Informaatioteknologian tiedekunnan julkaisuja
No. 58/2018

Jouni Pöyhönen

SWOT-analyysin soveltaminen yrityksen kyberturvallisuuden tilannekuvan muodostamiseen

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 58/2018

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7547-0 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2018

SWOT-analyysin soveltaminen yrityksen kyberturvallisuuden tilannekuvan muodostamiseen

Application of the SWOT analysis for forming situational awareness in company's cyber security

Jyväskylän yliopisto
Informaatioteknologian tiedekunta

Cyber Trust/CIRP-raportti
Tutkimusmenetelmän kuvaus
2.painos
2017

Jouni Pöyhönen

JYVÄSKYLÄN YLIOPISTO

TIIVISTELMÄ

Modernin yhteiskunnan toiminta perustuu useiden kriittisten infrastruktuurien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän luottamuksesta infrastruktuuriin kuuluvien organisaatioiden toimintakykyyn kybertoimintaympäristössä, jonka riskejä digitaalisen maailman uhkakuvat jatkuvasti kasvattavat.

SWOT-analyysi on tärkeä väline analysoitaessa organisaation toimintakykyä ja sen toimintaympäristöä kokonaisuutena. Se on nelikenttämenetelmä, jota käytetään yleisesti tilannekuvan muodostamiseen laadittaessa yrityksen strategioita, sekä oppimisen tai ongelmien tunnistamisessa, arvioinnissa ja toimintaprosessien kehittämisessä. SWOT-analyysin kohteena voi olla jonkin yrityksen toiminto, organisaatio koko laajuudessaan tai jonkin tuotteen tai palvelun asema ja kilpailukyky tai esimerkiksi kilpailijan toiminta ja kilpailukyky.

SWOT-analyysin pohjalta voidaan tehdä päätelmiä, miten vahvuuksia voidaan käyttää hyväksi, miten heikkoudet muutetaan vahvuuksiksi, miten tulevaisuuden mahdollisuuksia hyödynnetään ja miten uhat vältetään. Tuloksena saadaan toimintasuunnitelma tarkastelukohteesta. Tämä raportti käsittelee SWOT-analyysin soveltamista organisaation yleisen kybertilannekuvan muodostamiseksi.

Artikkelin keskeinen anti on kansallisen kyberturvallisuutta käsitelleen tutkimushakkeen julkisen sektorin tutkimiseen sovelletun SWOT-analyysimenetelmän kokemusten hyödyntäminen yksittäisen organisaation kyberturvallisuuden tilannekuvan muodostamisessa. SWOT-analyysin avulla voidaan tukea johtamista ja kehitystoimenpiteiden valintaa kehitettäessä kohteen toimintaprosesseja ja siten koko organisaation kyberturvallisuutta.

Toimenpiteiden jalkauttaminen edellyttää, että organisaation johto pitää kyberturvallisuuteen liittyviä luottamusta lisääviä toimenpiteitä yrityksen strategisena tavoitteena, pitää yllä suorituskykyisiä prosesseja ja viestittää niiden toteuttamista strategiaa tukevalla toimintapolitiikalla.

Asiasanat: kriittinen infrastruktuuri, kyberturvallisuuden johtaminen, luottamus, SWOT

TAULUKOT

KUVIOT

Sisällysluettelo

1. Johdanto

Modernin yhteiskunnan toiminta perustuu useiden kriittisten infrastruktuurien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu lähtökohdiltaan luotettavasta kansallisesta sähkövoimajärjestelmästä. Tämän lisäksi luotettavuus muodostuu organisaatioiden välisistä toimivista tiedonsiirtoverkostoista sekä palvelutason yritysten järjestelmien tiedon käytettävyydestä, luotettavuudesta ja eheydestä kybertoimintaympäristössä, jonka turvallisuusriskejä digitaalisen maailman uhkakuvat jatkuvasti kasvattavat.

Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä, ja yhteiskuntamme elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa. Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Tästä keskinäisriippuvaisesta ja moninaisesta sähköisessä muodossa olevan tiedon käsittelyyn tarkoitetusta ympäristöstä on kansainvälisesti ryhdytty käyttämään termiä kybertoimintaympäristö. Yhteiskunnan lisääntynyt tietointensiivisyys, ulkomaisen omistuksen kasvu ja toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen integraatio, kaikille avointen tietoverkkojen käyttö sekä lisääntynyt riippuvuus sähköstä ovat asettaneet uudenlaisia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvaamiseksi normaalioloissa, normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa. (Turvallisuuskomitean sihteeristö, 2013, 1 - 2.)

Kybertoimintaympäristö on huomioitava uhkien lisäksi myös mahdollisuutena ja voimavarana. Turvallinen toimintaympäristö helpottaa yksilöiden ja yritysten oman toiminnan suunnittelua. Se lisää yhteiskunnan taloudellista aktiviteettia ja mahdollistaa turvallisesti toimivalle yritykselle suhteellisen kilpailuedun aikaansaamisen. Hyvä toimintaympäristö parantaa myös Suomen kansainvälistä houkuttelevuutta investointikohteena.

Kansallista kyberturvallisuutta on kehitetty kymmenkohtaisen strategisten linjausten ohjelman mukaisesti (Turvallisuuskomitean sihteeristö, 2013, 7 - 11). Linjauksien kohta kolme koskettaa suoraan yritystoimintaa. Siinä todetaan, että toimenpiteillä ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta merkittävien yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet. Lisäksi ylläpidetään kykyä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa. Yritykset ja organisaatiot ottavat turvallisuus- ja valmiussuunnittelussaan sekä niihin liittyvissä palvelurakenteissa kattavasti huomioon yhteiskunnan elintärkeisiin toimintoihin liittyvät kyberuhkatekijät. Ne ylläpitävät tarvittavaa suojautumiskykyä tavoitteena riskiarvioiden mukaisten häiriöiden tunnistamisen ja havaitsemisen ja häiriöiden haitallisten vaikutusten minimoinnin. Keskeiset toimijat kehittävät sietokykyään muun muassa varamenetelmien suunnittelulla ja harjoittelulla.

Huoltovarmuusorganisaatio puolestaan tukee toimintaa selvityksillä, ohjeistuksilla ja koulutuksella.

