017) korostivatkin erityisesti välttämään strategisessa tilannekuvassa liian teknisiä yksityiskohtia.

Tutkimustuloksissa ennen kaikkea luotu tilannekuva on hyvin yleisluontoinen ja kuvaa tilannetta ylätasolla. Kovinkaan yksityiskohtaisia strategista tilannekuvaa ei ole mahdollista tehdä ilman kohdeorganisaatiota ja siihen liittyvän oleellisen informaation kuten strategian, toimialan tai muun spesifin informaatioiden puutteen vuoksi. Nämä tiedot vaihtelevatkin nimenomaan organisaatiokontekstin mukaisesti lähtien siitä, että organisaatio tunnistaa oman toiminnan kannalta oleellisimmat tekijät. Organisaation olemassaolon tarkoitus tulisikin olla omanlaisensa kybertilannekuvan tuottamisen lähtökohtana. Yleisen strategisen tilannekuvan luominen on kuitenkin perusteltua tässä kontekstissa yleisen kybertoimintaympäristöä koskevan aineiston pohjalta ja ettei tutkimusta ollutkaan tarkoitus yhdelle kohdeorganisaatiolle toteuttaa. Konkreettiset esimerkit olisivat voineet lisätä tilannekuvan selkeyttä lisää, mutta niiden puute liittynee edellä mainittuihin huomioihin.

Vertaamalla muodostettua tilannekuvaa Evesti ym. (2017) määrittelemien tilannekuvan yksilöiviin ja muokkaaviin tekijöihin pystyttiin kaikki nämä tekijät ottamaan huomioon tutkimuksen tilannekuvan luonnissa. Laajuudeksi valikoitui organisaatiotaso, toimintatasoksi strateginen, näkökulmaksi taloudellinen ripauksella oikeudellista ja päätöksenteontasoksi manuaalinen inhimilliseen päätökseen nojaava. Toteutettua tilannekuvaa arvioimalla Knerlerin ym. (2022) kybertilannekuvan ja sen tietoisuuden saavuttamisen kolmen komponentin kautta voidaan myös todeta tilannekuvan muodostamisen onnistuneen SWOT:n pohjalta. Informaatio viittaa erilaisiin tietolähteisiin, joita voi olla muun muassa laite- ja järjestelmätoimittajien julkaisemat haavoittuvuustiedot (Knerler ym., 2022), tässä tapauksessa informaatiomme oli kyberturvallisuusorganisaatioiden julkaisemat uhkatietoraportit. Analytiikka tässä tapauksessa oli manuaalisesti tehty SWOT-analyysi, jonka avulla kerättyä tietoa tulkittiin ja jalostettiin. Viimeisenä vaiheena visualisoinnissa aiemmin kerätystä ja jalostetusta tiedosta koostettiin esitettävä kokonaisuus päätöksenteon tueksi eli strateginen tilannekuva.

Tuloksista tilannekuvan tuottamisen lisäksi tunnistettiin myös melko laajasti tekijöitä ja uhkia, joita kybertoimintaympäristöön kuuluu. Lisäksi onnistuttiin tunnistamaan yleisesti haasteita, jotka vaikuttavat organisaation kyberturvallisuuden toteuttamiseen strategisella tasolla ja uhkien minimoimisessa, joka viittaa vahvasti siihen, ettei aihetta voida tai pidä pitää itsestään selvänä. Jo aiemmin mainitut kyberuhat ilmenivät myös aineistossa ja todistavatkin kybertoimintaympäristön moninaiset uhkatyypit ovat vahvasti läsnä. Lehdon ym., (2017) kuvaukset kybertoimintaympäristön verkottuneesta luonteesta on myös hyvin paikkaansa pitäviä aineiston perusteella. Toimintaketjuhaavoittuvuudet ovat hyvä esimerkki tästä.