Strategiassa määritellään myös keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus. Strategiaan liittyy myös toimeenpano-ohjelma, jossa on yhteensä 74 erillistä toimenpidettä tavoitteiden saavuttamiseksi (Turvallisuuskomitean sihteeristö, 2013, 1).

Kyberturvallisuusstrategian linjausten ja niiden toteuttamiseksi tarvittavien toimenpiteiden avulla pyritään kansallisesti hallitsemaan kybertoimintaympäristön tahallisia tai tahattomia haittavaikutuksia sekä vastaamaan niihin ja toipumaan niistä. Tavoitteisiin pääseminen edellyttää niin sanottua jatkuvan parantamisen toimintamallin aikaansaamista toimintaympäristöä hyödyntävien organisaatioiden osalta.

Syksyn 2016 aikana toteutetulla Suomen kyberturvallisuuden nykytilaa käsittelevällä valtioneuvoston kanslian tutkimushankkeella selvitettiin Suomen kyberturvallisuuden nykytilaa tavoitteisiin peilaten sekä kartoitettiin jatkotoimenpiteitä tavoitetilan saavuttamiseksi. Tutkimushankkeen tavoitteista tutkimussuunnitelmassa on todettu seuraavaa:

- Hankkeen tavoitteena on selvittää kokonaisvaltaisesti, kuinka vuoden 2013 kyberturvallisuusstrategiassa asetettu tavoite ”Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa” on saavutettu ja millainen Suomen kyberturvallisuuden tavoitetilan tulisi olla vuonna 2020?
- Hankkeen osatavoitteita ovat:
  - Kyberturvallisuustilanneanalyysin laatiminen.
  - Suomen kyberturvallisuustilanne ja strategian toimeenpanon toteutuminen julkisella ja yksityisellä sektorilla.
  - Kansainvälinen kyberturvallisuuden esikuva-analyysi ja Suomen vertautuminen verrokkimaihin.
  - Suomen kyberturvallisuuden tavoitetila vuonna 2020 ja tarvittavat linjaukset.

Tutkimushankkeen yksi työpaketti koski yksityisen sektorin tutkimusta. Työpaketin tavoitteena oli tuottaa tilannekuva kansallisesta kybersuorituskyvystä yksityisellä sektorilla sekä kuva siitä, kuinka kyberturvallisuusstrategian tavoitteet ovat toteutuneet. (Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen, 2017, 8.)

Tämä artikkeli käsittelee työpaketin tutkimusmenetelmänä käytetyn SWOT-analyysin soveltamista tutkimusympäristöön, jossa kohteesta pyritään muodostamaan kokonaisvaltainen kyberturvallisuuden tilannekuva. Artikkelin tavoitteena on edellä mainitusta tutkimushankkeesta saatuja kokemuksia hyödyntäen helpottaa vastaavien tilannekuva-analyysien toteuttamista yksittäisessä organisaatiossa sen kyberturvallisuuden

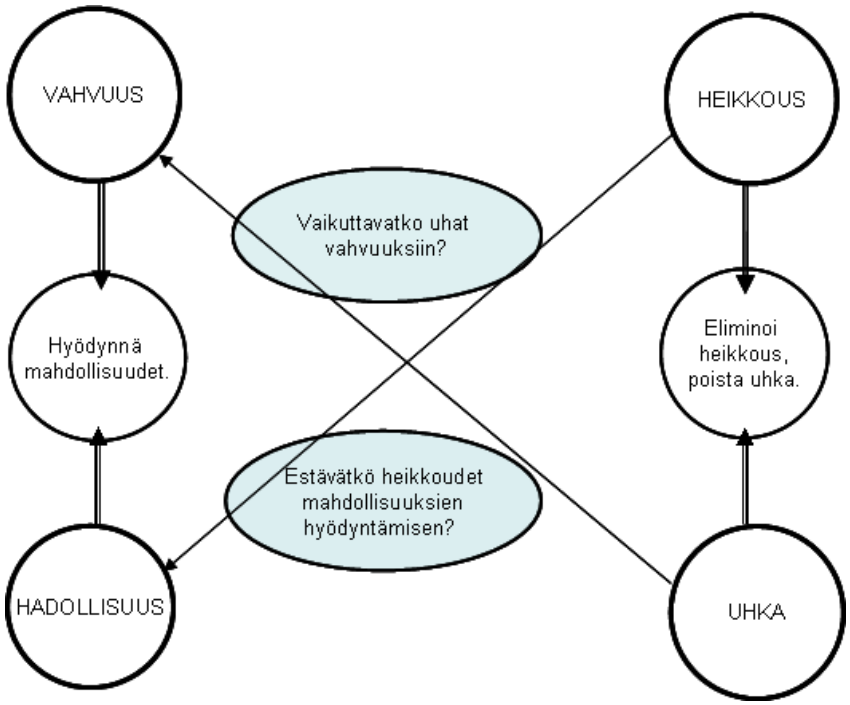
johtamiseen liittyvien tekijöiden määrittämiseksi ja niiden huomioimiseksi yrityksen toimintaprosessien rakenteissa jatkuvan parantamisen toimintamallia hyödyntämällä.

2. SWOT-analyysi

SWOT-lyhenne koostuu englannin kielisistä sanoista Strengths (vahvuudet), Weaknesses (heikkoudet), Opportunities (mahdollisuudet) ja Threats (uhat). SWOT-analyysi on tärkeä väline analysoitaessa organisaation toimintakykyä ja sen toimintaympäristöä kokonaisuutena. Se on nelikenttämenetelmä. Sitä käytetään yleensä yrityksen strategian laatimisessa, sekä oppimisen tai ongelmien tunnistamisessa, arvioinnissa ja toimintaprosessien kehittämisessä. SWOT-analyysin kohteena voi olla muun muassa yrityksen toiminto, organisaatio koko laajuudessaan tai tuotteen tai palvelun asema ja kilpailukyky tai kilpailijan toiminta ja kilpailukyky. (Nyarku & Agyapong, 2011, 1 - 2.)

SWOT-analyysi on kahden ulottuvuuden kuvaama nelikenttä. Kaavion vasempaan puoliskoon kuvataan myönteiset ja oikeaan puoliskoon negatiiviset asiat. Kaavion yläpuoliskoon kuvataan organisaation sisäiset asiat ja alapuoliskoon ulkoiset asiat. Tämän jälkeen SWOT-analyysin pohjalta voidaan tehdä päätelmiä, miten vahvuuksia voidaan käyttää hyväksi, miten heikkoudet muutetaan vahvuuksiksi, miten tulevaisuuden mahdollisuuksia hyödynnetään ja miten uhat vältetään. Tuloksena saadaan toimintasuunnitelma siitä, mitä millekin asialle pitää tehdä. (Melkman & Simmonds, 2016, 132 - 133.)

Kuviossa 1 on esitetty edellä kuvatut nelikenttäanalyysin eri osien riippuvuussuhteet.



KUVIO 1. Nelikenttäanalyysin eri osien riippuvuussuhteet
(Melkman & Simmonds, 2016, 133)

3. SWOT-analyysi teemahaastatteluna

SWOT-analyysi on laadullinen eli kvalitatiivinen tutkimus, jossa yritetään ymmärtää tutkittavaa ilmiötä. Eräs sovellus SWOT-analyysistä on tilannekuvan muodostaminen tutkimuskohteesta, jonka avulla voidaan kuvata siinä esiintyviä ilmiöitä. Ilmiöiden merkityksen tai tarkoituksen selvittämisen avulla puolestaan saadaan muodostettua kokonaisvaltainen ja syvällinen käsitys kohteesta. Teemahaastattelu on keskustelunomainen haastattelumenetelmä, jota voidaan pitää yhtenä laadullisen tutkimuksen aineiston hankinnan tapana. Teemahaastattelu on puolistrukturoitu haastattelu, koska se on rakenteeltaan avointa haastattelua ennalta tarkemmin määritelty, mutta väljempi kuin strukturoitu haastattelu.

Saaranen-Kauppinen ja Puusniekka (2006) ovat verkkodokumentissaan ”Menetelmäopetuksen tietovaranto” luonnehtineet teemahaastattelua ja sen käyttömahdollisuuksia muun muassa seuraavasti:

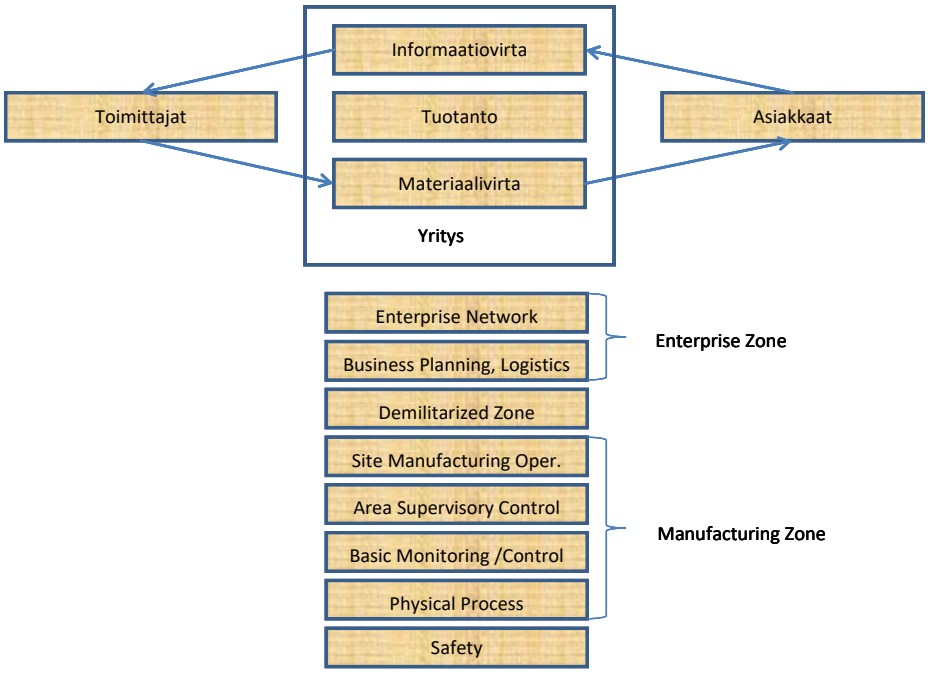
- Teemahaastattelu sijoittuu formaaliudessaan lomakehaastattelun ja avoimen haastattelun väliin. Haastattelu ei etene tarkkojen, yksityiskohtaisten, valmiiksi muotoiltujen kysymysten kautta vaan väljemmin kohdentuen tiettyihin ennalta suunniteltuihin teemoihin. Teemahaastattelussa pyritään huomioimaan ihmisten tulkinnat ja heidän merkityksenantonsa. Ihmisten vapaalle puheelle annetaan tilaa, vaikka ennalta päätetyt teemat pyritään keskustelemaan kaikkien tutkittavien kanssa.
- Teemahaastattelu on keskustelunomainen tilanne, jossa käydään läpi ennalta suunniteltuja teemoja. Teemojen puhumisjärjestys on vapaa, eikä kaikkien haastateltavien kanssa välttämättä puhuta kaikista asioista samassa laajuudessa. Tutkijalla on haastattelussa mukanaan mahdollisimman lyhyet muistiinpanot käsiteltävistä teemoista, jotta hän voisi keskittyä keskusteluun, ei papereiden tavaamiseen. Teemat voi listata esimerkiksi ranskalaisin viivoin ja lisäksi voi laatia joitakin apukysymyksiä tai avainsanoja keskustelun ruokkimista varten. Teemahaastattelun ei siis tulisi olla pikkutarkkojen kysymysten esittämistä tarkassa järjestyksessä paperilta lukien. Teemoista ja niiden alateemoista pyritään keskustelemaan varsin vapaasti. Teemahaastattelu on sopiva haastattelumuoto esimerkiksi silloin, kun halutaan tietoa vähemmän tunnetuista ilmiöistä ja asioista (vrt. puolistrukturoitu ja strukturoitu haastattelu).