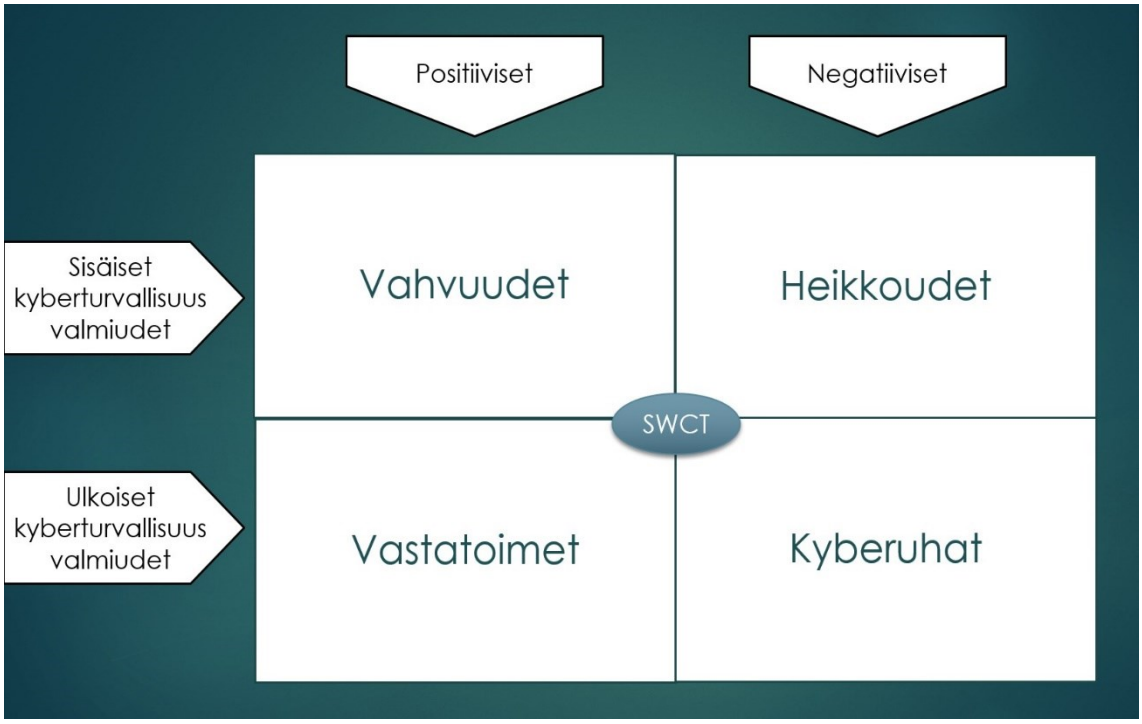
Voidaan tietenkin kyseenalaistaa SWOT:n tai uhkatietoraporttien käyttö tilannekuvan määrittelyssä, koska ne tarjoavat näkökulman menneeseen ja jo tapahtuneisiin ja havaittuihin asioihin. Muutosnopeassa ympäristössä nämä nopeasti saattavat jäädä jälkeen tai osoittautua vääriksi valinnoiksi. Toisaalta on hyvä ymmärtää tämän tutkielman toteutus- ja analysointitapojen noudattelevan enemmän proaktiivista lähestymistapaa kuin reaktiivista. Strateginen tilannekuva onkin hyvä ymmärtää pitkän ajan suuntaviittana ja eräänlaisena pohjana

tulevan arviointiin sekä yrityksenä ennakoida tulevia kehityssuuntia. Näiden pohdintojen perusteella onkin tärkeä nostaa ajallinen eriävyys ja tarpeet mahdollisessa strategisessa tilannekuvan arvioinnissa sekä reflektoinnissa tietyin väliajoin, että voidaan varmistua kehityssuunnasta ja tilannekuvaan nostettujen tekijöiden paikkansapitävyydestä.

6.1 Uusittu SWOT-kehys

Edellisessä luvussa koottu onnistunut tilannekuvan siis puoltaa SWOT:n hyödynnettävyyttä osana tilannekuvan koostamista ja jo taustakirjallisuudessa esiin nostetut asiat onnistuttiin tuomaan esille osana tilannekuvan luontia. Silti voidaan kyseenalaistaa SWOT:n onnistunut hyödyntäminen sellaisenaan osana tilannekuvaprosessia. Viitekehykseen sijoitetuista tiedoista erottaa selkeästi, että vahvuudet ja heikkoudet oli helppo tunnistaa ja sijoittaa. Uhat - osio sopi parhaiten kyberturvallisuuden arviointiin. Hankalinta oli sijoittaa löydettyjä tietoja raporteista mahdollisuudet - osioon. Mikään raporteissa esitetyistä tiedoista ei suoraan sopinut tähän kategoriaan. Muutenkin jos mietitään kybertoimintaympäristöä ja sen luonnetta, niin siellä olisi parempi puhua jopa vastatoimista kuin mahdollisuuksista. Kyseessä on kuitenkin muutosnopea, hektisiä tapahtumia ja kompleksisia järjestelmiä sisältävä toimintaympäristö (Lehto, 2021), jossa täytyisi kyetä vastaamaan uhkiin vastatoimilla. Kuten jo perusteltu niin SWOT:n perinteinen viitekehys ei täysin tehnyt oikeutta aineiston spesifille luonteelle. Toisaalta tarvitseeko sen täysin tehdäkään viitaten Picktonin ja Wrightin (1998) tutkimukseen, jossa he korostivat SWOT-analyysin osittaista sovellettavuutta kyvykkyyksien ja kehittämistarpeiden arvioinnissa ennemmin kuin koko totuuden määrittäjänä.

Näiden ja edellisissä luvuissa tehtyjen huomioiden pohjalta ehdottaisinkin SWOT-viitekehyksen muuttamista/editointia kyberturvallisuuden tilannekuvan tuottamisen tarpeisiin koostamalla seuraavanlaisen kuvio 7 mukaisen viitekehyksen:



Kuvio 7 SWCT - viitekehys

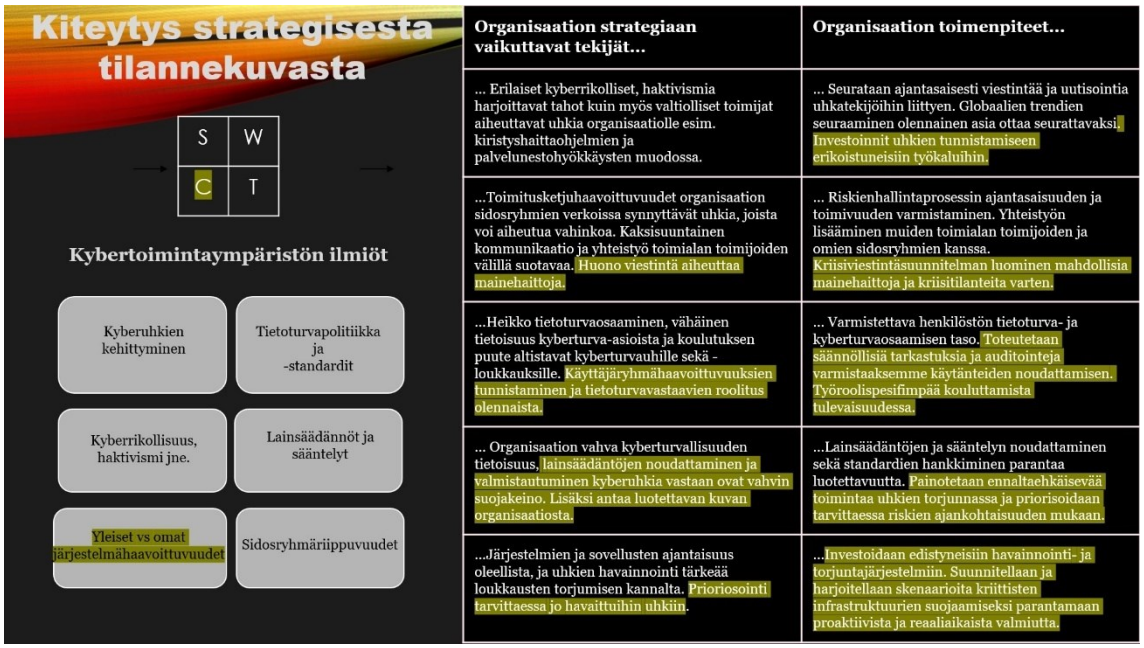
Alkuperäisen SWOT-viitekehyksen sisäisiin ja ulkoisiin osa-alueisiin jako on varsin toimiva tässäkin kontekstissa mielestäni, mutta sitäkin olisi mahdollista viilata hieman. Kybertoimintaympäristö on kuitenkin moniulotteinen ja verkostoitunut toimintaympäristö. Tässä ympäristössä valmius ja ennakointi ovat oleellisia asioita. Näiden pohjalta ehdottaisin päivittämään viitekehyksen sisältämään sisäiset kyberturvallisuusvalmiudet- ja ulkoiset kyberturvallisuusvalmiudet ulottuvuudet. Jolloin kyetään yhä sisäisten ja ulkoisten tekijöiden jakoon, mutta kyberturvallisuus ulottuvuus olisi nyt vahvemmin läsnä itse analyysissa ja korostettaisiin vahvemmin valmistautumista niin sisäisiin kuin ulkoisiin kehitystarpeisiin.

Vahvuudet ja **heikkoudet,** pysyisivät käytännössä muuttumattomina, liittyen yhä organisaation sisäisiin tekijöihin. SWCT-mallissa keskityttäisiin näiden osalta korostamaan ja analysoimaan erityisesti kyberturvallisuuden kannalta merkittäviä vahvuuksia ja heikkouksia. Esimerkiksi, vahvuuksia voisivat olla organisaation kyberturvallisuuskulttuuri ja laaja tietotekninen osaaminen. Heikkouksia taas voisivat olla puutteet kyberturvallisuuskoulutuksessa tai -infrastruktuurissa.

Suurimmat muutokset tulisivatkin ulkoisiin tekijöihin. Kokisin tarpeelliseksi korvata mahdollisuudet osa-alueen **vastatoimilla** (countermeasures), jota tulikin jo hieman aiemmin nostettua esille mahdollisena parannuksena. Tämä resonoisi paremmin kybertoimintaympäristön ja sen uhkien muutosnopeuden kanssa ja parantaisi organisaation resilienssikykyä. Mikäli ajattelemme kyberturvallisuutta kokonaisuutena ja osana toimintaympäristöä, mutta ennen kaikkea tilannekuvana, niin vastatoimet resonoivat paremmin organisaation vaateisiin.

Tässä tilanteessa ei nimittäin niinkään etsitä mahdollisuuksia vaan tapoja ja kohteita, joita vastaan suojautua eli millaisia vastatoimia toteuttaa oman liiketoimintansa suojaamiseksi ja ylläpitämiseksi. Vastatoimissa analysoitaisiin ja nostettaisiin esiin toimenpiteitä, joita organisaation tulisi toteuttaa vastatakseen ulkoisiin uhkiin ja jotka hyödyttävät organisaation turvallisuuttaa. Vastatoimet voisivat olla esimerkiksi uusien kyberturvallisuusteknologioiden käyttöönotto, henkilöstön kouluttaminen tai yhteistyö muiden organisaatioiden kanssa. **Uhat** osa-alueen osalta uudessa mallissa riittäisi kyberuhkien korostaminen. Uhkatyyppien tarkempi rajaaminen ja erityisesti oman organisaation kohtaamien kyberuhkien esiin nostaminen sekä analysointi