- Teemahaastattelu edellyttää huolellista aihepiiriin perehtymistä ja haastateltavien tilanteen tuntemista, jotta haastattelu voidaan kohdentaa juuri tiettyihin teemoihin. Sisältö- ja tilanneanalyysi on siis teemahaastattelussa tärkeää. Käsiteltävät teemat valitaan tutkittavaan aiheeseen perehtymisen pohjalta. Tutkimusaihe ja tutkimuskysymykset on muutettava tutkittavaan muotoon, eli operationalisoitava. Kysymysten harkitsemisen lisäksi myös haastateltavien valitsemiseen tulee suhtautua harkinnalla: Tutkimukseen osallistuvia ei tulisi valita satunnaisesti tarraten kehen tahansa kulkijaan. Tutkittaviksi tulee valita sellaisia ihmisiä, joilta arvellaan parhaiten saatavan aineistoa kiinnostuksen kohteena olevista asioista.
- Teemahaastattelun suosio perustuu esimerkiksi siihen, että vastaamisen vapaus antaa oikeuden haastateltavien puheelle. Lisäksi teemoihin kohdistunutta haastattelua on suhteellisen helppoa ryhtyä analysoimaan teemoittain. Tutkijan ennakkoon asettamat teemat eivät välttämättä ole samat kuin teemat, jotka aineistoa analysoimalla osoittautuvat olennaisesti aineiston sisältöä ja tutkimusaihetta jäsentäviksi. Aineiston teemoittelusta voi edetä tyypittelyyn. Teemahaastatteluaineistoa voidaan analysoida myös vaikkapa kokonaan kvantitatiivisesti tai kvantitatiivisuutta ja kvalitatiivisuutta yhdistellen. Kielelliset tarkastelutavat ovat myös tutkimusongelmasta riippuen mahdollisia. Teemahaastattelua ei siis tarvitse analysoida juuri tietyllä tavalla, vaikka teemoittelu ja tyypittely onkin tavallista ja looginen jatkumo kyseiselle haastattelutyypille.

4. Yrityksen kybertoimintaympäristö ja sen tilannekuva

Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja. (Turvallisuuskomitean sihteeristö, 2013, 12.)

Tämä artikkeli kuvaa tyypillisen kriittisen infrastruktuuriin lukeutuvan yrityksen yleistä tilannekuvan muodostamista SWOT-analyysiä hyödyntäen. Kriittinen infrastruktuuri pitää sisällään yrityksiä, joiden toiminnan taso muodostaa lopulta koko infrastruktuurin suorituskyvyn. Siksi on tärkeää, että jokainen siinä toimiva yritys pitää tärkeänä tietojärjestelmiensä ja tietojärjestelmävarantojensa tilannekuvan aikaansaamista. Kuviossa 2 on esitelty yrityksen, jolla on yritystason IT-järjestelmiä, tuotantotoimintaa ja toimintaverkostoja kybertoimintaympäristön rakenne järjestelmätasolla.



KUVIO 2. Yrityksen kybertoimintaympäristön rakenne järjestelmätasolla
(Bowersox, Closs, Jessop & Jones, 1986, 16; Knowles, Prince, Hutchison, Ferdinand, Disso & Jones, 2015, 53)

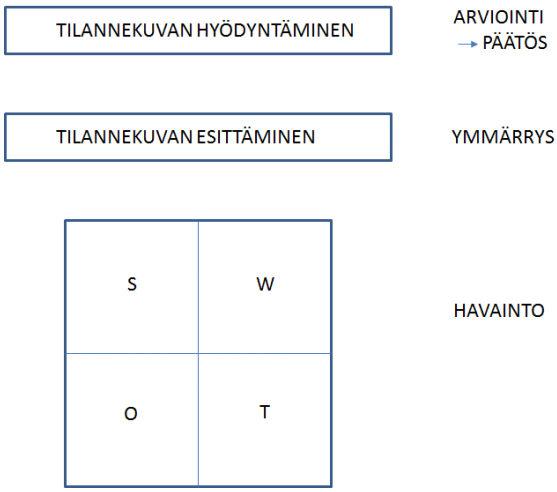
Kuvioon on yhdistetty yrityksen tyypillinen logistinen viitekehys, joka pitää sisällään yrityksen omien logististen toimintojen lisäksi toimittaja- ja asiakasverkostot sekä yrityksen tietojärjestelmät. Logististen toimintojen tavoitteena on hallita yrityksen oman tuotannon ohella sen toimintaan liittyviä materiaali- ja tietovirtoja mahdollisimman hyvän liiketoiminnan aikaansaamiseksi. Se tapahtuu tietojärjestelmiä hyödyntämällä. Kokonaisuudesta muodostuu yrityksen kybertoimintaympäristö.

Kyberympäristö koostuu yritystason ja tuotantotason tieto- ja automaatiojärjestelmistä. Ylimmällä tasolla hierarkiassa ovat yrityskohtaiset toimistojärjestelmät, toiminnanohjausjärjestelmä (Enterprise Resource Planning, ERP) ja internetin käytön mahdollistavat järjestelmät tiedonsiirtoverkkoineen. Seuraavalla tasolla ovat tuotannonohjausjärjestelmä (Manufacturing Execution System, MES) ja tuotantoprosessin ohjaukseen tarvittava teollisuuden automaatiojärjestelmä (Industrial Control System, ICS). Edellä mainitut järjestelmät eroavat toisistaan erityisesti rakenteeltaan, toiminnaltaan ja elinkaariltaan huomattavasti, joten niiden vaikutukset kybertoimintaympäristöön yrityskohtaiseen kehittymiseen ovat erilaiset ja vaativat siten kyberturvallisuuden näkökulmasta katsottuna kukin erillistarkastelun. Esimerkiksi ERP-järjestelmä voi olla laajasti koko logistisen toimintaverkoston käytössä, kun taas osa järjestelmistä palvelee paikallista tarvetta. Yritykset ovat myös voineet ulkoistaa ainakin osan IT-palveluistaan. Ulkoistukset lisäävät yrityksen toimintaverkoston rakennetta verrattuna perinteiseen logistiseen toimintaverkostoon. Kokonaisvaltaisen kyberturvallisuutta koskevan tilannekuvan aikaansaaminen edellyttää koko kybertoimintaympäristön analysointia.

Endsley (1995, 34 - 36) on kehittänyt tilannetietoisuuden mallia työskennellessään useissa eri tutkimustehtävissä Yhdysvaltojen ilmavoimien palveluksessa. Hänen mukaansa tilannetietoisuuden ydin koostuu kolmesta peruselementistä, jotka ovat havaitseminen (Level 1), tilanteen ymmärtäminen (Level 2) ja sen vaikutuksen arviointi tulevaisuuteen nähden (Level 3). Näin muodostettava tilannekuva antaa perusteet johtopäätöksiin ja niistä seuraavaan päätöksentekoon. Siihen vaikuttavat myös tilanteesta riippuen tehtävä- tai järjestelmäkohtaiset ominaisuudet sekä päätöksentekijän kokemukset ja arviointikyky. Päätöksenteko puolestaan ohjaa toimintaa, joka heijastuu takaisin havainnoitavaan toimintaympäristöön.

Endsleyn kehittämän tilannetietoisuuden mallin yleistä rakennetta voidaan soveltaa usea eri tason tilannekuvan muodostamiseen ja sen hyödyntämiseen. Yrityksen myös yleisen kyberturvallisuuden tilannekuvan muodostamisessa ja hyödyntämisessä sen periaatteet ohjaavat prosessin systemaattista etenemistä. Kuviossa 3 on esitetty SWOT-analyysin perustuva yrityksen yleinen tilannekuvaprosessi. Siinä ensiksi kohdistetaan yrityksen kyberympäristöön yrityskohtaisten vahvuuksien ja heikkouksien analysointi ja toisaalta arvioidaan toimintaympäristön antamia mahdollisuuksia sekä uhkia. Niistä muodostuvat havainnot. Havainnot esitetään tilannekuvana, joista voidaan muodostaan ymmärrys

nelikentän riippuvuussuhteiden mukaisesti. Tällöin kyseeseen tulevat arviot vahvuuksien kehittämisestä ja mahdollisuuksien hyödyntämisestä sekä sellaisten heikkouksen poistamisesta, jotka mahdollisesti tunnistettujen uhkien osalta aiheuttavat organisaatiossa haavoittuvuutta. Lisäksi tässä yhteydessä voidaan arvioida voivatko tunnistetut uhkat vaikuttaa haitallisesti voimavarana pidettyihin vahvuuksiin, tai toisaalta voivatko heikkoudet jopa estää mahdollisuuksien hyödyntämisen. Tilannekuvan lopullinen hyödyntäminen tapahtuu päätösprosessissa, joka parhaiten onnistuessaan johtaa toimenpiteisiin päätöksenteon kaikilla tasoilla; strategisella tasolla, operatiivisella tasolla ja taktisella tasolla. (Endsley, 1995, 34 - 36.)



KUVIO 3. SWOT-analyysi osana yrityksen kyberturvallisuuden tilannekuvan muodostamista

5. SWOT-analyysin soveltaminen yrityksen kybertoimintaympäristöön

SWOT-analyysin jaottelu sisäisiin ja ulkoisiin tekijöihin voidaan toteuttaa kybertoimintaympäristössä esimerkiksi seuraavasti:

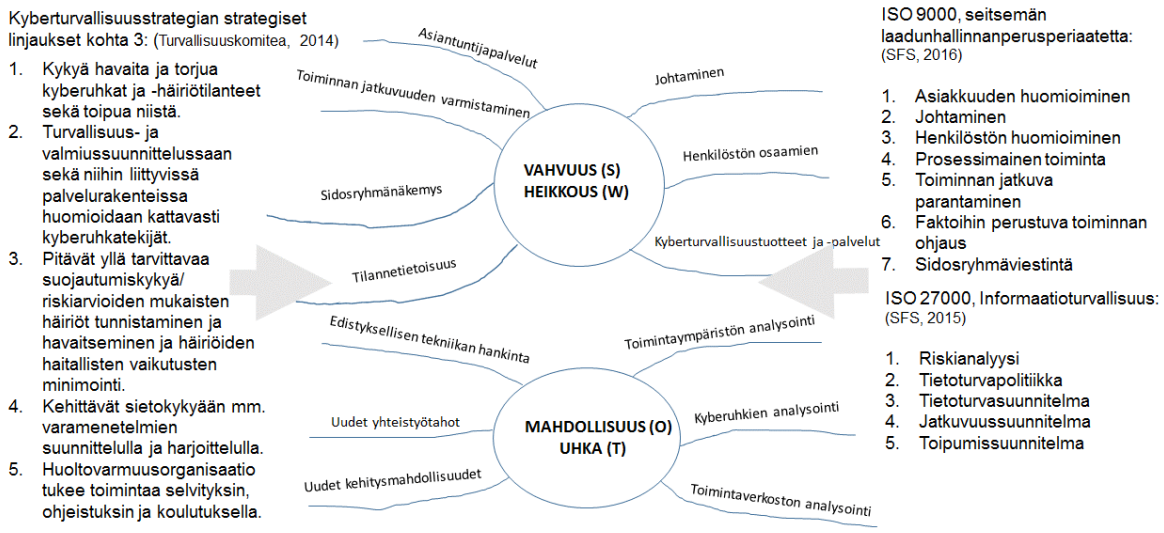
- Vahvuudet ja heikkoudet ovat sisäisiä tekijöitä. Organisaation vahvuus voi olla esimerkiksi hyvät toimintaedellytykset kybertoimintaympäristössä ja maine luotettavana toimijana toimintaympäristön haasteista huolimatta. Heikkous puolestaan voi olla organisaation kyvyttömyys tunnistaa toimintaansa osana yrityksen verkottunutta toimintaympäristöä tai puutteet toiminnan varmistamisessa toimintaympäristön asettamissa vaatimuksissa.

- Mahdollisuudet ja uhat ovat ulkoisia tekijöitä. Mahdollisuus voi olla esimerkiksi yrityksen vaikutusmahdollisuus kyberluottamusta lisääviin toimenpiteisiin ulkopuolisia resursseja hyväksi käyttäen. Uhka voi puolestaan muodostua siitä, että yritys ei tunnista toimintaympäristönsä kyberturvallisuuden haasteita ja yrityksen ulkopuolelta uhkaavia tietomurtoja.