Muokkaamalla SWOT-viitekehystä sisältämään sisäiset kyberturvallisuusvalmiudet ja ulkoiset kyberturvallisuusvalmiudet ulottuvuudet, korvaten mahdollisuudet vastatoimilla ja spesifioimalla uhat kyberuhiksi ja – riskeiksi, pystytään paremmin vastamaan kybertoimintaympäristön piirteisiin. Nämä muokkaukset tukisivat mielestäni paremmin organisaatioiden strategisen tilannekuvan muodostamista kybertoimintaympäristöstä. Näin organisaation kyvyt seurata ja vastata jatkuvasti kehittyviin uhkiin paranisivat. Uudet muutokset viitekehyksessä, tukisivat näiden ympäristön uhkien ja ilmiöiden analysointia ja korostaen paremmin käsitystä, että ollaan jatkuvien uhkien ympäröimänä. Muutokset myös edesauttaisivat keskittymään enemmän konkreettisiin toimenpiteisiin ja sitä kautta tuottamaan paremmin kyseiselle organisaatiolle toimivia sekä kohdistettuja ratkaisuvaihtoehtoja. Edellisessä luvussa luotu tilannekuva muodostuisikin hieman erilaiseksi, kuten kuviosta 8 voidaan todeta, tämän uuden SWCT-viitekehyksen pohjalta:



Kuvio 8 SWCT-viitekehyksen pohjalta muokattu strateginen tilannekuva

Kuvioon 8 ja sitä kautta tilannekuvaan ei radikaaleja muutoksia tule, mutta muutoksen terävöittäisivät organisaation riskienhallintaprosessia ja valmistautumista yllättäviin uhkiin. Nykyisellä tilannekuvalla ei pysty vielä erityisen hyvää esimerkkiä tuottamaan vastatoimien hyödyistä, koska tarvittavat vastatoimet ovat aika vahvasti organisaatio riippuvaisia ja näitä on peilattava muihin ulkoisiin tekijöihin eli uhkiin. Kuvion pohjalta voi kuitenkin jo kevyitä johtopäätöksiä vetää. Vastatoimet tuovat strategiseen tilannekuvaan käytännönläheisemmän näkökulman, samalla korostaen suoria vastauksia havaittuihin heikkouksiin ja uhkiin. Muutosten myötä organisaation riskienhallintaprosessin pitäisi parantua, koska havaituilla vastatoimilla voidaan suoraan minimoida havaittuja uhkia. Ne tuovat myös enemmän reaaliaikaista valmiutta ja näkökulmaa organisaation kyberturvallisuuteen proaktiivisuuden tueksi.

Strategiselle tilannekuvalle ei ole määritelty kiinteää aikataulullista sykliä, jolloin tilannekuvaa tulisi tarkastella tai tuottaa uudestaan. Ajallinen eriävyys on kuitenkin oleellinen asia ottaa huomioon. Strateginen tilannekuva tulisi vähintään kerran vuodessa koostaa ja arvioida mieluusti uudelleen muutaman kerran vuodessa. Tämä voisi tapahtua esim. vuoden alussa koostamalla strateginen tilannekuva, joka toimii strategisena pohjana kyberturvallisuuden toimille kyseiselle vuodelle. Tämän jälkeen käydä tilannekuva uudelleen läpi puolenvuoden päästä ja reflektoida mikä on toiminut vai tarvitseeko jotain muokata loppuvuotta tai pitempää aikaa silmällä pitäen.

Strategista tilannekuvaa koostaessa tuli myös huomioita, ettei taustakirjallisuudessa tarjota mitään esimerkkipohjaa tilannekuvalle ja valmiit yleisesti hyödynnettävissä oleva tilannekuvapohjat loistavat poissaolollaan. Tähän varmasti liittyy erilaiset lähtökohdat ja tarpeet tuottaa tilannekuvia, mutta jonkinlainen yleinen esimerkkipohja, jota hyödyntää tilannekuvan koostamisessa voisi olla hyödyllinen. Tästä inspiroituneena kehittyikin ajatus seuraavanlaisesta strategisesta tilannekuvapohjasta:

Kuvio 9 Strategisen tilannekuvan yleinen mallipohja

Kuviossa 9 esitellyt teemat syntyivät erityisesti SWCT-analyysin ja sen tilannekuvan ideoinnin pohjalta ja perustuvatkin siellä esiintyneisiin teemoihin. Tämä tilannekuvapohja sisältääkin mielestäni oleellisimmat näkökulmat kyberturvallisuuden strategisen tilannekuvan esittämisen kannalta. Se on myös visuaalisesti selkeä ja paremmin ymmärrettävissä kuin vaikkapa aiemmin esitellyt tilannekuvat. Selkeytynyt visuaalinen ulkomuoto auttaisi tilanneymmärryksen muodostumisessa ja teemojen välinen yhteys tulee paremmin esille helpottaen näin pitkän aikavälin analysointia. Edellä mainitut nostot tukisivatkin tilannekuvapohjan yleistä hyödyntämistä organisaatiolle kuin organisaatiolle ja tarjoaisi selkeän tilannekuvakokonaisuuden yhdessä analyysityökalun, SWCT-viitekehyksen, kanssa kyberturvallisuudesta vastaaville henkilöille hyödynnettäväksi.

6.2 Jatkotutkimus

Tutkimuksen edetessä tunnistettiin muutamia mahdollisia jatkotutkimusaiheita, joista tärkeimpänä tietenkin uusitun SWOT-kehyksen testaaminen käytännössä. Jatkotutkimuksessa voitaisiin siis käytännössä suorittaa samantyylinen tutkimus kuin tämä, mutta analyysi tehtäisiin uusitun SWCT-viitekehyksen pohjalta jollekin organisaatiolle tai organisaatioille. SWCT-analyysin jäljiltä muodostettaisiin sitten strategisen tilannekuvan aiemmin mainittujen hyvien tilannekuvan koostamisen käytänteiden mukaisesti ja hyödyntäen tilannekuvan mallipohjaa, joka ideoitiin edellisessä alaluvussa. Jatkotutkimuksessa olisi suositeltavaa valita yksi tai muutama organisaatio toteutuksen kohteiksi. Tämä antaisi paremmat ja

käytännönläheisemmät tulokset uuden SWCT-viitekehyksen ja strategisen tilannekuvapohjan hyödynnettävyydestä oikeasti organisaatioiden tarpeisiin verrattuna tämän tutkimuksen yleisluontoisiin tuloksiin.

Tällaisen jatkotutkimuksesta voisi vielä laajentaa tai jatkaa soveltaen organisaation päätöksentekoa sekä päätöksentekijöitä tilannekuvan hyödyntämiseen. Tutkittaisiin tilannekuvan muodostamisen kautta saatujen tulosten hyödynnettävyyttä kyberturvallisuuden johtamisessa organisaatio- ja verkostotasolla ja osana päätöksentekoa. Lisäksi ajallinen eriävyys olisi hyvä jatkotutkimuksen osana olevana kohde. Strategiselle tilannekuvan tuottamiselle ei nimittäin ole vakiintunutta vuosikelloa tai julkaisusykliä. Tavallisesti strategiset päätökset ajoittuvat vuodenvaihteeseen ja niihin harvemmin palataan. Kybertoimintaympäristön muutosnopealuonne kuitenkin vaatii ehkä useamman tarkastelujakson myös strategiseen tilannekuvaan.

7 YHTEENVETO

Tässä tutkielmassa selvitettiin SWOT-analyysin hyödynnettävyyttä kyberturvallisuuden tilannekuvan tuottamisessa. Tutkielmassa keskityttiin strategisen tilannekuvan määrittämiseen kyberturvallisuusyritysten uhkatietoraporttien pohjalta SWOT-analyysia hyödyntäen. Keskiössä oli arvioida SWOT-viitekehyksen sopivuutta kyberturvallisuus spesifissä analysoinnissa ja ennen kaikkea vastata tutkimuskysymykseen: Voiko SWOT-analyysista rakentaa viitekehyksen strategisen tilannekuvan tuottamiseksi?

SWOT-analyysin pohjalta saadut tulokset indikoivat, että SWOT-viitekehystä voidaan hyödyntää osana strategisen tilannekuvan tuottamista, mutta se ei täydellisesti sovi tähän tarkoitukseen. Strateginen tilannekuva oli mahdollista muodostaa SWOT-analyysin pohjalta, mutta nykyinen rakenne varsinkin mahdollisuuksien osalta tuotti vaikeuksia havaintojen tekoon ilman tiedon soveltamista. Tuloksiin pohjautuvan ajatustyön johdosta tultiinkin johtopäätöksiin vaihtoehtoisen SWCT-viitekehyksen luomisesta vastaamaan paremmin kyberturvallisuuteen liittyvän strategisen tilannekuvan muodostamisprosessin tarpeisiin.

Tämä SWOT-viitekehyksestä muokattu versio erityisesti kyberturvallisuuden tarkoituksiin vastaa paremmin kybertoimintaympäristön erikoispiirteisiin kuten verkottuneeseen ja uhkatekijöitä pursuavaan luonteeseen perinteistä paremmin. Tärkeimpinä nostoina uudesta viitekehyksestä mahdollisuuksien korvaaminen vastatoimilla, uhkien tarkentamiselle kyberuhiksi ja sisäisten sekä ulkoisten tekijöiden muokkaus sisäisiin ja ulkoisiin kyberturvallisuusvalmiuksiin. Näillä muutoksilla koetaan organisaatio pystyvän paremmin vastamaan tarkasteltavan tilanteen havaitsemiseen, ymmärtämiseen ja sen vaikutuksien arviointiin organisaation tulevaisuuteen nähden.

SWCT-viitekehyksen lisäksi huomattiin myös tarve tai mahdollinen hyöty yleisestä strategisen tilannekuvan mallipohjasta kyberturvallisuuteen, joten sellainen syntyi tilannekuvapohdintojen yhteydessä. Tämän tilannekuvapohjan/mallin tarkoituksena on auttaa tilannekuvan laatijoita selkeyttämällä

visuaalista esitystä, mahdollistamalla konkreettisten esimerkkien noston ja korostaen paremmin pitkän ajan trendejä strategisesta näkökulmasta. Johtopäätöksinä syntyneet artefaktit myös puoltavat design research sciencen eli suunnittelututkimuksen onnistunutta hyödyntämistä tutkimusmetodina ja nostavat esiin tutkimusmenetelmän iteratiivisen luonteen.

SWCT-viitekehyksen ja strategisen tilannekuvapohjan hyödyntäminen käytännöntasolla jäi jatkotutkimuskohteeksi. Ylipäätänsä tutkimuksesta saadut tulokset ovat hyvin yleisluontoisia, mutta yleisluontoisuutensa ansiosta testattavissa useille eri organisaatiotyypeillä. Syvempi perehtyminen ja käytännön hyödynnettävyys erityyppisissä organisaatioissa onkin syytä jatkotutkimuksissa ajallisen eriävyyden ohella ottaa huomioon.

LÄHTEET

Accenture. (2021). *Threats unmasked: 2021 Cyber Threat Intelligence Report*. https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Blakemore, B., & Awan, I. (2012). *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*. Taylor & Francis Group. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=4512562

Brocke, J. vom, Hevner, A., & Maedche, A. (2020). *Introduction to Design Science Research* (ss. 1–13). https://doi.org/10.1007/978-3-030-46781-4_1

Cisco. (2022). *Security Report: Defending Against Critical Threats*. https://www.cisco.com/c/en/us/products/security/defending-against-critical-threats.html

CSIRT. (2023). *GOVCERT.LU*. https://www.govcert.lu/en/cyberweather/

Eldardiry, O. M., & Caldwell, B. S. (2015). Improving Information and Task Coordination in Cyber Security Operation Centers. *IIE Annual Conference. Proceedings*, 1224–1233.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

ENISA. (2023). *About ENISA - The European Union Agency for Cybersecurity* [About ENISA]. ENISA. https://www.enisa.europa.eu/about-enisa

Evesti, A., Kanstren, T., & Frantti, T. (2017). Cybersecurity situational awareness taxonomy. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. https://doi.org/10.1109/CyberSA.2017.8073386

Gregor, S., Chandra Kruse, L., & Seidel, S. (2020). The Anatomy of a Design Principle. *Journal of the Association for Information Systems*, *21*, 1622–1652. https://doi.org/10.17705/1jais.00649

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Horsmanheimo, S., Puuska, S., Vankka, J., Kuusela, P., Kokkoniemi-Tarkkanen, H., & Tuomimäki, L. (2017). *Kriittisen infrastruktuurin tilannetietoisuus*. Valtioneuvoston kanslia. https://vnk.fi/julkaisu?pubid=18702

Huoltovarmuuskeskus. (2022). *Kyberturvallisuuden työkalupakki yritysjohtajille—Huoltovarmuuskeskus*. https://www.huoltovarmuuskeskus.fi/a/kyberturvallisuuden-tyokalupakki-yritysjohtajille/

Huoltovarmuuskeskus. (2023). *Huoltovarmuuskeskus*. https://www.huoltovarmuuskeskus.fi/a/toimialojen-kybervarautuminen-hyvaa-perustasoa/

IBM. (2022). *X-Force Threat Intelligence Index 2022*. https://www.ibm.com/downloads/cas/ADLMYLAZ

INTERPOL. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. https://www.interpol.int/en/News-and-

Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing* (NIST SP 800-150; s. NIST SP 800-150). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150

Juhila, K. (2023). Laadullisen tutkimuksen ominaispiirteet. Teoksessa *Tietoarkisto*. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullisen-tutkimuksen-ominaispiirteet/

Knerler, K., Parker, I., & Zimmerman, C. (2022). *11 Strategies of a World-Class Cybersecurity Operations Center* (1. p., Vsk. 2022). The MITRE Corporation. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Kuusisto, T., Kuusisto, R., & Roehrig, W. (2015). *Situation Understanding for Operational art in Cyber Operations*. *2015*.

Kyberturvallisuuskeskus. (2023). *Palvelumme*. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme

Laari, T., Flyktman, J., Härmä, K., Timonen, J., & Tuovinen, J. (2019). Kyberkäsikirja Puolustusvoimien henkilöstölle. *Maanpuolustuskorkeakoulu, Sotataidon laitos*.

Lehto, M. (2017). Martti Lehto: Kyber on kaikkialla. *2017*.

Lehto, M. (2021). DIGITAALISEN KYBERMAAILMAN ILMIÖITÄ JA MÄÄRITTELYJÄ. *6.4.2021*, 139.

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal*, *30*(3). https://doi.org/10.1080/19393555.2020.1813851

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi*. Valtioneuvoston kanslia.

Madahar, B. K. & Parish, B. R. (2016). *Understanding Cyberspace Through Cyber Situational Awareness*. https://www.semanticscholar.org/paper/Understanding-Cyberspace-Through-Cyber-Situational-Madahar/bd92f82ed048eed23107176a8740fa713e117d3b#citing-papers

Microsoft. (2023). *Microsoft Threat Intelligence—A year of Russian hybrid warfare in Ukraine*. Microsoft Threat Intelligency. https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

Namugenyi, C., Nimmagadda, S. L., & Reiners, T. (2019). Design of a SWOT Analysis Model and its Evaluation in Diverse Digital Business Ecosystem Contexts. *Procedia Computer Science*, *159*, 1145–1154. https://doi.org/10.1016/j.procs.2019.09.283

Norri-Sederholm, T., Laitinen, T., Lehto, M., & Kari, M. J. (2019). Terveydenhuolto ja kyberuhkat. *Finnish Journal of eHealth and eWelfare*, *11*(1–2), 86–99. https://doi.org/10.23996/fjhw.74183

Nyarku, K., & Agyapong, G. (2011). Rediscovering SWOT Analysis: The Extended Version. *Academic Leadership: The Online Journal*, *9*(2). https://doi.org/10.58809/KIQL1002

Palo Alto Networks. (2023). *2023 Unit 42 Attack Surface Threat Report*. Palo Alto Networks. https://www.paloaltonetworks.com/resources/research/2023-unit-42-attack-surface-threat-report

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*, 45–77.

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Savola, R., Salonen, J., Savolainen, P., Suominen, A., Toivanen, H., Kyheröinen, H., & Remes, J. (2016). *Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen*. valtioneuvoston kanslia. https://julkaisut.valtioneuvosto.fi/handle/10024/79562

Pickton, D., & Wright, S. (1998). What's SWOT in strategic analysis? *Strategic Change*, *7*, 101–109. https://doi.org/10.1002/(SICI)1099-1697(199803/04)7:23.0.CO;2-6

Pöyhönen, J. (2018). SWOT-analyysin soveltaminen yrityksen kyberturvallisuuden tilannekuvan muodostamiseen: Cyber Trust/CIRP-raportti : tutkimusmenetelmän kuvaus 2017. *Informaatioteknologian tiedekunnan julkaisuja / Jyväskylän yliopisto*, *2018, 58*. https://jyx.jyu.fi/handle/123456789/70082

Pöyhönen, J., Rajamäki, J., Nuojua, V., & Lehto, M. (2021). Cyber Situational Awareness in Critical Infrastructure Organizations. Teoksessa T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Toim.), *Digital Transformation, Cyber Security and Resilience of Modern Societies* (Vsk. 84, ss. 161–178). Springer International Publishing. https://doi.org/10.1007/978-3-030-65722-2_10

Rapid7. (2022). *The Annual Vulnerability Intelligence Report: 2022 Edition*. https://www.rapid7.com/info/vulnerability-intelligence-report-2022-edition/

Sanastokeskus. (2023). *TEPA-termipankki (erikoisalojen sanastojen ja sanakirjojen kokoelma)*. https://termipankki.fi/tepa/fi/

Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Negodenko, O. (2021). *Information Security Risk Analysis SWOT*. Cybersecurity Providing in Information and Telecommunication Systems.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Turvallisuuskomitea. (2018, lokakuuta 3). *Kyberturvallisuuden sanasto – Turvallisuuskomitea*. https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Ulkoministeriö. (2022). *Ajankohtaisselonteko turvallisuusympäristön muutoksesta* [Sarjajulkaisu]. Valtioneuvosto. https://julkaisut.valtioneuvosto.fi/handle/10024/163999

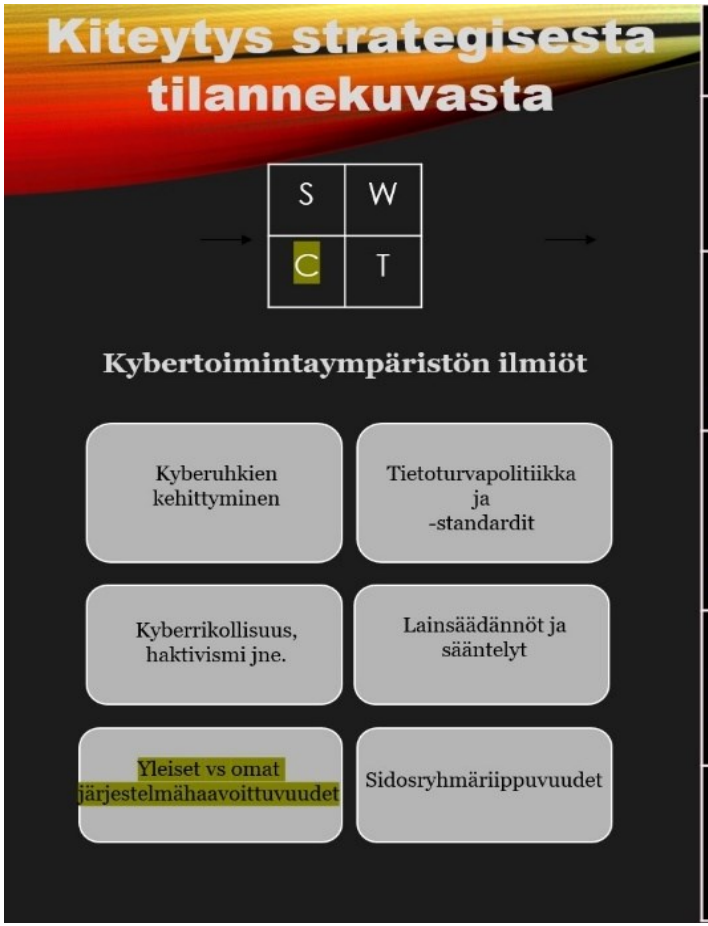
Ulkoministeriö. (2023). *Kyberturvallisuus ja kybertoimintaympäristö*. Ulkoministeriö. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

Vanek, M., Černý, I., Hudeček, V., Krčmarská, L., & Magnusková, J. (2014). *SWOT analysis – point of departure for strategic managers*. *3*, 591–598.

LIITE 1 STRATEGINEN TILANNEKUVA SWOT:N POHJALTA

Organisaation strategiaan vaikuttavat tekijät...	Organisaation toimenpiteet...
... Erilaiset kyberrikolliset, haktivismia harjoittavat tahot kuin myös valtiolliset toimijat aiheuttavat uhkia organisaatiolle esim. kiristyshaittaohjelmien ja palvelunestohyökkäysten muodossa.	... Seurataan ajantasaisesti viestintää ja uutisointia uhkatekijöihin liittyen. Globaalien trendien seuraaminen olennainen asia ottaa seurattavaksi.
...Toimitusketjuhaavoittuvuudet organisaation sidosryhmien verkoissa synnyttävät uhkia, joista voi aiheutua vahinkoa. Kaksisuuntainen kommunikaatio ja yhteistyö toimialan toimijoiden välillä suotavaa.	... Riskienhallintaprosessin ajantasaisuuden ja toimivuuden varmistaminen. Yhteistyön lisääminen muiden toimialan toimijoiden ja omien sidosryhmien kanssa haavoittuvuuksien minimoimiseksi.
... Heikko tietoturvaosaaminen, vähäinen tietoisuus kyberturva-asioista ja koulutuksen puute altistavat kyberturvauhille sekä -loukkauksille.	... Varmistettava henkilöstön tietoturva- ja kyberturvaosaamisen taso. Jatkuvat koulutukset ja tietoisuuden lisääminen parantaa valmiuksia toimia johdonmukaisesti sekä vaadittavalla tavalla tietoturvaloukkaustilanteissa.
... Organisaation vahva kyberturvallisuuden tietoisuus ja lainsäädäntöjen noudattaminen voi mahdollistaa kilpailuedun synnyn.	...Lainsäädäntöjen ja sääntelyn noudattaminen sekä standardien hankkiminen parantaa luotettavuutta luoden perustaa kilpailuedun synnylle.
...Järjestelmien ja sovellusten ajantaisuus oleellista, ja uhkien havainnointi tärkeää loukkausten torjumisen kannalta	...Havainnointijärjestelmien (SIEM ja/tai SOC), sekä käyttäjä- ja identifikaatioiden hallintajärjestelmien hyödyntäminen parantamaan proaktiivista ja reaaliaikaista valmiutta.

LIITE 2 STRATEGINEN TILANNEKUVA SWCT:N POHJALTA



Organisaation strategiaan vaikuttavat tekijät...	Organisaation toimenpiteet...
... Erilaiset kyberrikolliset, haktivismia harjoittavat tahot kuin myös valtiolliset toimijat aiheuttavat uhkia organisaatiolle esim. kiristyshaittaohjelmien ja palvelunestohyökkäysten muodossa.	... Seurataan ajantasaisesti viestintää ja uutisointia uhkatekijöihin liittyen. Globaalien trendien seuraaminen olennainen asia ottaa seurattavaksi. Investoinnit uhkien tunnistamiseen erikoistuneisiin työkaluihin.
...Toimitusketjuhaavoittuvuudet organisaation sidosryhmien verkoissa synnyttävät uhkia, joista voi aiheutua vahinkoa. Kaksisuuntainen kommunikaatio ja yhteistyö toimialan toimijoiden välillä suotavaa. Huono viestintä aiheuttaa mainehaittoja.	... Riskienhallintaprosessin ajantasaisuuden ja toimivuuden varmistaminen. Yhteistyön lisääminen muiden toimialan toimijoiden ja omien sidosryhmien kanssa. Kriisiviestintäsuunnitelman luominen mahdollisia mainehaittoja ja kriisitilanteita varten.
...Heikko tietoturvaosaaminen, vähäinen tietoisuus kyberturva-asioista ja koulutuksen puute altistavat kyberturvauhille sekä -loukkauksille. Käyttäjäryhmähaavoittuvuuksien tunnistaminen ja tietoturvavastaavien roolitus olennaista.	... Varmistettava henkilöstön tietoturva- ja kyberturvaosaamisen taso. Toteutetaan säännöllisiä tarkastuksia ja auditointeja varmistaaksemme käytänteiden noudattamisen. Työroolispesifimpää kouluttamista tulevaisuudessa.
... Organisaation vahva kyberturvallisuuden tietoisuus, lainsäädäntöjen noudattaminen ja valmistautuminen kyberuhkia vastaan ovat vahvin suojakeino. Lisäksi antaa luotettavan kuvan organisaatiosta.	...Lainsäädäntöjen ja sääntelyn noudattaminen sekä standardien hankkiminen parantaa luotettavuutta. Painotetaan ennaltaehkäisevää toimintaa uhkien torjunnassa ja priorisoidaan tarvittaessa riskien ajankohtaisuuden mukaan.
...Järjestelmien ja sovellusten ajantaisuus oleellista, ja uhkien havainnointi tärkeää loukkausten torjumisen kannalta. Priorisointi tarvittaessa jo havaittuihin uhkiin.	...Investoidaan edistyneisiin havainnointi- ja torjuntajärjestelmiin. Suunnitellaan ja harjoitellaan skenaarioita kriittisten infrastruktuurien suojaamiseksi parantamaan proaktiivista ja reaaliaikaista valmiutta.

LIITE 3 STRATEGISEN TILANNEKUVAN MALLIPOHJA