Kattava yrityksen kyberturvallisuuden analysointi toteutuu parhaiten siten, että tarkastelun näkökulmat ulotetaan organisaation strategiaan, operatiivisiin toimiin ja teknis-taktisen tason ratkaisuihin.

Viitteenä olevan tutkimuksen SWOT-analyysin teemat on johdettu Suomen kyberturvallisstrategian strategisten linjausten kohdan 3 yritystoimintaa käsittelevästä kokonaisuudesta. Lisäksi teemojen laadinnassa on hyödynnetty ISO 9000-laatustandardin seitsemää perusperiaatetta ja ISO 27000-informaatioturvallisuuden standardin keskeisimpiä pääkohtia. Kuviossa 4 on esitetty teemoja johtamisen lähtökohtiin ja teemat SWOT-analyysin pääkohtiin liittyen.

Teemat on yleistetty otsikkotasolle niin, että niitä voidaan soveltaa minkä tahansa organisaation tilannekuvan kartoitukseen. Teemojen organisaatiokohtaisia haastattelukysymyksiä voidaan johtaa tunnistetuista lähtötiedoista.



KUVIO 4. Viitetutkimuksen SWOT-analyysin haastattelun teemat (Lehto ym., 2017, 42)

Yrityksen vahvuuksia ja heikkouksia arvioitaessa haastatteluteemat olivat:

- Johtaminen
- Henkilöstön osaaminen
- Kyberturvallisuustuotteet ja –palvelut
- Tilannetietoisuus
- Sidosryhmänäkemys
- Toiminnan jatkuvuuden varmistaminen
- Asiantuntijapalvelut

Mahdollisuuksia ja uhkia arvioitaessa teemat olivat:

- Edistyksellisen tekniikan hankinta
- Uudet yhteistyötahot
- Uudet kehitysmahdollisuudet
- Toimintaympäristön analysointi
- Kyberuhkien analysointi
- Toimintaverkoston analysointi

Tutkimuksen haastattelun johdanto-osiossa kohdeorganisaatiolla oli mahdollisuus sijoittaa toimintansa osaksi kuvion 5 mukaista verkottunutta toimintaympäristöä. Kyseisellä toimintaympäristön yleisellä kuvauksella pyrittiin laajentamaan kohteena olevan organisaation haastatteluteemoja siten, että tutkimukseen saatiin kohteen sisäisen tutkimuksen lisäksi käsitys sen toiminnasta yhteiskunnan kriittisen infrastruktuurin osana.

KUVIO 5. Kyberturvallisuutta edistävä verkottunut toimintaympäristö (Lehto ym., 2017, 41)

Yrityksen kybermaailman rakenne voidaan kuvata viidellä kerroksella, jotka ovat: kognitiivinen kerros, palvelukerros, semanttinen kerros, syntaktinen kerros ja fyysinen kerros (Lehto, 2015, 6). Tutkimuksessa kyberrakenteeseen on sijoitettu tyypillisen kohdeyrityksen IT- ja teollisuusautomaatiojärjestelmien (ICS) rakenteet ja SWOT-näkökulmat (Taulukko 1). Näin on saatu esille tutkimuksen SWOT-analyysin teemojen näkökulmien kattavuus läpi koko tutkimuskohteen tyypillisen kyberrakenteen. Taulukon 1 kerroksia voidaan siten käyttää yrityksen oman toiminnan tutkimuksen kattavuuden arvioinnin tukena.

Kyberrakenne	**Yritystason IT-toiminto**	**ICS-toiminto**	**SWOT-teemat ja -näkökulmat**
Kognitiivinen kerros	Johtaminen, henkilöstö, sidosryhmät, toimintaverkosto	Johtaminen, henkilöstö, sidosryhmät, toimintaverkosto	Johtaminen, (kyberturvallisuuden hallinta, riskit, toimintapolitiikka, jatkuvuus), henkilöstön osaaminen, tilannetietoisuus, sidosryhmänäkemys, toiminnan jatkuva parantaminen
Palvelukerros	Verkkoyhteydet, IT-palvelut	Verkkoyhteydet	Tuotteet ja palvelut (suojattavat prosessit, ohjausmekanismit)
Semanttinen kerros	Käyttöliittymät, data	Valvomot, data	Tuotteet ja palvelut (suojattavat prosessit, ohjausmekanismit)
Syntaktinen kerros	IT-järjestelmät (SW, verkkoliikenne)	Prosessiasemat (SW, verkkoliikenne)	Tuotteet ja palvelut (suojattavat järjestelmät)
Fyysinen kerros	IT-laitteet	Kenttälaitteet, kaapeloinnit	Henkilöstön osaaminen (hallinta ja ohjausmekanismit)

TAULUKKO 1. Esimerkki yrityksen kybermaailman rakenteesta ja niihin liittyvistä asioista SWOT-analyysin näkökulmista

Taulukossa 2 on esitetty esimerkki SWOT-analyysissä esiin tulevista kyberturvallisuuteen liittyvistä peruskysymyksistä

	VAHVUUDET **Positiivisten tekijät**	**HEIKKOUDET** **Negatiivisten tekijät**
SISÄISET	1. Mikä on tärkeää yrityksessä kyberturvallisuuden kannalta tarkasteltuna? 2. Missä asioissa olemme vahvoja? 3. Mitä kykyjä kehitämme edelleen?	1. Onko kyberturvallisuus kokonaisuutena huomioitu yrityksessämme? 2. Mitä asioita emme ole huomioineet? 3. Mitä kykyä emme ole kehittäneet?
	MAHDOLLISUUDET **Lista mahdollisuuksista, jotka liittyvät asiaan**	**UHKAT** **Lista uhkatekijöistä, jotka liittyvät asiaan**
ULKOISET	1. Onko yrityksen mahdollista hankkia käyttöönsä edistynyttä teknologia? 2. Löydämmekö uusia kontakteja ja yhteistyökumppaneita? 3. Voimmeko toimia oppivana organisaationa ja kehittää toimintojamme?	1. Tunnistammeko toimintaympäristömme ja yrityksen ulkopuolelta uhkaavat tietomurot? 2. Voimmeko luotta hankkimiemme tuotteiden palvelujen tietoturvaan ja järjestelmiimme? 3. Voimmeko luottaa toimintaverkostoomme?

TAULUKKO 2. Esimerkki yrityksen SWOT-analyysin peruskysymyksistä

6. SWOT-analyysin kompastuskivet

Onnistuessaan SWOT-analyysi mahdollistaa yrityksen kilpailuedun parantamisen kehittämällä vahvuuksiaan ja hyödyntämällä tulevaisuuden mahdollisuuksia sekä hallitsemaan tulevaisuuden riskejä. Analyysin toteuttamiseen sisältyy kuitenkin seikkoja, jotka saattavat olla onnistumisen esteenä. Kompastuskivet voivat liittyä tiedollisiin seikkoihin, toimintatapoihin tai prosessissa mukana oleviin henkilöihin. Näitä seikkoja voidaan avata seuraavasti: (Meristö, Molarius, Leppimäki, Laitinen & Tuohimaa, 2007, 10.)

- Prosessin onnistuminen saattaa kaatua esimerkiksi tiedollisiin ja näkemyksellisiin seikkoihin. Heikot lähtö- ja taustatiedot heijastuvat haitallisesti koko strategiatyön myöhempiinkin vaiheisiin. Tietojen kattavuutta voidaan varmistaa käyttämällä monialaisia tausta-analyyseja. Tulevaisuussuuntautuneessa työssä pelkkä nykyhetkeen sijoittuva tieto ei ole riittävää vaan tarvitaan näkemyksellistä tietoa tulevaisuuteen liittyen. SWOT-analyysiä laadittaessa riskinä on pitäytyminen vanhoissa käsityksissä, jolloin perususkomukset jyräävät kaiken muun. Tässä tilanteessa kyseenalaistajat voivat olla tärkeitä innovatiivisen näkemyksen esiin tuojia. Työssä ei voida myöskään jäädä liikaa pelkän organisaation sisäisen näkökulman varaan vaan näkökulmaksi täytyy valita ”ulkoa sisälle”. Näkökulmaa voidaan laajentaa esimerkiksi verkostojen avulla tai analogiamalleja hyödyntämällä. Kompastuskiveksi saattaa nousta myös osallistujien tietojen ja näkemysten epärealistisuus, jolloin esimerkiksi omat vahvuudet voidaan nähdä liian subjektiivisesti. Lisäksi strategisten päämäärien epämääräisyys ja yhteisen vision puuttuminen voi osaltaan vaikeuttaa tehtävää työtä. (Meristö ym., 2007, 15.)

- Toimintatapoja valittaessa kannattaa huomioida, että tekniset ratkaisut voivat vaihdella eri organisaatioiden välillä, jolloin valitun tavan sopivuus yrityskulttuuriin on tärkeää. Prosessin vaiheistus ja ohjeistus on tehtävä huolella, sillä työ täytyy kytkeä normaaliin strategiatyöhän sekä panostaa sen viestintään läpi organisaation. Liian vähäiset tai virheellisesti arvioidut resurssit esimerkiksi ajan suhteen voivat muodostua työn pullonkaulaksi. Jos tehtävällä työllä ei ole johdon tukea, henkilöstön osallistuminen prosessiin on vaikeaa, eikä tehtävään pystytä sitoutumaan. Onnistuneenkaan työn tuloksilla ei ole merkitystä, ellei niitä kyetä siirtämään yrityksen käytännön toimintaan. Aivoriihien ja muiden työryhmämenetelmien epävarmuudet voidaan hallita prosessiohjeistuksella ja vetäjien kouluttamisella. Erityisen tärkeää on kouluttaa työhön innostavat ja jämäkät vetäjät, jolloin osallistujat eivät koe aikansa menevän hukkaan. (Meristö ym., 2007, 15.)

- Strategiaprosessiin myös osallistuvat ihmiset ja heidän osaamisensa saattaakin muodostua kompastuskiveksi. Yksi seikka on prosessin vetäjien osaaminen tai osaamattomuus. Heidän ammattitaitonsa välittyy läpi koko strategiaprosessin. Vetäjän psykologista silmää tarvitaan heti istunnon alussa, jotta hän voi omalla aloituspuheellaan poistaa mahdolliset negatiiviset asenteet osallistujilta. Ryhmätyöistunnoissa onnistumisen kannalta on olennaista, että ideointivaiheissa esiin nousseita asioita ei arvostella ennen kuin on kyseessä erikseen sovittu arviointivaihe. Henkilöjohtamistaidon merkitys korostuu. Ryhmän koostumus ja sitoutuminen ovat myös tärkeitä. Ryhmän koostumukselta vaaditaan monialaisuutta, jotta näkemykset eivät jää liian yksipuolisiksi. Täytyy myös huolehtia siitä, että pelkästään yhden osallistujan vahvat mielipiteet eivät tukahduta muiden näkemyksiä. Tällöin uhkana on se, että muiden mielipiteet eivät pääse esiin. Muiden mielipiteitä voidaan kerätä ennakkoon haastatteluilla tai kyselyillä, jolloin vetäjällä on kokonaisnäkemys tilanteesta etukäteen. Luottamus osallistujien kesken parantaa työn sujuvuutta ja lisää osallistujien rohkeutta ilmaista näkemyksiään ja mielipiteitään. Onnistumisen kannalta tärkeää on myös osallistujien asenne, kuten uteliaisuus, riskinottohalu tai oppimishalu. (Meristö ym., 2007, 15.)

Taulukkoon 3 on koottu edellä kuvatun jaottelun mukaisesti keskeisten ongelmakohtien ratkaisut tyypillisessä SWOT-analyysiin perustuvassa yrityskohtaisessa kyberturvallisuuden tilannekuvatutkimuksessa. Toimenpiteillä voidaan parantaa huomattavasti tutkimuksen luotettavuutta.

	Ongelmakohta	Ratkaisu tutkimuksessa
Tiedot	• Lähtötietojen kattavuus • Tietojen painottuminen nykyhetkeen • Pitäytyminen vanhoissa käsityksissä • Liian kapea näkökulma • Tietojen epärealistisuus • Päämäärien epämääräisyys ja vision puuttuminen	• Monialainen analyysi haastatteluteemojen valinnalla • Tämän hetkisen toiminnan analysointi • Tutkimuksessa kaksisuuntainen näkökulma; yritys ja palvelun tuottaja • Tiedot käytännöstä • Tutkimuskohteen päämäärät kansallinen kyberturvallisuuden viitekehyksestä
Toimintatavat ja työkalut	• Teknisten ratkaisujen valinta • Prosessin vaiheistus ja ohjeistus • Sitoutumisen puute • Tulosten ottaminen käyttöön • Väärät työkalut ja menetelmät • Osaamattomuus menetelmissä	• Teknologian arviointi • Kytkentä normaaliin strategiatyöhön • Viestintä läpi koko organisaation • Kehitysehdotukset huomioidaan • SWOT toimiviksi osoittautunut menetelmiä • Menetelmä kuvattuna edeltä toimitetussa materiaalissa
Henkilöt	• Vetäjien osaamattomuus • Ryhmän yksipuolinen koostumus/Hallitsevat yksilöt • Luottamuksen puute	• Haastattelijoilla oltava hyvä kokemus tutkimusalueesta • Tutkimuskohteen paras asiantuntemus haastateltavana • Avoimuus ja läpinäkyvyys

TAULUKKO 3. SWOT-analyysin keskeisimmät ongelmakohdat ja niiden ratkaisut sovellettuna tutkimusympäristöön (Meristö ym., 2007, 20)

7. Yhteenveto

SWOT-analyysiä pidetään yleisesti toimivana työkaluna yrityksen strategian laatimisessa, sekä oppimisen tai ongelmien tunnistamisessa, arvioinnissa ja toimintaprosessien kehittämisessä. Yrityksen strategiatyön ohella analyysiä voidaan soveltaa muiden edellä mainittujen kohteiden selvittämiseen harkitusti valittua skenaariota peilaten. Se auttaa tilannekuvan muodostamisessa tarkastelukohteesta. Tilannekuva ja siitä vedettävät johtopäätökset voidaan toteuttaa Endleyn kehittämän teorian mukaisesti, eli tarkasteltavan tilanteen havaitsemiseen, tilanteen ymmärtämiseen ja sen vaikutuksen arviointiin tulevaisuuteen nähden (Endsley, 1995). Tällä tavoin muodostettava tilannekuva antaa perusteet johtopäätöksiin ja niitä seuraavaan päätöksentekoon. Tämän artikkelin tutkimusesimerkissä tarkasteltavaksi skenaarioksi oli valittu yrityksen kyberturvallisuus ja siitä muodostettava tilannekuva. Tilannekuvan muodostamiseksi tutkimustavoitteita ja –kysymyksiä silmällä pitäen on tutkimusalueen viitekehyksestä ja lähtötiedoista muodostettu haastatteluteemat. Tutkimuksen organisaatiokohtaisista haastatteluista on koottavissa teemakohtaiset yhdistelmätiedot, joista puolestaan muodostuvat tutkimusalueen tilannekuva johtopäätöksiä ja kehitysehdotuksia varten.

Edellä kuvatulla tavalla muodostettu yrityksen kyberturvallisuuden tilannetietoisuuden muodostaminen SWOT-analyysin avulla mahdollistaa strategisten, operatiivisten ja teknillis-taktisen tason toimenpiteiden tarkastelun. Tutkimuskohteista on mahdollista saada tietoa kattavasti ja avoimesti kaikkiin päätöksenteon tasoihin liittyen, kuten valtioneuvoston kanslian kansallista kyberturvallisuutta käsitelleessä tutkimushankkeessa voitiin todeta. Tilannekuvan avulla muodostettavat kokonaisvaltainen ja syvällinen käsitys tutkimuskohteesta on keskeisessä roolissa, kun kehitetään koko organisaation toimintaa ja sitä kautta koko kansallisen kriittisen infrastruktuurin toimintakykyä.

Lähteet

Bowersox, D., Closs, D., Jessop, D. & Jones, D. (1986). Logistical Management. New York, John Wiley & Sons, Ltd.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors: *The Journal of the Human Factors and Ergonomics Society, 37(1),* 32 - 64.

Knowles, W., Prince, D., Hutchison, D., Ferdinand, J., Disso, J.F.P. & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection 9*. Saatavilla: 25.10.2015 https://ac.els-cdn.com/S1874548215000207/1-s2.0-S1874548215000207-main.pdf?_tid=447861da-17f0-4223-8563-d7ff6013850c&acdnat=1532352262_fcc694993b2991fe9670c3615ea7a5b3

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/201. Saatavilla: 18.7.2017 https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Lehto, M. (2015). Phenomena in the cyber world. Teoksessa Lehto, M. & Neittaanmäki, P. (toim.), *Cyber Security: Analytics, Technology and Automation* (3 - 29). Germany: Springer International Publishing.

Melkman, A. & Simmonds, K. (2016). Strategic Customer Planning: How to Develop and Implement a Strategic Account Plan. A specially commissioned report. Lontoo: Thorogood Publishing Ltd.

Meristö, T., Molarius, R., Leppimäki, S., Laitinen, J. & Tuohimaa, H. (2007). Laadukas SWOT. Työkalu pk-yrityksen innovaatiovetoisen tulevaisuuden menestyksen turvaamiseksi. Technical Report. Turku: Corporate Foresight Group CoFi / Åbo Akademi. Saatavilla: 18.7.2017 https://www.researchgate.net/publication/312020497_LAADUKAS_SWOT_Tyokalu_pk-yrityksen_innovaatiovetoisen_tulevaisuuden_menestyksen_turvaamiseksi

Nyarku, K. & Agyapong, G. (2011). Rediscovering SWOT Analysis: The Extended Version. *Academic Leadership: The Online Journal 9(2),* 1- 17. Saatavilla: 18.7.2017 https://scholars.fhsu.edu/cgi/viewcontent.cgi?article=1666&context=alj

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Menetelmäopetuksen tietovarannon internetsivusto. Saatavilla: 5.12.2016 http://www.fsd.uta.fi/menetelmaopetus

Turvallisuuskomitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. Saatavilla: 5.12.2016 https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Informaatioteknologian tiedekunnan julkaisuja
No. 58/2018

ISBN 978-951-39-7547-0 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO