Tuija Kuparinen-Koho

Havaintotiedon käsittely toimintaympäristöjen uhkiin varautumisessa

Pro gradu

Tekniikan ja innovaatiojohtamisen yksikkö
Tietojärjestelmätieteen Pro gradu -tutkielma
Teknisen viestinnän maisteriohjelma

Vaasa 2024

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen yksikkö
Tekijä: Tuija Kuparinen-Koho
Tutkielman nimi: Havaintotiedon käsittely toimintaympäristön uhkiin varautumisessa
Tutkinto: Kauppatieteiden maisteri (tekninen viestintä)
Oppiaine: Tietojärjestelmätiede
Työn ohjaaja: Tero Vartiainen
Valmistumisvuosi: 2024 **Sivumäärä:** 113

TIIVISTELMÄ:
Tutkielmassa perehdytään energiatoimialaan, sen turvallisuuteen ja uhkiin sekä havaintotietojen keräämiseen toimintaympäristöstä. Yleisen turvallisuustilanteen ollessa tutkimusaikana voimakkaassa muutoksessa on perusteltua luoda katsaus kriittisen infrastruktuurin toimijan mahdollisuuksiin luoda ja ylläpitää uhkatilannekuvaa huoltovarmuuteen liittyvän varautumisen ja resilienssin toteuttamiseksi.

Tutkielmassa sovelletaan kirjallisuuskatsauksen ja aineistoanalyysin menetelmiä tutkimuksen lähtökohdan ja merkityksen esille tuomiseksi sekä tutkimustuloksen tuottamiseksi. Tutkielman tarkoituksena on tuoda esiin mekanismeja ja menettelyitä, joiden avulla energia-alan toimija voi kehittää varautumis- ja ennakointikyvykkyyttään uhkien havaitsemiseksi muuttuvassa toimintaympäristössä. Tavoitteena on tuoda esiin perusteluja liiketoimintauhkien kokonaisvaltaisen havainnoinnin tarpeellisuudelle laaja-alaisen turvallisuuden kontekstissa.
Tutkielmassa selvitetään uhkien havainnoinnin ja tilannekuvan hallinnan tietoteknisen tuen toteutusta sekä huomioita tiedonhankintatekniikoiden, tietotuotteen ja teknologisen analyysikyvykkyyden näkökulmista. Tutkielmassa kuvataan monilähdetietoa yhdistelevän fuusiojärjestelmän toimintaperiaatetta ja soveltamista monitahoisten uhkien tiedonkäsittelyn kontekstissa. Inhimillisen havainnoinnin osuutta tarkastellaan suhteessa tiedon tuottamiseen ja liittämiseen osaksi teknistä järjestelmäratkaisua.

Tutkielman tuottama päähuomio muodostuu monialaisen, sektori- ja organisaatiorajat ylittävän tarkastelutarpeen ympärille. Uhkatietojen käsittely on monenvälistä sekä inhimillistä että konepohjaista toimintaa, jolle löytyy monitieteellistä laajaa tarkastelupinta-alaa. Tutkimushavaintona onkin, että inhimillisen havainnoinnin asemasta sekä havainnoitavien kohteiden monipuolisuudesta ja kattavuudesta erilaisine teknologiaympäristötoteutuksineen tarvitaan lisää tarkentavaa ja määrittävää monialaista tieteellistä tutkimusta. Energia-alan toimijoiden uhkatilannekuvan muodostumista tulee vahvistaa kokonaisvaltaisen tapahtumaketjuanalysoinnin sekä tiedustelevien ja ennakoivien turvallisuusmenettelyiden avulla välittömien operatiivisten uhkien torjunnan rinnalla. Tietoa uhkatoimijoiden identiteeteistä, motivaatioista, tavoitteista, strategioista sekä kyvykkyyksistä tulee kerätä järjestelmällisesti.

Tutkielman tuloksella pyritään ymmärryksen lisääntymiseen yleisellä tasolla uhkakuvien, uhkien ennakoinnin sekä verkostoyhteistyön merkityksistä ja soveltamisesta energiatoimialalla. Tämän vuoksi on suositeltavaa tarkentaa tutkielman teemaa jatkotutkimuksella, jossa voitaisiin tuottaa tapaustutkimuksellinen tapahtuma-analyysi energia-alaan kohdistuneesta uhkatilanteesta laukaisevine tekijöineen sekä häiriö- ja varautumisvaikutuksineen. Jatkotutkimusehdotukset liittyvät myös liiketoimintatiedustelun kontekstin laajentamiseen ja soveltamiseen uhkien hallintaan.

AVAINSANAT: Energiatoimiala, sähköntuotanto, kyberturvallisuus, uhka, havaitseminen, tilannetietoisuus, ennakointi, varautuminen, tiedonhallinta, datafuusio

Sisällys

Kuvat

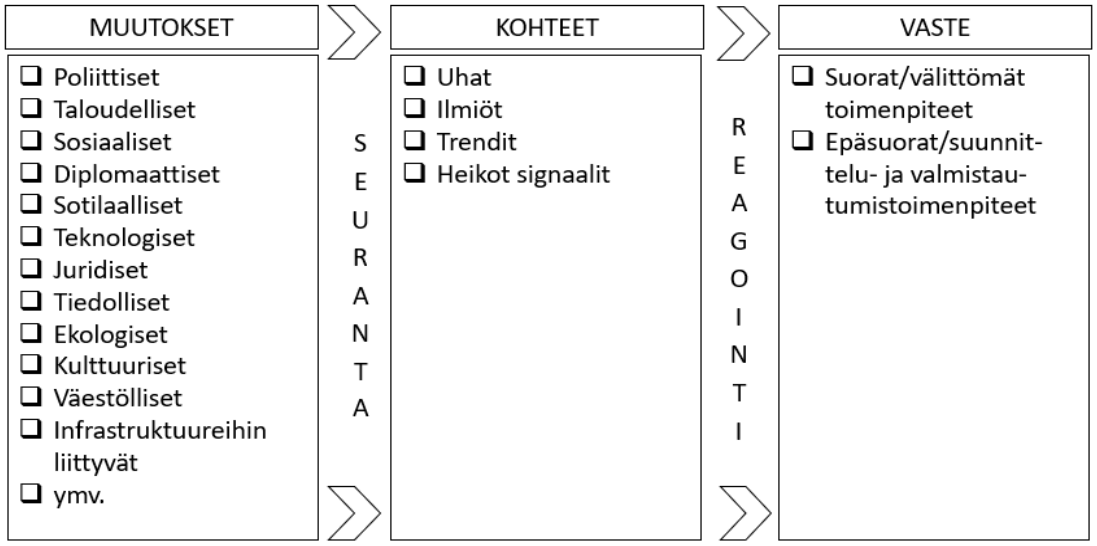
Kuviot

Taulukot

1 Johdanto

Tämän tutkielman tekohetkellä eri puolilla maailmaa on käynnissä hyökkäyssotaa, talous- ja kauppasotaa, hybridisodankäyntiä, vakoilua ja tiedustelua, ympäristökriisejä sekä energiateknologioiden käyttöönottoja ja käytöstä hiipumisia. Saamme lähes päivittäin lukea erilaisia energiaan liittyviä uutisointeja, kuten esim. uusiutuvien energiaratkaisujen käyttöönottovaikeuksista (Pantsu, 2023), yhteistoimijoiden investointihaasteista ja kilpailuasetelmista (Ukkonen & Ruokangas, 2024), kyberiskuista tuotantolaitoksiin (Ortamo, 2024) sekä laitosten yllättävistä toimintahäiriöistä (Mäklin, 2024). Tutkielman aihealue on edellä mainittujen kaltaisten tapahtumien ja niiden taajuuden vuoksi ajankohtainen ja vaatii tarkempaa tarkasteltua uhkahavainnoinnin kontekstissa.

Tutkielmassa tarkastellaan organisaatioiden ja yhteisöjen uhkien havaitsemisen merkitystä jatkuvasti muuttuvassa toimintaympäristössä. Toimintaympäristö muodostuu poliittisista, taloudellisesta, sosiokulttuurisista ja ekologisista komponenteista, joihin niiden resurssit, toimijoiden keskinäinen vuorovaikutus sekä niiden väliset tapahtumat vaikuttavat (Rubin, 2024). Toimintaympäristössä selviytyminen vaatii kykyä tunnistaa siinä tapahtuvia muutoksia sekä kykyä reagoida niihin. Toimija voi varautua toimintaympäristömuutoksiin tunnistamalla niitä eri näkökulmista, arvioimalla muutosten vaikutusta toimintaan sekä suunnittelemalla reagointitoimenpiteet. Toimintaympäristön muutoksia tulee tarkastella useasta ulottuvuudesta tai näkökulmasta. Seuraava kuvio kuvaa tätä järjestelmällistä ja ennakoivaa tarkastelutapaa.



Kuvio 1 Viitekehys toiminnan suunnitteluun

Keskinäisriippuvaisten muutosten seuranta edellyttää kykyä ymmärtää, tulkita ja analysoida niitä omassa kontekstissa, jotta omaan toiminnan päätöksentekoon liittyvät valinnat ovat tuloksekkaita. Havaitsemisen tulee olla laaja-alaista ja tarkkailun herkeämätöntä, jotta uhkiin kyetään varautumaan ja kasvattamaan samalla niistä tietopääomaa. Viestinnän ja tiedon käsittelyn merkitys korostuvat tämän saavuttamiseksi. Eri muutosnäkökulmista muodostuu toisiinsa sidoksissa olevia ja vuorovaikuttavia ajureita, jotka eri tilanteissa voivat toimia toistensa kilpailijoina, kirittäjinä, laimentajina tai voimistavina tekijöinä (Pherson & Pherson, 2017). Tämän vuoksi tiedonkeruun muutostekijöistä tulee olla suunniteltua, johdonmukaista ja järjestelmällistä.

Kyberturvallisuuden merkitys on suuri energiatoimialan kuuluessa kriittiseen infrastruktuuriin. Suomalaisten energiayhtiöiden joutuessa päivittäin verkkohyökkäysten kohteeksi (Korhonen, 2024) on syytä ottaa huomioon vahingoittavien toimien suunnitelmallisuus ja tavoitteellisuus tällä geopoliittisten ja taloudellisten jännitteiden, väärän ja harhaanjohtavan tiedon, kyberhyökkäysten, hybridioperaatioiden ja useiden valtioiden välisten konfliktien (Rimppi & Kivisaari, 2024) aikakaudella.

Tutkimuskohteena ovat toimintaympäristön uhkiin varautumisen tietotarpeet ja menetelmät energiatoimialan yrityksen näkökulmasta, energiatoimialan ollessa 2020-luvun toimintaympäristön muutosten vuoksi erityisen kiinnostava. Energiankulutus tulee kasvamaan kaikkialla maailmassa. Tämä vaatii useiden energianlähteiden hyödyntämistä ja aktiivista kehitystyötä tuotanto-, varastointi- ja siirtoteknologioissa. Jotta hiilidioksidipäästöjä pystytään leikkaamaan, on tavan tuottaa ja kuluttaa energiaa muututtava radikaalisti. Uusiutuvaa energiaa pyritään tukemaan poliittisin ja verotuksellisin linjauksin.

Ilmastonmuutoksen uhat ja lisääntynyt ympäristötietoisuus kasvattavat toiminnan ympäristövaatimuksia myös niihin mukautuvan lainsäädännön ja sääntelyn kautta, mistä syystä toimijoiden on perusteltua seurata poliittista päätöksentekoa. Poliittiseen päätöksentekoon vaikutetaan mm. eri edunvalvontajärjestöjen toimin. Vuorovaikutus kehittää toiminnan ennakointivalmiuksia. Ennakointia toteutetaan järjestelmällisellä tiedonkeruulla, jota tuetaan digitaalisen palveluympäristön teknologiainnovaatioilla. Kerätyn tiedon avulla toimijat kykenevät strategiseen suunnitteluun ja tiedolla ohjaukseen sekä torjumaan toimintaympäristössään ilmeneviä riskejä. (Järvenpää, Kunttu & Mäntyneva, 2020)

Energiatoimiala joutuu sopeutumaan ilmastonmuutokseen kaikin tavoin. Britanniassa uutisoitiin 25.4.2021 (Pilgrim, 2021), että brittiläinen tiedustelupalvelu MI6 alkaa seurata isoja teollisuusmaita siinä, miten ne sitoutuvat ilmastonmuutoksen torjunnan tavoitteisiin. Vakoilun ja tiedustelun oletetaan aktivoituvan aiempaa vilkkaammaksi toiminta- ja elinympäristöjen muutosten voimistuessa, mikä puolestaan synnyttää uusia tarkkailtavia uhkia.

Tutkielman tuottaa tuloksinaan määritelmää energiaturvallisuudesta sekä ajanhetken kuvausta energia-alan kohtaamista uhista. Tutkielma luo ohjaavan viitekehyksen uhkien havaitsemista tukevalle tiedonhankinnalle ja järjestelmäratkaisun suunnittelulle. Tutkiel-

massa tuodaan esiin mahdollisia lähitulevaisuuden merkittäviä tutkimuskohteita. Seuraavassa alaluvuissa kuvataan tarkemmin tutkielman tavoitetta, käytettyjä aineistoja, tutkimusmenetelmää sekä tutkielman rajausta.

1.1 Tutkielman tavoite

Tutkielman teoreettinen tehtävä voidaan määritellä siten, että tutkimustuloksena tavoitellaan ymmärryksen lisäämistä yleisellä tasolla uhkakuvien soveltamisesta energiatoimialalla. Tällöin tutkielma tukee kriittisenä funktionaan ns. arki- tai yleisen uhkiin liittyvän tiedon muuntamista tietoiseksi tiedoksi, käytännöllisenä funktionaan tutkimuskohteen eli uhkien havaitsemisen tutkimuksellista hallittavuutta sekä retorisena funktionaan oletetusti kiinnostavan tiedon tuottamista aihealueestaan. Lisäksi tutkielmalla pyritään suuntamaan tutkimuksellista huomiota tuomalla esiin aihealueen monitahoisuutta ja ehdottamalla jatkotutkimusaiheita. (Saaranen-Kauppinen & Puusniekka, 2006)

Tutkielmaa ohjaa lähtöajatus siitä, että uhkien hallinta on edelleen tehotonta ja tilannetietoisuutta tukevia teknologiamahdollisuuksia ei hyödynnetä, vaikka toimijat kohtaavat yhä jalostetumpia, monimutkaisempia ja vaikeasti vastattavia uhkia (McMahon, Rohozinski & Canada, 2013). Tutkielman tavoitteena on selvittää energia-alan toimijan toimintaympäristössä ilmeneviä uhkia ja muodostaa tämän pohjalta ymmärrys siitä, miten toimintaympäristön uhkien inhimillisesti suoritettavaa havaitsemista voidaan tukea tieto- ja viestintäteknisesti. Tutkimusoletukseksi asetetaan, että toimijan turvallisuutta edistää laaja-alaisen turvallisuuden soveltaminen uhkien kattavan havaitsemisen toteuttamiseksi. Tutkielman tuloksena pyritään tuomaan esille tieteellisesti perusteltavissa oleva käsitys siitä, miksi toimintaympäristöjen havainnoinnin tukeminen on tärkeää toimijan kannalta. Lisäksi tutkielmalla pyritään toteamaan, miten tieteellisessä tutkimuksessa on käsitelty laaja-alaiseen uhkien havainnointiin liittyviä tarpeita sosioteknisissä järjestelmissä ja miten kuvataan inhimillisen havainnoinnin osuutta tässä.

Tutkielman tarkoituksena on tuoda esiin menettelyjä, hallintamalleja tai viitekehyksiä, joiden avulla energia-alan toimija voi kehittää varautumis- ja ennakointikyvykkyyttään

dynaamisessa ympäristössä. Tutkielman tavoitteena on perustella liiketoimintauhkien kokonaisvaltaisen havainnoinnin tarpeellisuutta laaja-alaisen turvallisuuden kontekstissa nopeasti muuttuvassa toimintaympäristössä. Tapausesimerkkinä käytetään energia-alan toimijaa. Lisäksi tarkastellaan sitä, miten havainnointia on kuvattu tietoja yhdistävien järjestelmäratkaisuiden tieteellisissä tutkimusartikkeleissa. Edellä kuvatun tavoitteen saavuttamiseksi asetetaan seuraavat tutkimuskysymykset:

(1) Mitä energiaturvallisuus on?
(2) Millaisista tekijöistä toimintaympäristön uhat voivat muodostua?
(3) Millaisia tietoja energia-alan toimijan kannattaa kerätä toimintaympäristöstään uhkiin varautumiseksi?
(4) Miten inhimillisen havainnoinnin osuutta esitellään tietojärjestelmäratkaisuissa?

Edellä kuvattujen tutkimuskysymysten vastausten pohjalta tutkimuksessa pyritään selvittämään ja määrittelemään toimintaympäristön liiketoiminnallisia tietoon liittyviä tarpeita. Tutkielman neljännessä pääluvussa vastataan kysymyksiin energiaturvallisuudesta (tutkimuskysymys 1) sekä toimintaympäristön uhkatekijöistä (tutkimuskysymys 2). Viidennessä pääluvussa kuvataan uhkiin liittyvien tietojen hankintaa ja käsittelyä vastaamalla kysymykseen tietojen keräämisestä (tutkimuskysymys 3). Toisessa pääluvussa kuvataan läpikäydyn tutkimusaineiston avulla inhimillisen havainnoinnin esille tuontia järjestelmäratkaisuissa (tutkimuskysymys 4).

1.2 Tutkimusaineisto

Tutkielman lähdeaineiston käytössä pyrittiin mahdollisimman suureen kattavuuteen ja laaja-alaisuuteen. Käytetty materiaali on aiemmin julkaistua ja tutkijan valitsemaa tutkimusaiheeseen liittyvää ns. toissijaista aineistoa. Aineistona hyödynnettiin kirjallisuutta, uutisartikkeleita ja tutkimusraportteja, joita teemoiteltiin ja koottiin tutkimuskysymyksiin vastaamista varten.

Kirjallisuuskatsaukseen valittiin yliopiston hakupalvelun kautta saatavilla olevat tieteellisesti vertaisarvioidut julkaisut, joita esivalintavaiheiden jälkeen oli 17 kappaletta. Laadullisen tutkimuksen paradigman (Saaranen-Kauppinen & Puusniekka, 2006) mukaisesti tutkija tarkastelee energia-alan uhkien ymmärtämistä ilmiönä uhkien tilastollisten yhteyksien sijaan, jolloin määrältään pienikin tutkimusaineisto on riittävä. Kirjallisuuskatsauksen tulokset esitetään tutkielman toisessa pääluvussa.

1.3 Tutkimusmenetelmä

Tutkielmassa perehdytään energiatoimialaan ja sen turvallisuuteen ja uhkiin sekä havaintotietojen keräämiseen toimintaympäristöstä. Tutkielmassa avataan energiatoimialan uhkia suunnittelu-, tulevaisuus- ja turvallisuustieteellisessä kontekstissa kirjallisuuskatsauksen keinoin. Tutkielmassa analysoidaan 17 kpl vuosina 2018–2024 julkaistua vertaisarvioitua tieteellistä julkaisua uhkatiedon hallinnasta tietovirtoja kokoavissa järjestelmissä. Tutkimusmenetelmänä käytetään sisällönanalyysia tutkimusotteen ollessa käsitteellis-teoreettinen (Saaranen-Kauppinen & Puusniekka, 2006).

Kerättyä tietoa teemoiteltiin tutkielman osa-alueiden määrittämiseksi. Teemojen pohjalta muodostettiin tutkielmaraportin pääluvut, joista ensimmäisessä johdatellaan lukija tutkielman ajankohtaisuuteen, kohteeseen, merkitykseen ja tärkeyteen sekä lyhyesti tuloksiin. Toinen pääluku koostuu kirjallisuuskatsauksesta aiempaan tutkimukseen. Kolmannessa pääluvussa kuvataan tutkielman teoriapohjaisuutta ja menetelmiä tutkielman tuottamisessa. Neljännessä pääluvussa käydään läpi esimerkiksi ts. tutkimustapaukseksi valittua energiatoimialaa ja sen ajankohtaisia uhkia. Viidennessä pääluvussa perehdytään uhkien havaitsemiseen, havaitsemisen merkitykseen ajallisessa kontekstissa ja uhkiin liittyvään tiedonkäsittelyyn. Kuudennessa pääluvussa esitetään kirjallisuuskatsauksen tulos. Synteesi ja diskussio tutkielman merkityksestä ja aihealueen mahdollisista tulevista käsittelynäkökulmista esitetään viimeisessä seitsemännessä pääluvussa.

1.4 Tutkielman rajaus

Tutkielmassa tarkastellaan yleisesti energiatoimialaan liittyvien mahdollisten uhkien havainnointia tarkemmin määrittämättömän energia-alan organisaation näkökulmasta. Tutkielman ulkopuolelle rajautuvat varsinaisten järjestelmävaatimusten tuottaminen uhkien havaitsemiseen käytettävästä teknisestä alustasta. Tutkielmassa ei myöskään suunnittelutieteen periaatteiden mukaisesti tuoteta uhkahavainnointiin täsmällistä artefaktia tai tietotuotetta, eikä siten testata ts. todenneta sen toimivuutta, tarkoituksenmukaisuutta tai käyttötarpeisiin vastaavuutta. Edellä kuvatun pohjalta tutkielmassa ei tutkita visualisoinnin alaa eli merkityksien kuvaamista, symbolien käyttöä tai sopimukseen perustuvia asioiden kuvaamistapoja, jotka ovat tilannekuvajärjestelmissä olennaisia elementtejä, kuten esim. kartografioissa, geoinformatiikkajärjestelmissa tai joukkojen ja kriisinhallinnan seurannassa. Samoin visualisointiin kuuluva uhkamallintaminen (esim. hyökkäyspuut, tapahtumakulut ymv. kuvausmenetelmät) jää tämän tutkielman ulkopuolelle.

Uhkien havainnointi liittyy vahvasti ihmisen toimintaan ja kognitioon. Nämä, kuten myös tilannetietoisuuteen liittyvä päätöksenteko rajataan tämän tutkimuksen ulkopuolelle niiden ollessa oma tutkimusalansa. Tutkimuksessa ei tarkastella havainnointiin liittyviä vääristymiä, vaan tavoitteena on saada esiin se, mitä tulisi havainnoida ja mistä. Tutkimus toimii ylätason periaatteellisena linjauksena siitä, mitä uhkien havainnoinnissa voidaan ottaa huomioon. Tällöin tutkimusta ei voida rajoittaa yksinomaan kyberturvallisuuteen, vaan siinä pyritään tuomaan esille turvallisuus sen laajassa merkityksessään.

Tutkielmassa ei kuvata minkään tietyn organisaation tai kohteen nykytilaa, tarpeita tai olemusta tapaustutkimuksena tai käsitteellisesti, eikä mitata kehittämistuloksena saatavan ratkaisun hyötyä. Tutkimuksessa ei myöskään suoranaisesti korjata epäkohtia esim. tuottamalla vaatimusmäärittelyitä tai arvioimalla liiketoiminnan tietojärjestelmäratkaisuille asettamien vaatimusten toteutumista. Vaatimusmäärittelyllä tarkoitetaan vaatimusten keräämistä, niiden tarkentamista, sekä mallintamista ja dokumentointia, millä saadaan vastaus kysymyksiin, jotka koskevat kehitettävää kohdetta, ratkaistavia asioita,

järjestelmätarpeita, tuotettavia ja käytettäviä tietoja, suoritettavia toimintoja, rajoitteita ja rajapintoja (Tieturi, 2013).

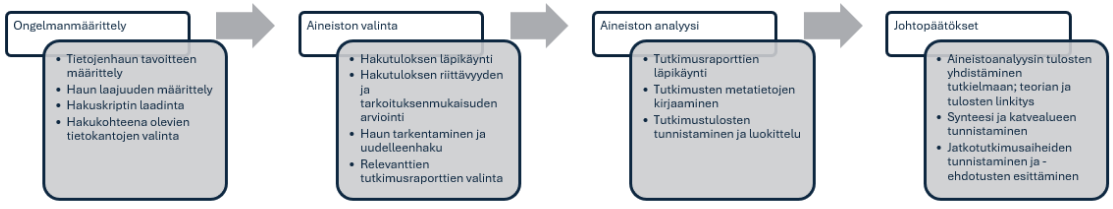
Myös riskienhallinta rajataan tämän tutkielman ulkopuolelle. Vaikka riskienhallinalla on looginen kytkös uhkien hallintaan, muodostaa se kuitenkin oman viitekehyksenä, jota ei tässä tarkastella.

2 Kirjallisuuskatsaus aiempaan tutkimukseen inhimillisen havainnoinnin osuudesta järjestelmäratkaisuissa

Tutkielman tavoitteena on johdannossa esitetyn mukaisesti teoriapohjan ohjaamana tuoda esille sitä, miten uhkien havainnointia käsitellään monilähdetietoja yhdistävissä järjestelmäratkaisuissa. Tässä yhteydessä inhimillisellä havainnoinnilla tarkoitetaan ihmisen havainnoimaa, keräämää ja käsittelemää tietoa, jota tuodaan osaksi monilähdetietoa käsittelevää tilannekuvajärjestelmää tiedon tuottamisen ja yhdistämisen vaiheissa. Tarve inhimilliselle havainnoinnille on tässä lähtöoletuksena uhkakentän ja tietolähteiden laajuuden vuoksi, sillä toimijan toimintaympäristöstään tarvitsemaa kaikkea tietoa ei ole oletetusti ole saatavilla automatisoidusti tuoden koneluettavaan muotoon tai muutoin valmiiksi tietoeriksi tai -tuotteiksi jo jalostettuina. Tiedon tulkintaan tarvitaan myös inhimillistä työpanosta.

2.1 Havaitsemiseen liittyvä aineistoanalyysi

Aineistoanalyysissa edettiin järjestelmällisesti alla esitetyn prosessikuvion mukaisesti tietojenhaun määrittelystä aineiston valintaan ja sen analyysin sekä johtopäätösten tekemiseen. Tietojenhaku toteutettiin yliopiston hakupalvelun kautta saatavilla oleviin tieteellisiin vertaisarvioituihin julkaisuihin. Tietojenhakua kokeiltiin ensiksi suomenkielisenä, mutta tulosten ollessa vähäisiä, päädyttiin käyttämään englanninkielistä materiaalia sen runsaamman tuloksen vuoksi.



Kuvio 2 Aineistoanalyysi

Hakutulosten kohdentumista hallittiin tutkimuksen teoriassa ja viitekehyksessä esiintyvien käsitteiden avulla, joiden merkitystä haun laajuuteen on kuvattu seuraavassa taulukossa.

Taulukko 1 Hakutermit

Avainsana / hakutermi	**Käsitteen merkitys haussa**
business risk	riskienhallinnan kokonaisuus; riskeihin varautuminen tiedonhallinnan näkökulmasta
business threat	liiketoimintaan, toimijan toimintaympäristöön tai kriittisen infrastruktuuriin kohdistuvien uhkien määrittely ja hallinta; tietojen kerääminen haitallisista tapahtumista tai kehityskuluista
data fusion	tietojen saatavuus toiminnasta ja toimintaympäristöstä ja niiden hyödynnettävyys osana riskienhallintaa ja uhkiin varautumista; monilähdetietojen looginen ja tekninen yhdistäminen
environment scanning	menetelmä toimintaympäristön tarkkailemiseksi; tiedonkeruu toimijan toimintaympäristöstä
horizon / horizont scanning	vrt. ’environment scanning’; vaihtoehtoinen nimi tiedonkeruumenetelmälle
information	tieto; yhdistävä pääkäsite aloitushaussa
intelligence	tiedustelu; liiketoimintatiedustelu
JDL	JDL-mallin kehittänyt tutkimusyhteisö; yhdistävä tunniste
JDL model	datafuusiomalli; mahdolliset sovellutukset toimijan tietojenkeruussa riskienhallintaa ja uhka-arviointia varten

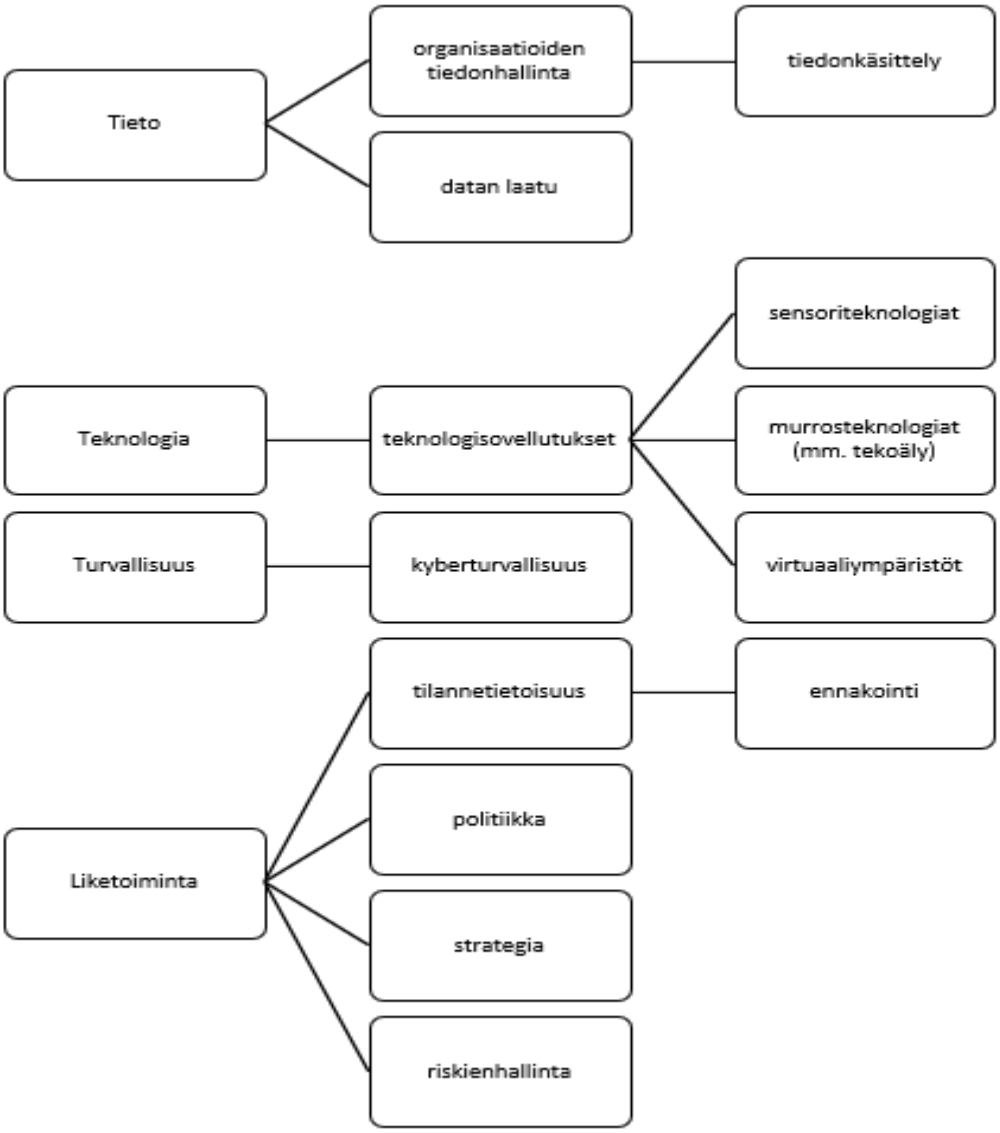
perception	havaitseminen; toimijan tilan ja toimintaympäristön muutosten havainnoinnin suorittaminen, tietopohjainen riskien ja uhkien havainnointi osana tilannetietoisuutta
situation awareness	tilannetietoisuus; tilannetietoisuuden toteuttaminen tiedonkeruun avulla; tilannekuvajärjestelmä

Em. avainsanojen avulla pyrittiin rajaamaan hakutulosten kohdentumista liiketoiminnan kontekstin uhkavarautumiseen ja sen tietojenhallintaan. Haku kohdennettiin Tritonian Finna-kantaan. Haku suoritettiin kolmessa vaiheessa, joissa jokaisessa hakuehtoina käytettiin sekä vertaisarvioitua että englanninkielistä julkaisua.

Ensimmäisessä haussa avainsanoiksi valittiin ja-operaattorilla (”AND”) *JDL, information, perception, situation awareness* sekä *environment scanning* tai (”OR”) *horizont scanning*, jolloin haun tulokseksi saatiin 11 julkaisua. Toisessa haussa avainsanoiksi valittiin *horizon scanning, environment scanning, data fusion, business risk, business threat* sekä *intelligence*, jolloin tulokseksi saatiin 66 julkaisua. Tässä vertaisarvioitu- ja englanninkielisen hakuehdon lisäksi sovellettiin myös julkaisuvuosi-hakuehtoa vuosille 2018–2100. Kolmannessa haussa avainsanoina käytettiin *data fusion, JDL model, perception* ja *intelligence* -termejä, jotka vertaisarvioitu-, englanninkielisyys- ja julkaisuvuosi 2018–2100 -hakuehtojen kanssa antoivat tulokseksi 17 julkaisua.

Hakutulosten kaikki julkaisut luettiin ja aineistoon valittiin ne, mitkä käsittelivät viitekehyksiä tai edustivat laajaa näkökulmaa. Lopulliseen tuloslistaukseen ei sisällytetty julkaisujen kaksoiskappaleita eikä sellaisia julkaisuja, joissa keskityttiin yhteen tiettyyn teknologiaan. Poistettaviksi sisällöiksi luokiteltiin esim. kyberturvallisuuden tapahtumienhallintaa tai pelkästään yhtä teknologiaa (koneoppimismalli, virtuaali- tai lisätty todellisuus, robottisovellutus) käsittelevät julkaisut, kuten myös tieteellistä metodologiaa (aineistoanalyysi) ja yritysten suhdetoimintaa (PR, liiketoimintadiplomatia) esittelevät julkaisut. Jäljelle jäi 17 tutkimusta, joiden sisältö purettiin auki.

Julkaisuista löydettiin erilaisia pääaihealueita ja tulokseksi saatiin tiedon, teknologian, turvallisuuden ja liiketoiminnan pääteemat. Teemakokonaisuutta on kuvattu seuraavassa kuviossa:



Kuvio 3 Aineiston pääteemat

Kyberturvallisuuden teema toistui useimmissa hakuun sisällytetyissä tutkimuksissa. Yhden julkaisun voidaan myös katsoa kuuluvan useampaan teemaan esim. kyberturvallisuuden teknologioita käsitellessä. Analyysiin valituissa julkaisuissa toistui useimmiten teknologiateema.

2.2 Aineistoanalyysin keskeinen sisältö

Tarve tietojen yhdistämiseen tehokkaamman tiedustelun prosessien ja menetelmien kehittämiseksi on tunnistettu myös EU-tasolla. Gruszczack (2022) tutkii datafuusion ja analytiikan kyvykkyyksien kehittämistä EU:n yleisen turvallisuuden ja puolustuksen politiikan (Common Security and Defence Policy CSDP) kontekstissa osana EU:n tiedustelu- ja tilannekeskuksen (EU Intelligence and Situation Center INTCEN) toimintaa. Tutkimuksessa todetaan datafuusiokyvykkyden rajoittunut ja vähäinen tuki kansainväliselle turvallisuudelle johtuen tehottomista ja puutteellisista tiedon jakamisen kansallisista järjestelmistä sekä kansainvälisten toimielimien ja yhteistyökäytäntöjen puutteista. Huolimatta tiedonjaon tunnustetuista hyödyistä, poliittisesta tahtotilasta ja yrityksistä rakentaa ohjaavaa viitekehystä monilähdetietojen keräämiseen ja tietotuotteiden tuottamiseen, ovat hallitusten väliset yhteistyötoimenpiteet tiedonjaon prosessikehitys tavoitetta palvelevine ICT-järjestelmineen ja turvallisine tiedonvälityskanavineen kohdanneet jatkuvasti vaikeuksia. Organisaatiotason viitekehysten kehittäminen on sekä toissijaista että alisteista tiedon yhdistämiselle ja jakamiselle, jonka pääperiaatteena on toteuttaa tarkan, luotettavan, ajanmukaisen ja arvoa tuottavan tietojen saatavuus. EU:ssa tämän tehdään mahdolliseksi lainsäädännöllä, tinkimättömällä poliittisella tahtotilalla, tiedon turvaamisella, uhkahavainnoimisella ja -arvioimisella sekä keskinäisellä luottamuksella. Gruszczak (2022) toteaa, että tiedon yhdistelyn (engl. data fusion) ja monilähteisyyden (engl. all-source analysis) konsepti voi luotettavasti toteutua vain yhteisissä yhteistyöelimissä, joissa jatkuva tietovirta, tiedonkäsittely ja -jalostus, analytiikka ja tietotuotteistus toteutuessaan palvelevat kaikkia sidosryhmiä jäsenvaltiotasolla.

Uudet teknologiat tuottavat etuja ja kyvykkyyksiä eri sidosryhmille. Csernatori ja Martins (2023) tarkastelevat turvallisuuden ja puolustuksen murrosteknologiakäsitettä ja murrosteknologioihin liittyviä viitekehyksiä ajallisuuden, suorituksellisuuden ja kuvailevuuden näkökulmista. He toteavat, että pyrkimys uhkien havaitsemiseen sekä julkisella että yksityisellä sektorilla on lisääntymässä sekä kansallisen turvallisuuteen liittyvistä että

strategisista syistä. Havainnointi asettaa vaatimuksia teknologioiden ajalliselle ja nopeutta tuottaville kyvykkyyksille erityisesti sotilaallisessa ja puolustuksellisessa käytössä, jossa ne lisäävät taistelukapasiteettia. Tekoäly, automatisoidut järjestelmät, kvanttilaskenta sekä kaaos- ja kompleksisuusteorioiden soveltaminen muokkaavat sodankäyntiä aiempaa tieteellisemmäksi. Heidän mukaansa tarvitaan monialaista ja poikkitieteellistä tarkastelua teknologiaymmärryksen kasvattamiseksi muuttuvassa sosiaalisessa, poliittisessa ja teknologiaympäristössä. (Csernatori & Martins, 2023)

Murrosteknologiat ovat saaneet jalansijaa turvallisuuden lisäksi myös maapallon tutkimisessa. Nitoslaswki ym. (2021) tarkastelevat teknologioiden käyttöä puiden, metsien ja metsäekosysteemien muutosten havainnoinnissa, kuten mm. miehittämättömien ilmaalusten kamera- ja tutkavalvontaa, satelliittikuva-analyysia ja erilaisia sensoriteknologioita. Näiden keräämää suurta tietomassa (big data) käsitellään koneoppimistyökaluilla ja tuloksia hyödynnetään mm. metsänhoidollisissa ja puunkorjuutoimenpiteissä. Virtuaaliympäristöillä tuotetaan näkyviin ihmisen ja luonnon välistä vuorovaikutusta sekä havainnollistetaan ympäristön tilaa ja mahdollista tarvetta suunnitteluun ja muokkaukseen. Tutkijat toteavat, että useilla eri teknologioilla suoritetulla tiedon keruulla ja yhdistämisellä moniin eri lähteisiin on paljon mahdollisuuksia digitaalisessa metsänhoidossa, mikäli tietojen keruuta voidaan joukkoistaa esim. avoimeen lähdekoodiin perustuvilla alustoilla. Uusien teknologioiden käytössä tulee huomioida haasteet tiedonhallinnan näkökulmasta sekä datan laadusta ja tarkkuudesta tiedon vääristymien torjumiseksi. (Nitoslawski ja muut, 2021).

Terveysuhista havaintoja keräävät sekä kansan, kansallisen ja kansainvälisen turvallisuuden yhteen kytkevät epidemiatietokeskukset (Epidemiological Intelligence Fusion Centers) lisäävät terveysturvallisuutta, toteavat Albert ym. (2023) julkaisussaan. Tässä avointen lähteiden tietojen keruu (engl. open-source intelligence OSINT) mm. sosiaalisesta mediasta ja signaalitiedustelu (engl. signal intelligence SIGINT) mm. teleliikenne- ja sijaintitiedoista ovat tarkoituksenmukaisia menetelmiä, mutta niiden soveltamisessa tulee

ottaa huomioon esim. yksityisyydensuojaan liittyvät juridiset ja eettiset rajoitteet. Paikallisen datan keruulla ja paikallisen tiedon ymmärtämisellä on merkittävä osuus kokonaistilannekuvan muodostamisessa. Monilähteinen tietojenkeruu edellyttää myös tiedon käsittelijöiltä ja analysoijilta monialaista ymmärrystä, osaamista ja organisaatiorajat ylittävää verkostoitumista. Tiedon yhdistäminen (engl. information fusion) tiedusteluanalyysin kontekstissa vaatii tiedon inhimillistä muuntamista esitettävään muotoon päätöksentekoa varten, jotta uhkien torjuntaa voidaan toteuttaa. (Albert ja muut, 2023)

Datafuusioteknologioita voidaan hyödyntää myös luonnonympäristön lisäksi kulttuuriperintöympäristöjen muutosten havaitsemiseen geospatiaalisen mallinnuksen avulla. Lercari ym. (2019) julkaisussa korostuu tekninen tiedonkeruu sensoreiden avulla, jossa inhimillistä tulkintaa tarvitaan aiemman digitaalisen ja analogisen aineiston yhdistämisessä uusilla teknologioilla tuotettuun eri tyyppisiin data-aineistoihin. Yhdistämisestä syntyy uutta aineistoa, josta voidaan tulkita uusia havaitsemisen ja seurannan tarpeita. (Lercari ja muut, 2021)

Karagiannopoulou ym. (2022) tarkastelevat datafuusiota ja ihmisen vaikutusta maapallon tarkkailun (Earth Observation) konteksissa. Julkaisussa mainitaan käsite kansalaistiede (Citizen Science), jolla tarkoitetaan kansalaisten roolia aktiivisina tiedon tuottajina ja osallistujina esim. ilmastonmuutoksen torjuntaan. Tutkijat kävivät läpi joukkoistamisen välineinä käytettyjä verkkoalustoja ja -työkaluja, joihin yksittäinen ihminen tai kansalaisryhmä voi vapaaehtoisesti tuottaa tietoa esim. ilmanlaadun mittaustuloksina tai muina maantieteellisinä havaintoina. Havaintojen tekemisen apuna voi käyttää kuluttajien saatavilla olevia sensoreita, joita jo on älypuhelimissa. Kansalaisen rooli voi kasvaa datan kerääjästä ja yksipuolisesta tuottajasta tieteellisen projektiin osallistuvaksi aktiiviseksi toimijaksi. Datan laatu on välttämätöntä todentaa ja tutkijat mainitsevatkin laadun vaihtelevan datasta, datalähteestä ja siihen sovellettavasta validointimenetelmästä riippuen. (Karagiannopoulou ja muut, 2022)

Daskalakis ja muut (2022) ryhmittelevät datafuusiojärjestelmät neljään tuotetiedon, taloustiedon, liiketoimintatiedon ja asiakastiedon pääluokkaan tarkastellessaan verkkokauppatoiminnan monilähteisen tiedon yhdistämisen ratkaisuja. Alaluokkiin kuuluvat mm. kysynnän ennustamisen ratkaisut, toimituksen optimointitoiminnallisuudet, talousriskien ja hinnan ennustamisen sovellutukset, petostentorjunnan toiminnallisuudet sekä muut erilaiset kuluttajakäyttäytymistä ennustavat ratkaisut. Koneoppimismenetelmiä hyödynnetään erityisesti talousrikosten ja taloudellisten riskien ennustamiseen. Verkkokaupassa (e-commerce) tiedon tulkitaan usein olevan epätarkkaa ja epäluotettavaa, jolloin datafuusiojärjestelmissä tulee hakea tiedon laatua parantavia ratkaisuja. Suurien tietomassojen analysointi palvelee liiketoimintatiedustelua, jolla varmistetaan toimijoiden elinkelpoisuus globaalissa markkinataloudessa tuottamalla kyvykkyyttä ennakoida kilpailijoiden, toimittajien, asiakkaiden, teknologioiden, hankintojen, markkinoiden sekä tuotteiden ja palveluiden tilaa liiketoimintaympäristössä. (Daskalakis ja muut, 2022)

Tutkijoiden (Daskalakis ja muut, 2022) näkökulma on tässäkin teknologiapainotteinen ja ihmisen toimintaa kuvataan päätöksenteon vaiheeseen liittyvänä, eikä niinkään tietosignaaleja ympäristöstä vastaanottavana ja havaitsevana. Datafuusiomalli voidaan esittää myös datan, tiedon ja tietämyksen ulottuvuudet (knowledge-information-data-fusion) yhdistävänä kehyksenä, jossa inhimillisen kokemuksen ja asiantuntijuuden sekä sosiaalisen ja kulttuuriympäristön tuottama tieto huomioidaan omina tietovirtoinaan mukaan fuusiokokonaisuuteen. Kattava kehysmalli soveltuu erityisesti talouden, rahoituksen, johtamisen ja ympäristön toimialoille tilanneymmärryksen luomiseen ja toimintaympäristön muutosten ennakointiin. Verkkokaupan alalla sovelletaan myös reaalimaailman kuluttajakäyttäytymisestä saatavia tietoja, joita yhdistetään käyttäjän toimintalokitietoihin kybermaailmassa, ja näin toimimalla käännetään psykologinen malli laskennalliseksi palvelualustan suosittelutoiminnallisuudessa hyödynnettäväksi malliksi. Inhimillisen toiminnan tuottamia tietoja voidaan hyödyntää sekä tietovirran alkupäässä olevana raakadatana (kuluttajakäyttäytyminen, ostovalinnat ymv.) että asiantuntijakatselmointina fuusiojärjestelmässä käytettyjen laskentamallien tulosten käsittelyssä (validointi) ja mallikehityksessä. (Daskalakis ja muut 2022)

Eri sovellutusalat tarvitset tukea viitekehyksistä ja arkkitehtuureista. Becerra (2021) tarkastelee tietojen yhdistämistä tiedon laadun näkökulmasta analysoimalla datafuusion viitekehyksiä, malleja, arkkitehtuureja, vaatimuksia ja teknisiä prosesseja. Datafuusiomallit voidaan luokitella dataan, toimintaan ja rooleihin pohjautuviin malleihin, joista mm. SAWAR (Situation Awareness) ensiksi mainituista korostaa ympäristön tilan havainnoinnissa tilannetekijätietojen yhdistämistä inhimillisestä ja tietosisältönäkökulmasta tilannetietoisuuden saavuttamiseksi, ja voi siten kuulua tarkastelunäkökulmasta riippuen kaikkiin kolmeen luokkaan. Suosittu JDL korostaa dataan pohjautuvaa tietojenkeruuta ja tietojen yhdistämistä teknisestä, eikä inhimillisestä näkökulmasta, eli esim. sensoreiden avulla. OODA (Object-Orient-Decide-Act) voidaan luokitella toiminnalliseksi malliksi ja OTO (Oriented to Object) edustaa roolinäkökulmaa tietojen yhdistämisessä. Tiedon laadulla on suuri merkitys datafuusiojärjestelmän tiedon käsittelyn varmuuteen, tarkkuuteen ja tehokkuuteen, ja tutkija tunnistaakin useita eri menetelmiä ja metriikoita tiedon laadun arviointiin niissä. Useissa malleissa, lukuun ottamatta JDL-mallia, tiedon laadun arviointi ei suoraan sisälly malleihin. JDL-mallissa tiedon laatu kuvataan tiedon yhdistämisen prosessien, tietosisällön, tilanteen, lähteiden ja lähteen tietomallin, päätösten ja toimien sekä tiedon esittämisen ja visualisoinnin laatuna. (Becerra, 2021)

Heidän mukaansa Blaschin (2006) kehittämä JDL-malli on datakeskeisempi ja alhaalta ylöspäin etenevä verrattuna Endsleyn (1997) malliin. JDL-mallissa tilannearviointi perustuu eri asioiden (muuttujat; tekijät) keskinäisten suhteiden ja vuorovaikutuksen tarkastelulle, kun taas Endsley etenee havainnoinnin, ymmärryksen ja ennakoinnin päätoiminnallisuuksista tulkinnan kautta päätöksentekoon. Nazir & Han (2022) mainitsevat myös muita tiedon yhdistämisen malleja, kuten mm. tiedustelun, Boyd'n, Dasarathy'n, Omnibus'n ja OODA-mallin sekä havaintoihin pohjaavia assosiatiivisia ihmisen ajattelua matkivia päättelymalleja. He kuvaavat kuitenkin em. JDL-mallin olevan kaikkia muita tuloksellisempi tiedon yhdistämisessä, sillä se perustuu kohteen, tilanteen, riskien ja prosessien tarkentamiseen, jossa jokainen taso kerryttää tietoa edelleen seuraavalle tasolle

päätöksentekoa varten. Nazir & Han (2022) jatkavat, että eri malleilla on kuitenkin tilannetietoisuuteen, mallin kehämäisyyteen ja prosessien toistuvuuteen sekä palautteeseen liittyviä yhteneväisyyksiä.

Zhang ym. (2023) tarkastelevat verkkoturvallisuuden tilannekuvajärjestelmien kehitystä sekä teknologioita ja toteavat havainnointivaiheessa hyödynnettävän eri tutkimus- ja seurantamenetelmiä haavoittuvuuksien, verkkoon tunkeutumisen, haittaohjelmien ja järjestelmälokien dataan. Tutkijat määrittelevät havainnointivaiheen osaksi myös tunkeutumisen testauksen (penetration testing) sekä tapahtumahallinnan ja auditoinnin löydösten tarkastelun. Verkkoturvallisuuden tiedonhankinta kohdentuu haavoittuvuus-, hälytys-, hyökkäys-, tapahtuma- ja tilannedataan sekä monilähteiseen turvallisuusinformaatioon, joiden tietojen yhdistäminen toimii perustana moniulotteiselle korkean tason tilannetietoisuudelle. Julkaisussa kiinnitetään huomiota myös tiedon visualisoinnin tärkeyteen osana kattavan tilanneymmärryksen muodostumista. (Zhang ja muut, 2023)

Verkkoturvallisuuden tilannekuva perustuu suurten datamassojen tiedonkeruulle, kuten Wang ym. (2023) toteaa. Useimmissa tilannetietoisuuden malleissa tiedonkeruu kuvataan teknisenä havainnointina sensoreiden ja teknologisten aistimien avulla. Julkaisussa viitataan Tim Bass'n malliin (1999), jossa inhimillinen toiminta toteutuu analyysina ja tilan todennuksena vasta ylimmällä tiedon käsittelyn tasolla (data -> informaatio -> tietämys). Verkkoturvallisuuden uhkien lisääntyessä tutkimustoimintaa tulee laajentaa uusille alueille teknologiakehityksen myötä sekä kiinnittää huomiota tiedon visualisointiin järjestelmien käyttäjien tietoisuuden ja ymmärryksen edistämiseksi. (Wang ja muut, 2023)

Uhkien havainnoinnin edellyttää kykyä niiden vaikutusten ja todennäköisyyksien arviointiin, jolloin niistä voidaan tunnistaa riskejä (Thiele, 2020). Tässä sille, mitä emme vielä tiedä ettemme tiedä (unknown unknows), ei voida tunnistaa dataa tai tietokokonaisuuta, eikä myöskään siihen perustuen voida esittää kysymyksiä tai tehdä mallinnuksia puuttuvien syy-seuraussuhteiden hahmottamisen vuoksi. Uhkien yksiulotteisen ennustamisen

asemasta tulee pyrkiä ennakoimaan eri tilanteita, tapahtumapolkuja ja mahdollisuuksia ja ottamaan huomioon epävarmuustekijät. Thiele lainaa Eisenhoweria (1957) esittämällä sitaatin ”Suunnitelmat ovat arvottomia, mutta suunnittelu on kaikki kaikessa” pyrkiäkseen osoittamaan joustavan ennakoinnin hyödyn. Inhimillisen työpanoksen ja asiantuntijamenetelmien sijaan ennakointia tullaan enenevässä määrin toteuttamaan datapohjaisesti tekoälytyökaluilla. Tästä huolimatta paras tulos saadaan aikaan yhdistämällä inhimillinen osaaminen koneella luotuun kyvykkyyteen. Thiele (2020)

Eräänä kyberturvallisuuden tutkimusalueena on havainnointi ja trendien ennustaminen. Li’n ym. (2019) luomassa loogisessa analyysiviitekehyksessä tietojen keruu ja päättely esitetään kattavana koko turvallisuusympäristöä koskien, päinvastoin kuin perinteinen tapahtumapohjainen analytiikka. Yksittäisten turvallisuustapahtumien analyysitulokset muodostavat siten vain osan useita tietovirtoja hyödyntävästä verkkoturvallisuuden tilannekuvasta. Kyberturvallisuuden tilannetietoisuuden muodostaminen nojaa vahvasti lukuisiin erilaisiin teknisiin tietoihin (esim. IP-osoitteet ymv.) pohjautuviin havaintoalgoritmeihin ja inhimillisen havainnoinnin osuutta ei juurikaan tarkastella alan tutkimuksissa. Tutkijat toteavatkin turvallisuuden olevan lähinnä suurten datamassojen (big data) analysoinnin ongelma, joka ratkaistaan pohjautuen laskenta- ja teknologiakapasiteettiin sekä automaattiseen päätöksentekoon. Koneen näkökulmasta mallien tunnistamiseen (pattern recognition) perustuva havaintoprosessi käynnistyy silloin, kun tekijäindeksijoukon X ja havaintotulosjoukon Y välistä suhdetta ei voida määrittää funktion tai loogisen päättelyn avulla. Ihmisen havainnointikykyä käsitellään lähinnä analyysitulosten visualisoinnin yhteydessä, jossa abstraktiset mallit ja kielelliset ilmaisut esitetään graafisesti asioiden ja niiden tilan luontaisen merkityksen tarkentamiseksi sekä kognition parantamiseksi. Tutkijat korostavat, että tilannekuvajärjestelmän suunnittelussa (design) tulee noudattaa ohjelmistokehityksen periaatteita havaitsemiseen liittyvien inhimillisten käyttäjätarpeiden sekä ihmisen ja koneen välisen vuorovaikutuksen (human-machine interaction) toteutumiseksi. Pyrkimyksenä on tuottaa havainnointitulos mahdollisesta uhasta ennen kuin se toteutuu lauenneena riskinä. (Li ja muut, 2019)

Dorsser'n ja Taneja'n julkaisussa (2019) tuodaan esiin havaitsemisen mahdollistaman ennakoinnin tuottaminen megatrendeistä ja epävarmoista kehityskuluista. He mainitsevat STEE(EE)P-mallin, jossa yhtenä trendien tarkastelun ulottuvuutena tai teemana voidaan käyttää energiaa (energy). Mallin avulla voidaan seurata esim. energian tuotantoa ja kulutusta, energiatuotteita ja mitä tahansa energiaan liittyviä tapahtumia, kuten energiakriisejä, ja näin saada kuvaa vuosikymmenten tai satojen vuosien energia-alaan liittyvistä kehityskuluista. Ennakoinnin tuottamiseksi ja siten tuleviin tapahtumiin ja muutoksiin varautumiseksi on oleellista muodostaa ymmärrys tarkastelukohteiden suhteista ja riippuvuuksista toisiinsa, esim. energiantuotannon talous-, ympäristö- tai sosiaalisista vaikutuksista, tai poliittisista jännitteistä tai teknologiaomavaraisuudesta jne. Inhimilliseen toimintaan liittyvänä mahdollisena tulevana kehityskulkuna tutkijat mainitsevat myös bioniikan tulevaisuudenkuvana kyborgimaisen ihmisen aivojen kytkeytymisen lisättyihin aistimispalveluihin edistyneiden sensoriteknologioiden avulla, jolloin fyysinen, biologinen ja digitaalinen tieto yhdistyvät verkossa. (Dorsser & Taneja, 2019)

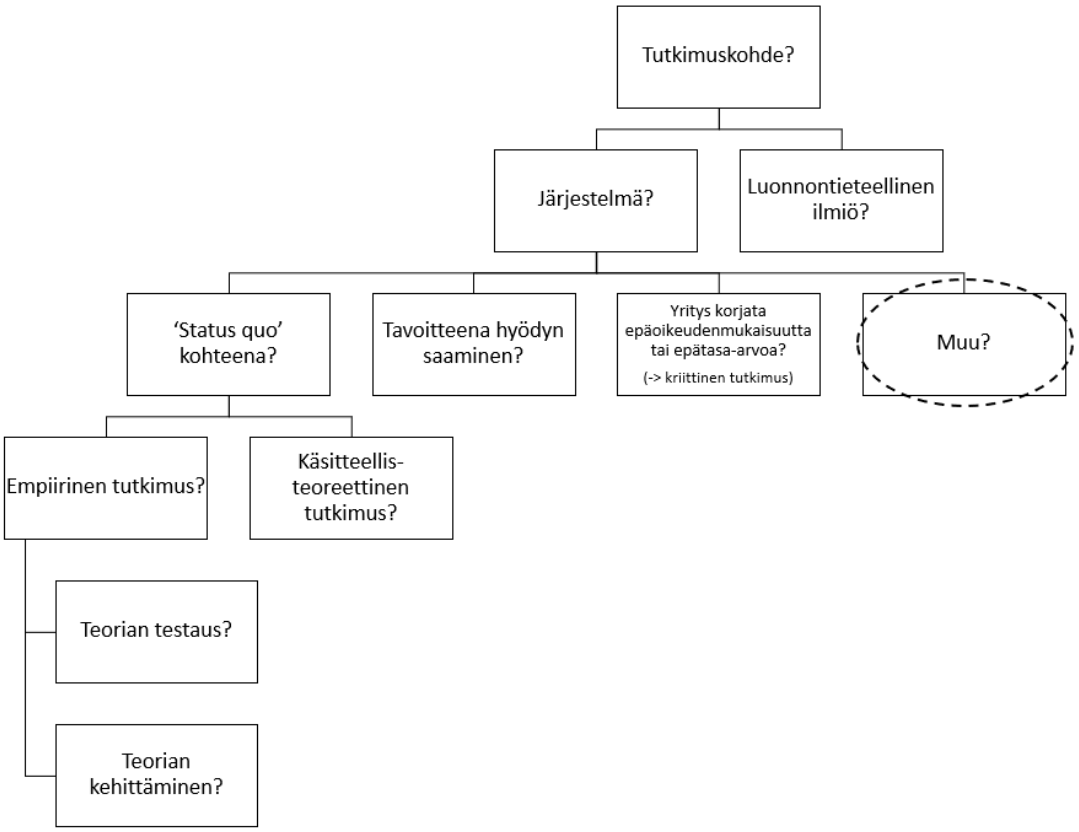
Edellä kuvattua tukee myös Peters ym. (2020) nostamalla esiin bioinformatiikan ja biologian digitaalisena informaationa, joka luo uutta teknotieteellistä tietoekologiaa. Tutkijat esittelevät biodigitaalisen tiedon lähentymisen käsitteen, jossa syntyy uusia hybridejä elämänmuotoja sulauttamalla teknologioita eliöihin tai parantamalla niiden olemassa olevia kyvykkyyksiä lisäominaisuuksilla. Tämä johtaa uudenlaisen kriittisen infrastruktuurin muodostumiseen, kun orgaaninen muoto yhdistyy digitaaliseen muotoon bioteknologisessa fuusiossa tällä ns. jälkidigitaalisella aikakaudella. (Peters ja muut, 2020)

Luis ym. (2021) puolestaan toteavat, että yhdistetty tulevaisuuden ja riskien hallinta tukee organisaatioiden kykyä strategiseen päätöksentekoon epävarmuuksien vallitessa. He käyttävät tapausesimerkkinä Portugalin suurinta vesilaitosta, jonka tietoutta epävarmuuksista, kyvykkyyttä arvioida ulkoisten kehityskulkujen vaikutuksia omaan toimintaan ja kykyä sopeutua tulevaisuuden muutoksiin parannetaan toisiinsa liittyvällä strategisella riskiarvioinnilla ja tulevaisuuden skenaariosuunnittelulla. Skenaarioanalyysissa ensimmäisenä tavoitteena on kuvata ne uskottavat tapahtumakulut, jotka tarjoavat riittävän

laajan lähtökohdan riskien arviointiin ja testaukseen. Tähän jatkotavoitteena on saada käsitys riskien seurausten laajuudesta ja riskienhallinnan toteutumisen riittävyydestä erilaisissa tulevaisuuksissa, jotta organisaatio saavuttaa resilienssin moninaisten strategisten riskien kehittymiselle. Tulevan ymmärrys muodostetaan tosiseikkoihin koskevien todisteiden avulla, asiat kattavasti ilmaisevalla tai todentavalla asiantuntijatietämyksellä sekä yleisellä havainnoinnilla. Julkaisussa ei kuitenkaan kuvata tarkemmin havaintodatan hankintaa. Tutkijat esittelevät tapahtuma-altistus-haitta -mallin (event-exposure-harm model), jossa tapahtumia voivat olla esim. metsäpalot, saastuminen, hävikki, pandemia tmv. Tapahtumat aiheuttavat seurauksia esim. tuotteen laadun heikkenemisenä tai kontaminoitumisena tai kysynnän kasvuna, jotka puolestaan tuottavat haittoja esim. tuotteen jakelussa tai myynnissä, ja muodostuvat organisaation strategisiksi esim. toimintaan tai maineeseen liittyviksi riskeiksi. (Luis ja muut, 2021)

3 Teoriapohjainen tutkimuskohteen määrittely menetelmänä

Tutkielman tavoitteena on yleisen uhkatietouden tuottamisen lisäksi tuoda esiin tiedonhallinnallisen järjestelmätuotteen kehittämisessä tarvittavia uhkien havaitsemiseen liittyviä seikkoja ja edellytyksiä. Tämän mukaisesti tutkimusmenetelmää voidaan tarkastella seuraavan, tutkimuksen suuntautumista kuvaavan kuvion avulla. Kuviossa liikutaan ylhäältä alas ja vasemmalta oikealle vastattaessa ”kyllä” tai ”ei” jokaiseen kysymykseen. Mikäli taksonomian mukaisesti päädytään kohtaan ”*Muu*” on tutkijan valitsema kohde uusi ja hänen täytyy kehittää uusi tutkimusmetodi. (Järvinen, 2021)



Kuvio 4 Tutkimusmenetelmien taksonomia (Järvinen, 2021)

Tämä tutkielma kohdentuu järjestelmään, eikä luonnontieteelliseen ilmiöön tai totuuteen. Tässä ei tutkita reaalimaailman olemassa olevaa staattista kohdetta tai pysyvää toimintoa, jolloin kuviossa siirrytään eteenpäin. Tavoitteena on tuottaa hyötyä yleisen tason tietämyksen kasvattamisen kautta, mutta kuitenkaan ei kehitetyn tietotuotteen arvioinnin kautta. Tutkielmalla ei myöskään korjata epäoikeudenmukaisuutta, eikä siinä hyödynnetä sosiaalitieteiden teorioita tai käsitteistöjä. Tällöin kuviossa esitetyssä taksonomiassa päädytään kohtaan ”muu”, jolloin määrättyä suositusta tutkimustyypiksi tai metodiksi ei ole (Järvinen, 2021).

Tässä laadullisessa tutkielmassa teoriaa hyödynnetään tulkintojen tekemiseen. Tutkimus voidaan luokitella teoriasidonnaiseksi (Saaranen-Kauppinen & Puusniekka, 2006), sillä siinä pyritään valitun lähde- ja tutkimusaineiston pohjalta hahmottamaan rakenteita ja malleja uhkien havainnointiin liittyvien tietotarpeiden esiin tuomiseksi sekä tuottamaan tutkimusaihetta valaisevia taustatietoja, kontekstia ja esimerkkejä. Tutkimuksessa esiintuotua metatason viitekehikkoa sekä tehtyjä johtopäätöksiä voi soveltaa uusien tietotuotteiden ja järjestelmäratkaisujen kehittämisessä erityisesti kehitysaihioiden tunnistamisen, liiketoimintatarpeiden määrittelyn ja konseptoinnin vaiheissa.

Tutkielman voidaan katsoa edustavan tiedonhallinnallista näkökulmaa. Tiedonhallinnan tutkimus kohdistuu tiedonhallinnan toimintaympäristössä toimijoiden, tiedon, toiminnan ja tiedonkäsittelyllisten sekä viestinnällisten menetelmien ja palveluiden ja niiden välisten suhteisiin, ja on luonteeltaan monitieteellistä ja osin uutta tuottavaa tutkimusta (Kuusisto-Niemi & Saranto, 2009). Tämä tutkielma liittyy uhkatiedon hallinnan kokonaisuuteen.

Toiminnallisten tarpeiden tarkasteluun ja ongelmanmäärittelyyn sovelletaan tässä tutkielmassa suunnittelutieteellistä tutkimusotetta liiketoiminnallisen suunnittelun ja informaatio- ja kommunikaatioteknologian kehittämisen liittyessä kiinteästi toisiinsa (Hevner, Salvatore, Park & Ram, 2004). Tarvetarkastelussa ja ongelmanmäärittelyssä käytetään

tulkintaa, jonka merkitys yleisesti ottaen on lisääntymässä tietojärjestelmätutkimuksessa. Tulkinnallisessa tutkimuksessa tulkitaan ihmisen ajatusta ja käyttäytymistä sosiaalisissa ja organisationaalisissa asiayhteyksissä mm. kielen, tietoisuuden, jaettujen tarkoitusten ja dokumentaation kautta, jotta ymmärretään tietotuotteen tai -järjestelmän sisällön merkitystä ihmiselle ja organisaatiolle. Tutkielmassa pyritään toteuttamaan tulkinnallisen tutkimuksen edellytyksiä kohdekokonaisuuden ja sen osien ymmärtämisessä sekä kohteen kontekstualisoinnissa, yleistämisessä ja kehityskulun hahmottamisessa. (Järvinen, 2021, viittaa Niederman, 2020 ja Klein & Myers, 1999)

Peffersin ja muiden (2008) suunnittelutieteen prosessimallin (engl. DSRM – Design Science Research Model) mukaisesti ongelman määrittämiselle ja sen ratkaisemiselle luodaan siten arvo eli motivaatio perustelemaan tutkimuksen kiinnostavuutta. Parhain motivoiva tekijä on ongelman ymmärrettävyys ja samalla ongelmanratkaisun tuottaman arvon ymmärrettävyys. Tähän päästään tunnistamalla ongelma, määrittämällä se sekä osoittamalla sille merkitys. (Peffers ja muut, 2008)

Tutkielman teossa edetään ongelmanmäärittelyn keinoin aloittamalla siitä, mitä tutkija tietää aihealueesta tutkimuksen tekohetkellä (viittaus mm. ajankohtaisiin uutisointeihin energiasektoria vastaan tehdyistä hyökkäyksistä). Seuraavaksi tunnistetaan se, mitä tutkija ei tiennyt eli mikä oli vielä tuntematonta ja mitä piti selvittää (viittaus kirjallisuuskatsaukseen ja asetettuihin tutkimuskysymyksiin). Tässä yhteydessä todetaan lisätietotarve siitä, miten uhkien havainnointia käsitellään monilähdetietoja yhdistävissä järjestelmäratkaisuissa (viittaus aineistoanalyysiin). Tästä edetään jo tiedetyn ja ei-tiedetyn välille muodostuvien vaikutussuhteiden tunnistamiseen (lähtöoletuksena uhkien monitahoisuus ja laaja ulottuvuuskenttä suhteessa havainnointiin). Ongelmanmäärittelyprosessin tulokseksi tavoitellaan päätelmää siitä, miten tiedustelullisella ja ennakoivalla havaitsemisella voitaisiin torjua uhkia tietojenkäsittelyllisin ja viestinnällisin keinoin.

Tässä tutkielmassa edellä kuvatut ongelmanmäärittely ja tulkinta kuvastuvat uhkamäärittelyn ja uhkien merkityksen tarkastelun kautta. Energiatoimialan ajankohtaisia turvallisuustapahtumia seuraamalla voidaan päätellä uhkien ilmaantumiseen vaikuttavia taustatekijöitä. Tutkimusaineistoa läpikäymällä voidaan tehdä johtopäätöksiä siitä, miten uhkahavainnointia tarkastellaan ja määritellään useasta eri lähteestä tietoja tuovien ja koostavien ICT-ratkaisujen tieteellisissä tutkimuksissa.

Tutkielma suuntautuu myös kuvaavaan ja ennakoivaan tutkimukseen, jossa ensiksi mainittu tavoittelee informaatio- ja kommunikaatioteknologian luonteen ymmärtämistä ja jälkimmäinen ICT:n tehokkuuden parantamista. Suunnittelutiede puolestaan keskittyy suunnittelun kohteena olevan tuotteen muotoiluun siten, että tuotteen avulla päästään asetettuihin toiminnan tavoitteisiin ja että tuote tuottaa arvoa sekä hyötyä. Tämä saavutetaan kahdella ulottuvuudella, joista ensimmäinen kattaa tuloksena olevan tuotteen rakenteistamisen ja mallinnuksen ja toinen näihin liittyvät teorioinnin, arvioinnin ja oikeutuksen toiminnot. (Järvinen, 2021, viittaa March & Smith, 1995)

Edellä mainitulla ensimmäisellä eli tuotteen rakenteistamisen ja mallinnuksen ulottuvuudella on yhteys tässä tutkielmassa esitettyyn katsaukseen teknologisesta kyvykkyydestä. Viidennessä pääluvussa tarkastellaan tämän mukaisesti uhkatiedon hankintaan ja analysointiin liittyviä kyvykkyyksiä sekä järjestelmätuotteen kehittämisessä huomioitavia seikkoja.

Tutkielma ottaa vain epäsuorasti kantaa edellä mainittuun ICT:n tehokkuuden parantamiseen tuomalla esiin uhkien havaitsemiseen liittyvää tiedonjakoa, jolloin sivutaan myös suunnittelutieteellistä ulottuvuutta. Suunnittelutieteessä sovelletaan positivistisia oletuksia tutkimuskohteeseen, kun tavoitteena on hyödyn kuvaaminen ja saaminen. Suunnittelutieteellisessä tutkimuksessa hyödynnetään usein viitekehystä (Hevner, Salvatore, Park & Ram, 2004), jossa tutkimuksen tavoitteena tulee olla elinkelpoinen tuotos (eng. design as an artifact), johon liitetyn teknologian avulla liiketoiminnan ongelmia voidaan

ratkaista (engl. problem relevance). Viitekehyksen ympäristö muodostuu ihmisistä, organisaatioista ja organisaatioiden hyödyntämästä teknologioista. Organisaation tarpeet saadaan esille tarkastelemalla organisaation ominaisuuksia, liiketoimintaprosesseja, strategioita, rakenteita ja toimintakulttuuria. (Hevner, Salvatore, Park & Ram, 2004)

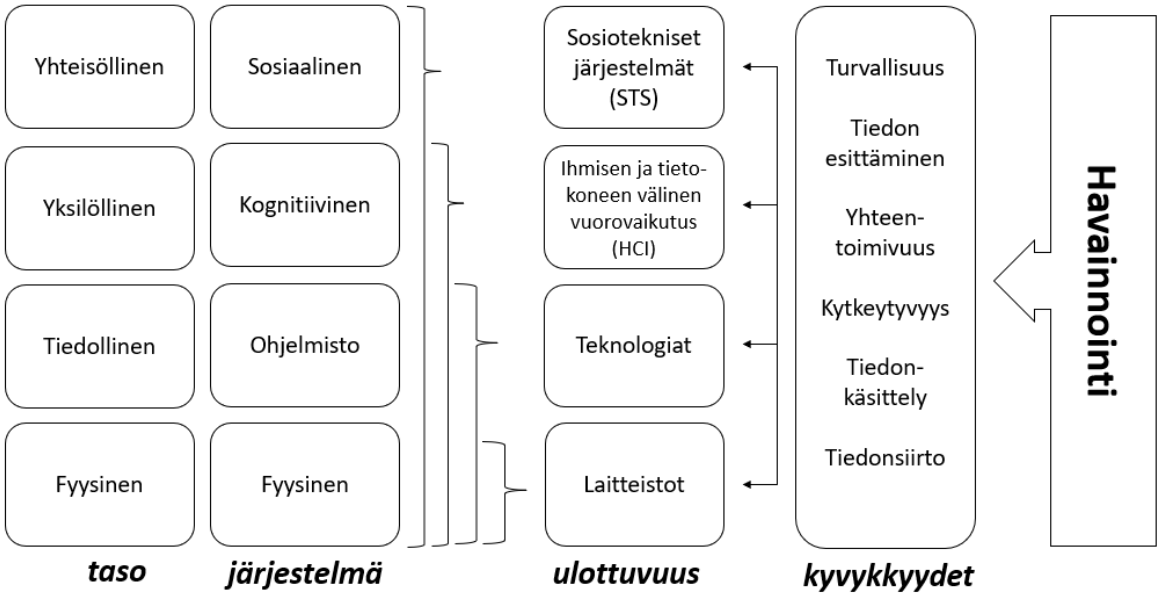
Edellä mainitun organisaation toimintaympäristön ongelmia ratkaisevan tuotoksen tutkimuksessa täytyy soveltaa sekä kehittämisen ja rakentamisen ensimmäisessä päävaiheessa että oikeutuksen, perustelun ja arvioinnin toisessa päävaiheessa hyväksyttävissä olevia tutkimusmenetelmiä (engl. research rigor), jotta ongelmanmäärittely- ja -ratkaisu voidaan toteuttaa (engl. design as a search process) (Hevner, Salvatore, Park & Ram, 2004). Järvinen (2021) haastaa viitekehyksen ja ehdottaa täydennyksenä rakentamisprosessin kuvaamista lähtötilavaiheineen, rakentamisvaiheineen ja tavoitetilavaiheineen.

Tässä kuvatun mukaisesti tämä tutkielma keskittyy Järvisen (2021) ehdottamaan lähtötilavaiheeseen, jolloin tutkimuksessa tulkitaan toimintaympäristön tapahtumia ja päätellään ympäristöstä syntyviä tietojärjestelmäkehittämisen tarpeita karkealla tasolla. Tutkimuksessa kuvataan yleisesti jatkossa mahdollisesti kehitettävän tietoteknologiatuotteen luonnetta ja ennakoidaan toimintaympäristön tuotevaatimuksiin vaikuttavia muutoksia. Tutkijan kirjallisuuskatsauksestaan saamat havainnot käsitellään ja tunnistetaan kehittämisen lähtötila niiden pohjalta. Tutkielma noudattaa siten suunnittelutieteellisen tutkimuksen prosessimallia (Peffers, Tuunanen, Rothenberger & Chatterjee, 2008) ainoastaan sen ensimmäisten prosessivaiheiden osin. Lähestymistapa on ongelma- ja tavoitekeskeinen, jolloin tutkimuksessa keskitytään ongelman tunnistamiseen ja motivointiin sekä tavoitteiden tarkasteluun. Toisessa pääluvussa esitetyn kirjallisuuskatsauksen sekä neljännessä ja viidennessä pääluvuissa esitettyjen esiehtojen, vaatimusten ja huomioiden pohjalta voidaan muodostaa ongelmanmääritystä, motivointia sekä esimerkinomaista laadullista tavoitteidenmäärittelyä.

Peffersin, Tuunasen, Rothenbergerin ja Chatterjeen (2008) suunnittelutieteen tutkimuksen prosessimallissa edetään päättelyn, teorioinnin, tietoisuuden ja analysoinnin kautta

kurinalaisen tietämyksen kehittymiseen. Prosessi käynnistyy ongelman tunnistamisella, sen määrittelyllä ja motivoinnilla, mistä edetään ratkaisun tavoitteiden määrittämiseen. Tavoitteet voidaan esittää laadullisina siten, että niillä kuvataan se, miten suunnittelutuote ratkaisee havaittuja ongelmia. Vasta tämän jälkeen, kun on saatu määritettyä se, mitä halutaan, voidaan edetä tuotteen suunnitteluun ja kehitykseen. Tuotteen ensituotos esitetään (demonstrointi) ja testataan. Tämä tuotos ja sen tulos arvioidaan ja lopulta aikaansaannoksesta viestitään tieteellisessä ja ammatillisessa kontekstissa. Prosessi on iteroituva eli suunnittelun, arvioinnin ja viestinnän vaiheista voidaan tarvittaessa palata tavoitteiden määrittelyyn ja tuotteen suunnitteluun. Tutkimus voidaan suunnata ensimmäisen prosessivaiheen ongelmakeskeisyyteen, toisen prosessivaiheen tavoite- ja ratkaisukeskeisyyteen, kolmannen prosessivaiheen suunnittelukeskeisyyteen tai neljännen prosessivaiheen asiayhteyden toteutumiseen tuotetta käytettäessä asiakasympäristössä. (Peffers, Tuunanen, Rothenberger & Chatterjee, 2008)

Huolimatta siitä, että tässä tutkielmassa ei tuoteta varsinaista tavoitteidenmäärittelyä (vaatimusmäärittely), eikä siten edetä tuotteen testaukseen tai arviointiin, pyritään tutkielmassa tuomaan esiin asiayhteyttä toimintaympäristöön. Suunnitteluprosessissa suunniteltavan tietotuotteen asiayhteys (Hevner, Salvatore, Park & Ram, 2004) kumpuaa sosiaalisteknisestä ympäristöstä, jossa sovellusalueina ovat ihmiset, organisaatio- ja tekniset järjestelmät sekä ongelmat ja mahdollisuudet. Tutkielman keskittyessä edellä kuvattuun lähtötila- ja ongelmanmäärittelyvaiheisiin, pyritään asiayhteys mahdolliseen tietotuotteeseen luomaan sosioteknisen järjestelmän tiedollisen tarkastelun kautta (Appelbaum, 2014) suhteessa energia-alan toimijan vuorovaikutukseen toimintaympäristössään. Tietovirtoja tulkitaan sosiaalisten ja teknisten tarpeiden kohteina. Kehittämisongelman lähtökohtana on tietojen saatavuus toimintaympäristöstä, jolla tuetaan organisaation strategisen, taktisen ja operatiivisen päätöksenteon sekä suunnittelun prosesseja.



Kuvio 5 Sosioteknisen järjestelmät (mukaillen Whitworth, 2010) ja tutkimuskohde

Sosioteknisellä järjestelmällä tarkoitetaan teknologisiin ratkaisuihin perustuvaa monimutkaista ihmisten, koneiden ja ympäristöjen välistä vuorovaikutusjärjestelmää, kuten esimerkiksi erilaisia energiantuotannon järjestelmiä (Tieteen termipankki, 2016). Tieto- ja viestintäteknisen järjestelmän vaatimukset tai toiminnallisuudet voidaan luokitella fyysisiin, tiedollisiin, käyttäjäkohtaisiin tai yhteisöllisiin; nämä yhdessä muodostavat sosioteknisen ytimen. Pelkän energian ja datan välityksen lisäksi järjestelmässä välitetään yhteisöllisiä normeja, sääntöjä ja merkityksiä. Järjestelmän kontekstin laajetessa myös sen suorituskyvyn oletetaan kehittyvän edetessä alemmalta tasolta kohti ylempää tasoa. (Whitworth, 2010)

Tutkimuksen tiedollinen konteksti uhkateemoineen pohjautuu turvallisuustieteisiin, joiden tutkimus on usein monitieteellistä, laaja-alaista ja poikkileikkaavaa. Erityiset turvallisuustieteet tarkastelevat turvallisuuden tilaa toimija- ja toimintotasolta, jolloin esimerkiksi organisaatiot ja yhteisöt hyödyntävät aineellisia ja aineettomia turvallisuusvälineitä turvallisuutensa ylläpitämiseen (Kitler, 2021).

Tutkielma pohjautuu myös ennakointiin osana tulevaisuudentutkimuksen tai futurologian tieteenalaa. Ennakoinnilla tarkoitetaan päätöksenteon tueksi sovellettavaa tulevaisuudentutkimusta tulevaisuudentutkimuksen ollessa yleinen kattotermi (Malaska, 2013). Tulevaisuudentutkimus voidaan lukea mukaan suunnittelutieteiden kehikkoon luonnehtimalla sitä "suunnittelun uudeksi muodoksi" (Niiniluoto, 1993 ja 2013, viittaa Julien ja muut, 1979). Suunnittelutieteellisen periaatteen mukaisesti tällä tutkielmalla pyritään tuottamaan välineellistä, tavoitteiden ja keinojen välisiä yhteyksiä ilmaisevaa tietoa siitä, miten asioiden (uhkien havainnointi) tulisi olla, jotta tavoitteet (uhkiin varautuminen) saavutetaan (Niiniluoto, 2013). Tutkielmassa tarkastellaan ennakointia osana uhkiin varautumisen kontekstia. Tutkielma ei kuitenkaan suoranaisesti edusta suunnittelua ja päätöksentekoa avustavaa tulevaisuudentutkimusta, sillä tutkielmassa ei tuoteta ennakoivia tai riskianalyyseja tai evaluaatioita (Niiniluoto, 2013). Tieteenfilosofista ja spekulatiivista ilmiötason futurologiaa (Malaska, 2013) tutkielma sivuaa vain kaukaa, sillä aineistoon koostetut reaalimaailman tapahtumat eivät yksinään riitä edustamaan ilmiötason tutkimista.

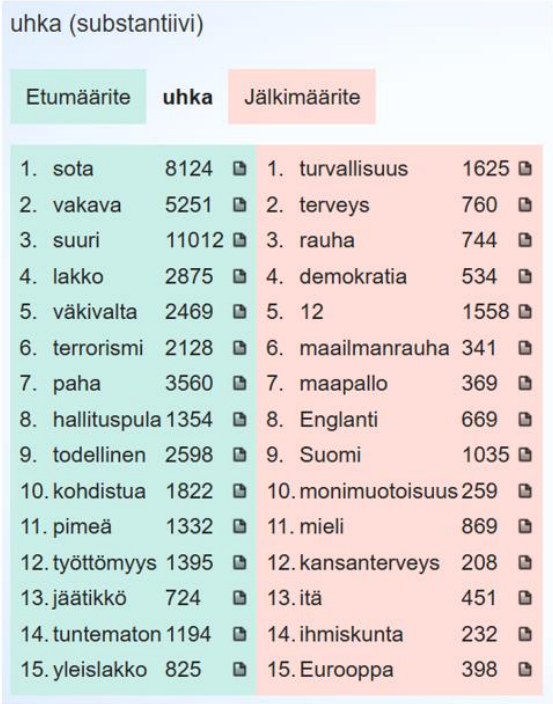
Edeltävässä pääluvussa esitetyn aiemman tutkimuksen katsauksesta saadaan tutkimuksellisiksi avainalueiksi tai teemoiksi seuraavat: turvallisuus, tiedustelu, tietojen tuottaminen, yhdistäminen ja jakaminen, tietoyhteistyö, tiedon ajallisuus, datamassojen käsittely, datafuusiomallit ja tilannetietoisuus sekä uhkaulottuvuudet. Nämä teemat on tiivistetty tutkielman otsikkoon ” Havaintotiedon käsittely toimintaympäristöjen uhkiin varautumisessa”, jolloin ydinkäsitteeksi muodostuu uhka. Uhkamääritelmää kuvataan seuraavassa alaluvussa.

3.1 Uhan määritelmä

Sanastokeskuksen TEPA-termipankin (2024) mukaan uhalla tarkoitetaan mahdollisesti toteutuvaa haitallista epämieluisaa, pelottavaa tai vahingollista seikkaa, tapahtumaa tai kehityskulkua. Vaaran ollessa käytännöllinen ja riskienhallinnallisin toimenpitein käsiteltävissä oleva, on uhka puolestaan luonteeltaan sitä epävarmempi kehityskulku. Termipankki viittaa Sisäministeriön 2023 julkaisemaan sisäisen turvallisuuden sanastoon,

SESKO-standardointijärjestön 2023 julkaisemaan Sähköntuotannon ja -jakelun huoltovarmuuteen liittyvään käsitteistöön, TSK:n 2009 Varautumisen ja väestönsuojelun sanastoon sekä EU:n IATE-termipankkiin 2024. Uhka ilmenee häiriötilanteen, energian huoltovarmuuden. kyberturvallisuuden, yhteiskunnan, kriittisen infrastruktuurin sekä tietotekнologian, tietojenkäsittelyn ja teknisten sääntelyiden käsitekaavioissa ja -suhteissa. (TEPA-termipankki, 2024)

KORP-kielipankista (2024) tehdyllä 862 korpusta sisältävällä haulla uhka-substantiivilla on eniten sotaan ja turvallisuuteen liitettyä käsitesuhdetta, kuten alla olevassa kuvassa esitetään.



Kuva 1 Uhka-käsitesuhteet sanakuvana ja konkordanssiotteena (KORP-kielipankki, 2024)

Yhdysvaltojen sisäisen turvallisuuden viraston määritelmän mukaan uhalla tarkoitetaan mitä tahansa olosuhdetta tai tapahtumaa, jolla on mahdollisuus vaikuttaa haitallisesti organisaation toimintaan, ml. tehtäviin, toimintoihin, mielikuviin tai maineeseen, organisaation varantoihin ja kyvykkyyksiin, organisaation prosesseihin ja toimintaketjuihin,

organisaation jäseniin tai toisiin organisaatioihin ja sidosryhmiin, tai toimialaan ja kansakuntaan. Uhkatapahtuma aiheuttaa potentiaalisesti epätoivottuja seurauksia tai vaikutuksia erityisesti silloin, kun tapahtumat seuraavat ajallisesti perättäisinä jaksoina, sarjana tai tapahtumaketjuina (HSSEDI, 2018). Sisäisten tai ulkoisten toimijoiden toiminta luo uhan, minkä lähteenä voi olla tahallinen vahingoittava toiminta, ei-tarkoituksellinen toiminta (vahinko), rakenteellinen toiminta ja toimintaympäristön toiminta. Jokaisella toimijalla, ml. valtiollisilla, on omanlaisensa kyvykkyydet ja tavoitteet, mikä vaatii vastaavasti myös kohdennetut uhkien ja riskien hallintakeinot. Uhkaa voidaan tarkastella piirretyyppien ja käyttäytymisen kautta, jolloin uhalle pyritään määrittämään sen kohde, tarkoite ja prosessivaiheet sekä siinä käytetyt taktiikat, tekniikat ja menetelmät (HSSEDI, 2018). U.S. National Institute of Standards and Technology liittää riskienhallinnan uhkamääritelmäänsä (2012) myös uhan aiheutumisen tai ilmenemisen tietojärjestelmään tunkeutumisen kautta, tiedon epäämisen tai muokkaamisen kautta tai tietojärjestelmäpalvelun estämisen kautta. (NIST, 2012)

Uhka on tietoon saatettu vahingollinen aie tai teko siinä missä riski on mahdollisuus kokea em. aie tai teko; tästä riippuvuudesta johtuen riskienhallinta kattaa uhkien arvioinnin (RiskIntelligence, 2024). Liiketoiminnassa riskin käsitteellä tarkoitetaan mahdollisuutta kärsiä tappiota tai menettää jotakin taloudellisessa, toiminnallisessa, teknologisessa, tuotokseen liittyvässä tai strategisessa ulottuvuudessa. Strategisilla riskeillä tarkoitetaan laajempaan liiketoimintaympäristöön liittyviä markkina- ja kilpailuasetelmissa, keskipitkän ja pitkän aikavälillä, toimialalla ja toimintaehdoissa ilmeneviä riskejä, joilla on vaikutus toiminnan jatkumiseen ja tuottavuuteen. (MSO, 2014)

Uhkatoimijat ja toiminnan tavoitteet poikkeavat toisistaan satunnaisista onneaan kokeilevista huomionhakuisista hakkereista valtiollisiin toimijoihin ja järjestäytyneisiin rikollisryhmiin asti. Taloudellista hyötyä pyritään saamaan esim. hankkimalla edelleen myytävissä olevaa tietoa eri menetelmillä tai omaa geopoliittista asemaa pyritään vahvistamaan aiheuttamalla taloudellista tai poliittista epätasapainoa. (HSSEDI, 2018)

4 Energiaturvallisuus ja energiatoimialaan liittyviä uhkia

Energiaturvallisuus on energian saatavuutta, energiantoimituksen ja -jakelun keskeytymättömyyttä, energian tuotannon ja kulutuksen tasapainoa sekä markkinahintojen kohtuullisuutta ja kilpailukykyä. Lyhytaikainen energiaturvallisuus kohdentuu energian kysynnän ja tarjonnan muutoksenhallintaan häiriö- ja poikkeustilanteissa. Pitkäaikainen energiaturvallisuus keskittyy investointeihin, joilla turvataan energian toimitus tulevaisuudessa yhteiskunnan infrastruktuurin ylläpitämiseksi ja kehittämiseksi. (Tieteen termipankki, 2015; IEA 2021)

Energiaturvallisuudessa korostuu sen fyysinen, taloudellinen, sosiaalinen ja ympäristöllinen ulottuvuus ulko- ja turvallisuuspoliittisessa, talouspoliittisessa sekä ympäristöpoliittisessa päätöksenteossa (Vainio, 2016). Energiaturvallisuus limittyy muihin turvallisuuden sektoreihin. Poliittisen turvallisuuden kontekstissa on kyse yhteisistä keinoista ja yhteistyöstä, joilla energian tuotanto ja kulutus turvataan. Taloudellinen turvallisuus liittyy mm. energia-alan tuottajayritysten elinvoimaisuuden sekä energian kuluttajien maksukyvyn turvaamiseen. Ympäristöturvallisuutta voi tarkastella energialähteiden ja raaka-aineiden hyödyntämisen kautta ympäristövaikutusten ja kestävän kehityksen viitekehyksessä. Sotilaallista turvallisuutta voi analysoida energiantuotantoon liittyvän geopoliittisen vakauden ja tuotantoalueisiin sekä tuottajiin kohdistuvien vihamielisten valtauksien avulla. Sosiaalinen turvallisuus liittyy sosiokriittisten toimintojen suojaamiseen mm. energiahäiriötilanteissa ja -kriiseissä. (mukaillen Moilanen, 2021a, viittaa Buzan, 2003)

Energiaa pyritään turvaamaan sen kaikissa ilmenemis- ja sidossuhteissaan. Energian saatavuus on välttämätöntä toimivalle yhteiskunnalle. Energian tarjontaan ja toimittamiseen kohdistuu useita haasteita sen rajoittuneen varastointimahdollisuuden ja jatkuvan tarpeen vuoksi. Euroopan unionin vauraus ja turvallisuus riippuvat vakaasta ja riittävästä energiansaannista. Euroopan unioni tuo hieman yli puolet kulutetusta energiasta ja tämä korostaa tarvetta varmistaa sietokyky äkillisiin energiansaannin häiriöihin, sekä suojata strategisia infrastruktuureja. Energiainfrastruktuurit ovat osa suojattavaa kriittistä infrastruktuuria. 2008 annetulla direktiivillä (2008/114/EY) ohjataan yhteisön jäsenmaita

tunnistamaan elintärkeät infrastruktuurit ja parantamaan niiden suojausta, varautuman riskeihin sekä varmistamaan tietoteknistä turvallisuutta. (Euroopan komissio, 2014 ja 2016).

Integroidut energiamarkkinat ja -järjestelmät edellyttävät EU-mailta tiivistä yhteistyötä sähkökriisien ehkäisemisessä ja hallinnassa. EU :n asetuksessa 2019/941 (4.7.2019) sähköalan riskivalmiudesta vaaditaan EU:n jäsenvaltioita tekemään yhteistyötä keskenään sen varmistamiseksi, että sähkökriisissä sähkön toimitus varmistetaan sen käytön tarpeen mukaisesti eli, että sähköä saadaan sinne, missä sitä eniten tarvitaan. Asetuksella varmistetaan, että jäsenvaltiot ottavat käyttöön sopivat välineet mahdollisten sähkökriisien ehkäisemiseksi, varautumisiksi ja hallitsemiseksi yhteisvastuun ja avoimuuden hengessä. Asetuksella tavoitellaan myös yhteisten menetelmien käyttöönottoa Euroopan tasolla kriisiskenaarioiden tunnistamiseksi sekä sähkön tuotannon ja kulutuksen välisen lyhyen ja kausittaisen riittävyyden arvioimiseksi verkon vakauden säilyttämiseksi ja pulan välttämiseksi. Komissio on vaatinut jäsenvaltioita toimittamaan ensimmäiset strategiansa 1.1.2020 mennessä. Strategiat tullaan päivittämään viiden vuoden välein ja seuraavat uudet strategiat vaaditaan toimitettavaksi kymmenen vuoden päästä. (Euroopan komissio, 2020)

Euroopan parlamentin ja neuvoston asetus (EU) 2019/941 5.6.2019 (EUR-LEX 2019) riskeihin varautumisesta sähköalalla ohjaa jäsenvaltioita tekemään riskeihinvarautumissuunnitelman ja kuvaamaan siihen sähköverkon riittävyyttä ja käyttövarmuutta sekä energian huoltovarmuutta määrittäviä riskejä vähintään luonnonuhkien, onnettomuusuhkien ja välillisten uhkien (esim. hyökkäykset) näkökulmista. Suomessa Energiavirasto (2021) on toimittanut 7.4.2021 komissiolle riskienvarautumissuunnitelman, jossa on määritetty kansallisiksi sähkökriisiskenaarioiksi myrskyn, äärimmäisen kapasiteettia heikentävän säätilan, pandemian, kyberhyökkäyksen tuotantolaitoksiin tai sähkömarkkinatoimijoihin, kriittiseen henkilöstöön kohdistuvan uhkan, fyysisen hyökkäyksen ohjauskeskuksiin tai kriittisiin komponentteihin, vahingoittamisen sisältä käsin esim. sabotoimalla toimitusketjua sekä poliittinen tuotannon tai energiantuonnin pysäyttävän riskin.

Komissio on antanut lausuntonsa 14.6.2022 Suomen riskeihinvarautumissuunnitelmasta ja on todennut siinä mm. seuraavassa kuvatut puutteet. Kriisiskenaarioita tulisi arvioida suunnitelmassa esitettyä tarkemmin EU:n turvallisuustilanteen muuttumisen vuoksi Venäjän Ukrainaan kohdistuva hyökkäyssota huomioiden. Suunnitelmaa on päivitettävä geopoliittisten riskien, polttoaineriippuvuuksien, kolmansien maiden toimitusketjuriippuvuuksien sekä muiden sektoreiden alaan heijastuvien vaikutusten kannalta. Skenaarioiden laajuuksia tulisi tarkentaa alueellisesta ja kansallisesta ulottuvuudesta. Skenaarioiden tapahtumaketjut tulee kuvata. Polttoainetoimitusten suunnitelmia tulisi täydentää tiedoilla vaihtoehtoisista järjestelmistä. Ilmastonmuutokseen varautumista tulisi tuoda esille muutoksille haavoittuvuuden torjumiseksi. Alueelliset ja kahdenväliset yhteistyö- ja avustustoimenpiteet jäsenvaltioiden välillä tulisi sisällyttää suunnitelmaan. Sähkökriisin käsite täytyy määritellä ja ilmaista se suunnitelmassa, kuten myös se, missä olosuhteissa sovellettavat toimet ja menettelyt otetaan käyttöön. Tämän tutkielman kannalta erityisen huomioitavaa on komission lausuma menettelyiden, ml. tiedonjako- ja yhteistyömekanismien, toimivuuden testaamisesta ja sähkökriisien simuloinnista kahden vuoden määrävälein. Komissio huomauttaa, että Energiavirasto ei ole esittänyt näiden hätätilannetestien aikataulua. Suunnitelmaa tulisi asetuksen mukaisesti päivittää useammin kuin joka neljäs vuosi. Yhteistyötä erityisesti muiden Pohjoismaiden kanssa tulisi syventää. (Euroopan komissio, 2022)

4.1 Uhkien laaja-alaisuus

Poliittisessa päätöksenteossa joudutaan huomioimaan energiaturvallisuus yhä enemmän. Tämä johtuu energiamarkkinoiden globalisaatiosta ja markkinajärjestelmän monimutkaistumisesta, energiainfrastruktuurihankkeiden muuntumisesta valtioiden rajat ylittäviksi hankkeiksi, energiantuottajamaiden määrän vähentymisestä ja keskittymisestä tietyille alueille (riippuvaisuus lisääntyy), sekä teknologiakehityksen ja talouden keskinäisriippuvuuden kasvamisesta. Energiavarmuus tarvitsee moniulotteista ja monitieteellistä tarkastelutapaa, jossa esim. politiikan ja vallan sekä talous- ja luonnontieteiden näkemykset yhdistyvät. (Vainio, 2016)

Energiatoimiala takaa energiavarmuutta osana Suomen kriittistä infrastruktuuria. Christian Fjäderin eduskunnalle hallituksen siviilitiedustelua koskevan lainsäädännön esityksestä antaman Huoltovarmuuskeskuksen asiantuntijalausunnon (2019) ”Huoltovarmuuden toimintaympäristön muutos ja uhkakuvat” mukaan yksityisen ja julkisen sektorin yhteistyöllä on suuri merkitys tuotettaessa yhteiskunnan vastuulla olevia kriittisiä tuotteita ja palveluja. Toimintaan liittyy myös markkinaehtoisesti toimivia ulkomaalaisia tahoja. Tämän vuoksi Suomen kansalliseen kriittiseen infrastruktuuriin kytkeytyy rajojen ulkopuolisia toimintaan vaikuttavia rakenteita, resursseja ja prosesseja. Lausunnossa korostetaan erityisesti digitalisaation kehityksen suhdetta toimintaan liittyvien tietojärjestelmien ja -varantojen integroitumiseen ylikansallisiin toimintaprosesseihin ja siten erilaisiin kyberympäristössä tapahtuviin ilmiöihin. (Fjäder, 2019)

Monitahoisessa toimintaympäristössä on pyrittävä jäsentämään tietoa kokonaiskuvan hahmottamiseksi. Euroopan komission tutkimuskeskuksen (Joint Research Centre JRC) mukaan (2012) energiajärjestelmän riskit ovat tunnistettavissa eri luokkiin. REACCESS-, SECURE- ja EURACOM-hankkeissa[1] kartoitettiin unionin energiajärjestelmään kohdistuvia riskejä ja ryhmiteltiin ne eri riskivektoreihin ja luokkiin: teknisiin, sosiaalisiin, poliittisiin (sis. geopoliittiset), taloudellisiin, sääntelyihin liittyviin sekä ympäristölähteiden mukaisiin. Kullakin vektorilla tai luokalla oli omat indikaattorinsa, esim. konflikti-indikaattorit kuuluivat poliittiseen vektoriin. Riskejä luokiteltiin myös tahallisiksi tai tahattomiksi- (Bolado-Lavin ja muut, 2012)

Edellä kuvattua riskiluokittelua voidaan soveltaa myös uhkiin. Uhat voivat siten syntyä talous- tai muun järjestelmän rakennemuutoksesta tai epävakaudesta ja aiheuttaa järjestelmien romahduksen tai energiakriisin. Uhkien torjuminen ja kriiseihin varautuminen edellyttää energiajärjestelmien nk. aseistamista kyberturvallisuusteknologioin (esim.

[1] European Risk Assessment and Contingency Planning Methodologies for Interconnected energy Networks EURACOM http://www.euracom-project.eu/ ; Risk of Energy Availability ja Common Corridors for European Supply Security REACCESS http://reaccess.epu.ntua.gr/ ; Security of Energy Considering its Uncertainty, Risk and Economic implications SECURE http://www.secure-ec.eu/

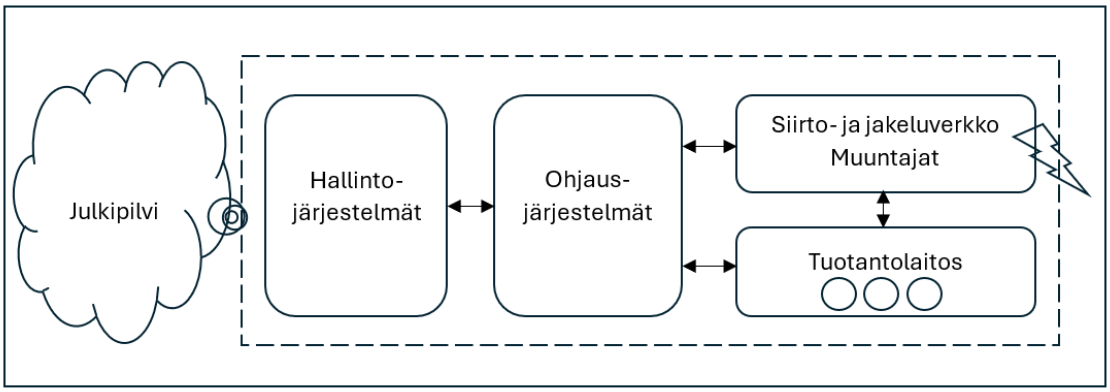
tunkeutumisen havaitseminen ja estäminen). Teknologiakeskeisyyden lisääntyessä toimintaympäristö monimutkaistuu, jolloin yksittäisten järjestelmän ominaisuuksien tai yksiulotteisen uhkamallinnuksen sijaan on pyrittävä tarkastelemaan kokonaisuutta. Lisäksi on huomioitava, että kybertoimintaympäristössä digitaalisia kyvykkyyksiä hyödyntävät myös rikolliset toimijat esim. energia-alan toimijoihin kohdistuvina kyberhyökkäyksinä. (Moilanen, 2021a)

Edellä mainittu aseistaminen viittaa sotilaalliseen toimintaan. Myös tietoylivoima on sodankäynnissä käytetty termi. Sillä viitataan kyvykkyyteen kerätä, käsitellä ja jakaa jatkuvaa tietovirtaa samalla kun torjutaan niin kutsutun vihollisen kyvykkyyttä toteuttaa vastaavaa tiedonhallintaa. Tämä saadaan aikaan hyödyntämällä tietoa keräämiä sensoreita, nopeaa verkkokapasiteettia, tiedon visualisointia sekä edistyksellistä mallinnusta ja simulointia. Pelkän raakadatan keräämisellä ei saavuteta tätä kyvykkyyttä, vaan tietoylivoimaan tarvitaan tiedonhallinnan kaikkia prosessivaiheita. Tässä sotilaallinen käsite on verkostokeskeinen sodankäynti, jossa kattavan datan nopealla käsittelyllä voidaan toteuttaa tehokasta toiminnanohjausta. Tiedonhallinnassa inhimillisellä toiminnalla on kuitenkin suuri merkitys, sillä on sanottu monen sodan tulleen hävityksi tai voitetuksi kognition alueella eli tietoa havaitsemalla, vastaanottamalla, tallentamalla, käsittelemällä, käyttämisellä ja ilmaisemalla. (Freedman, 2013)

4.2 Tieto ja viestintätekninen kyberturvallisuus energiatoimialalla

Energiasektoriin luetellaan kuuluviksi kaikki teollisuudenalat, jotka osallistuvat energiantuotantoon, jakeluun ja siirtoon (Kovanen, Nuojua & Lehto, 2018). Alan toimijoille on yhteistä hyödyntää ns. teollista tieto-/ohjausjärjestelmää (Industrial Information System IIS; Industrial Control System ICS) energian tuotannon, jakelun ja siirron prosesseissa. IIS/ICS muodostuu useista sensoreiden ja laitteistojen ohjaus- ja seurantajärjestelmistä alaverkkoineen. Sensorit tuottavat tietoa laitteiden, kuten esim. pumppujen tai moottoreiden ohjaukseen, jota voidaan toteuttaa verkon yli komponenttikohtaisella IP-osoitteella etähallintana (Remote Terminal Unit RTU), itseohjautuvana (Programmable Logic Controller PLS; Programmable Automation Controller PAC) tai hajautettuna (Distributed

Control System DCU). Järjestelmät ja laitteistot visualisoivat seuranta- ja ohjaustietoa (Supervisory Control And Data Acquisition SCADA) ihmisen toteuttamaa hallintaa (Human Machine Interface HMI; Human Systems Integration HSI) varten ja linkittyvät tuotannonohjausjärjestelmään. Tuotantoketjusta sensoreista ja järjestelmistä (Industrial Automation Systems IASs) saatava data voidaan koota omalle alustalleen (Industrial Internet) analysoitavaksi. Seuraavassa kuviossa on esitetty infrastruktuuriarkkitehtuuri yksinkertaistettuna (Desarnaud, 2018)



Kuvio 6 Energiainfrastruktuurin arkkitehtuuri (mukaillen Desarnaud, 2018)

SANS Instituutin (2015) mukaan turvallisuusarkkitehtuuri jakaa ICS-järjestelmäkokonaisuuden loogisesti yritysvyöhykkeeseen, demilitarisoitu vyöhykkeeseen (DMZ), tuotantovyöhykkeeseen ja aluevyöhykkeeseen. Tuotanto- ja aluevyöhyke muodostavat varsinaisen ICS-verkon. Internet-yhteys tulisi sallia vain yritysvyöhykkeelle ja tiedonsiirron tulisi tapahtua ainoastaan DMZ-vyöhykkeen kautta etäyhteyspalvelimien avulla. Laitostekniikka kuuluu tuotantovyöhykkeeseen. Aluevyöhyke sisältää kolme tasoa, joista korkein sisältää ihmisen ja koneen välisen käyttöliittymän (HMI) ja hälytysjärjestelmät. Keskikerros koostuu ohjelmoitavista logiikkaohjaimista (PLC), etäpääteyksiköistä (RTU) ja hajautetuista ohjausjärjestelmistä (DCS). Pohjakerros koostuu antureista ja fyysisistä toimilaitteista (esim. pumput, moottorit, venttiilit jne.). Kaikki vyöhykkeet tulisi erottaa palomuureilla ja niitä tulisi tarkkailla tunkeutumisen ilmaisujärjestelmillä (IDS). Tunkeutumisen estojärjestelmä (IPS) tulisi sijoittaa seuraamaan liikennettä yritysvyöhykkeen sisällä.

Erityistä huomiota olisi kiinnitettävä turvallisuustietoihin ja tapahtumien hallintajärjestelmiin (SIEM) ja lokien keräämiseen, jotka erotetaan vyöhykkeistä omalla palomuurilla ja IDS-järjestelmillä. (Kovanen, Nuojua & Lehto, 2018)

Tietojen välittämisen ja yhdistämisen tarve on järjestelmäkokonaisuudessa välttämätön, jotta laajasta toimintaympäristöstä kerättävää suurta tietomassaa voidaan hallita ja hyödyntää toiminnanohjaukseen. Energiatoimialan digitaalinen kehitys on toteutunut viiveellä verrattuna muihin toimialoihin ja kohtaa jatkuvasti uusia haasteita energiatekniikan murrosten, murrosteknologioiden syntymisen (esim. tekoäly) toimitusketjujen uudistumisen, tuotanto- ja toimitusketjuista saatavan datan reaaliaikaisen hyödyntämismahdollisuuksien sekä samanaikaisesti laajentuvien kuluttajapalveluiden (esim. älymittarit) vuoksi. Tästä syystä energiantuotannon kustannushyötyä ja toimintavarmuutta on kyettävä seuramaan ja tuotantoa ohjaamaan kattavan datan avulla sekä kyettävä toteuttamaan huolto- ja ylläpitopalveluissa tarvittavan datan hallittua ja turvallista saatavuutta. (Desarnaud, 2018).

Euroopan kyberturvallisuusviraston (ENISA) mukaan (2020) uhkaympäristöllä tarkoitetaan tietämystä tietyssä asia-/sisältöyhteydessä ilmenevistä uhista sekä niihin liittyvistä kohteista, haavoittuvista kyvykkyyksistä, riskeistä, uhkatoimijoista ja kehityksestä (trendit). Kyberturvallisuus tulee ymmärtää usealla tasolla kokonaisuuden turvaamiseksi, jolloin turvallisuus muodostuu ihmisen, prosessien ja teknologioiden toiminnasta (Kovanen 2021, viittaa Pöyhönen & Lehto, 2020). Jokaisella järjestelmän toimintakerroksella (kognitiivisella, palvelu-, semanttisella, syntaktisella, fyysisellä) turvataan tietopääomaa ja suojataan omaa toimintaa eri menetelmin. Ylin kognitiivinen kerros mahdollistaa käyttäjän tietoisuuden ja tilannetiedon tulkinnan ja ymmärryksen toimintaympäristössä sekä siten mahdollistaa strategisen päätöksenteon (Kovanen 2021, viittaa Pöyhönen ja Lehto, 2020).

Kybertoimintaympäristöllä puolestaan tarkoitetaan yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaa toimintaympäristöä, esimerkiksi liikenteen ohjausjärjestelmiä tai kuljetus- ja logistiikkajärjestelmiä (Kyberturvallisuuden sanasto, 2018). Kybertoimintaympäristöllä viitataan kybermaailman rinnakkaiskäsitteeseen, jolla tarkoitetaan digitaalisessa muodossa olevan informaation käsittelyyn tarkoitettujen tietoverkkojen ja -laitteiden, tietojärjestelmien ja niiden käyttäjien sekä käyttöympäristöjen ja toimintaprosessien muodostamaan kokonaisuutta (Lehto, 2019). Turvallisuuskomitean 2018 julkaiseman Kyberturvallisuussanaston mukaan kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kyberturvallisuus on kybertoimintaympäristön tavoitetila, jossa siihen voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristön tietoturvalla tarkoitetaan oloja, joissa tietoturvariskit ovat hallinnassa. Tietoturvaan kuuluu tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Kybertoimintaympäristön haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa, ja niillä tarkoitetaan sellaisia heikkouksia, jotka mahdollistavat vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Kyberhäiriötilanne on toiminnalle haittaa ja/tai vaaraa aiheuttava tapahtuma tai kehityskulku kybertoimintaympäristössä. (Sanastokeskus TSK, 2018)

Tietoja kokoavat ICT-järjestelmät ja niitä käyttävät organisaatiot ovat alttiita vahingoittaville toimille, kuten kaikki muutkin kybermaailmassa toimivat systeemit. Vahingoittamiseen liittyvät rakenteet, tekijät ja toimijat on tunnistettava, jotta sen jälkeen pystytään havainnollistamaan ja mallintamaan mahdollisia vahingoittamismenetelmiä. Tällä pyritään mahdollisimman kattavaan kyberfyysisten ja sosioteknisten järjestelmien sekä toiminnan suojauksen suunnitteluun. Suunnittelun pohjalta voidaan harjoitella vahinko-, häiriö-, hätä- ja vaaratilanteiden varalta.

Energia-alan kyberturvallisuuteen on tuotettu monien eri kansallisten ja kansainvälisten yhteisötoimijoiden, mm. Europan kyberturvallisuusviraston (ENISA) sekä USA:n kansallisen standardi- ja teknologiainstituutin (NIST) toimesta lukuisia ohjeistuksia, standardeja

ja sääntelyitä. Kansainväliset standardointiorganisaatiot (ISO) ovat julkaisseet useita kyberturvallisuusstandardeja (ISO/IEC 27000: Information Technologies) ja riskienhallintastandardeja (ISO/IEC31000: Implementation of risk management). Energia-alan erityinen standardi (ISO/IEC 27019: Information security controls for the energy utility industry) julkaistiin osana ISO/IEC 27000 -sarjaa lokakuussa 2017. Euroopan komissio päivittää suosituksiaan ja sääntelyään energiaomavaraisuuden kehittämiseksi ja tuotannon suojaamiseksi[2]. (Euroopan komissio, 2019)

USA:n energiaviraston 2012 luoma energiasektorin kyberturvallisuuskyvykkyyden kypsyysmalli (C2M2 2022) sisältää ohjeistuksia kyberturvallisuuskäytäntöjen käyttöönottoon ja hallintaan tiedon, tieto-, viestintä- ja operaatioteknologian varantojen sekä toimintaympäristön näkökulmista. Ohjeistuksessa tarkastellaan mm. muutos-, uhka-, riski-, tilanne-, tapahtuma- ja vastehallinnan ulottuvuuksia. (U.S. Department of Energy, 2022)

Suomessa ohjeistuksesta ja huoltovarmuusriskien arvioinnista vastaavat tahot ovat valtioneuvosto, Huoltovarmuuskeskus, Energiavirasto, kantaverkkoyhtiö ja jakeluverkonhaltijat. Suomen eri laeissa ilmaistujen velvoitteiden mukaisesti valtioneuvosto asettaa huoltovarmuuden yleiset tavoitteet, jotka määrittävät yleisen valmiustason suhteessa väestön vähimmäistarpeisin. Huoltovarmuuskeskus hyväksyy yleiset huoltovarmuustoimenpiteet ja toimenpiteet vakavien poikkeusolojen varalta. Siirtoverkonhaltija varmistaa kantaverkon luotettavuuden ja jakeluverkonhaltijat jakeluverkon ja loppuasiakkaiden toimitusten luotettavuuden. (Euroopan komissio, 2016)

Suomen Kyberturvallisuuskeskuksen mukaan kyberturvallisuuden kriisitilanteiden toimintamallit ovat usein puutteellisia. Haasteina on, että käytännön tilanteissa toimintamallit ulottuvat kumppaniverkostossa organisaatiorajojen yli, paperilla kuvatut toimintamallit eivät tositilanteessa kata kaikkia tarpeita ja viestintä sekä päätöksenteko eivät vält-

[2] Critical infrastructure and cybersecurity https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

tämättä toimi oikein. Kyberturvallisuus mielletään usein tekniseksi, mutta ihmisten merkitys on siinä suurin. Tekninen tiedonvaihto yhdessä ihmisten yhteistyöverkostojen kanssa asiantuntijoista johtoon rakentavat kyberturvallisuutta. Suomessa on verkostoiduttu hyvin ja yhteydenpito viranomaisten ja yritysten kesken on tiivistä. Kyberturvallisuusharjoitukset edistävät yhteistoimintaa, josta esimerkkinä on Huoltovarmuuskeskuksen Digipoolin organisoima TIETO20-harjoitus. Harjoituksen tarkoituksena on luoda menetelmiä ja parhaita käytänteitä, joilla autetaan kyberhyökkäyksen kohteeksi joutunutta toimijaa selviämään siitä ja muita välttämään hyökkäys. Kansallisen laajan häiriötilanteen hallintamallin kehittämisen lisäksi yhteinen asiantuntijuus kasvaa kokemuksia vaihtamalla ja vertaistukea saamalla. (Luukkainen, 2020)

Huoltovarmuuskeskus ohjaa yrityksille kohdennetuissa kyberturvallisuussuosituksissaan tunnistamaan tietojen käsittelyyn ja tallennukseen liittyvät vaatimukset, varmistamaan palveluntarjoajan kyvyn turvata tietojen eheys ja saatavuus sekä varmistamaan lainsäädännön huomiointi sopimuskäytännöissä. Yritysten tulee harjoitella toimintatavat häiriö- ja poikkeamatilanteisiin sekä varmistaa kyky tietoturvaloukkauksen tai sen uhan havaitsemiseen. Yritysten tulee myös varautua selvittämään, mitä tietoja häiriö- tai loukkaustilanteessa voidaan käsitellä sekä käsittelyn toimijat ja käsittelyperusteet. (Huoltovarmuuskeskus, 2020)

Häiriötilanteissa oleellinen osa johtamista ja päätöksentekoa on olla tietoinen tilanteesta. Tilannetietoisuus saavutetaan tilannekuvan avulla, mikä on tärkeä kaikilla hallinnollisilla tasoilla eli paikallisella, alueellisella ja kansallisella. Häiriötilanteiden aikana tilannekuvaa muodostetaan ja päivitetään mahdollisimman reaaliaikaisesti. Varautuminen tarkoittaa toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet normaaliolojen häiriötilanteissa ja poikkeusoloissa. (Tuominen, Rapeli & Mussalo-Rauhamaa, 2014)

Omaehtoisen harjoittelun merkitys on suuri kyberhäiriötilanteisiin varautumisessa. Valmiussuunnittelu on yksi varautumisen toimenpiteistä, johon tilannekuvan muodostamisen kyky kuuluu (Turvallisuuskomitea, 2017).

4.3 Esimerkkejä uhista ja niiden seurauksista

Energiatoimialalla kyberhyökkäyksiä tapahtuu päivittäin. Hyökkäysala on suuri ja tunkeutumisreittejä useita. Kohteina voivat olla laiteinfrastruktuuri, ICT-järjestelmät , tietokannat tai henkilöstö. Energianjakelussa järjestelmien suojaaminen on haastavaa niiden ympäri vuorokauden, useille toimijoille ja useista maantieteellisistä paikoista saatavillaolovelvoitteen vuoksi. (Westerdahl, 2019)

Energiatoimialalla dokumentoitiin maailmanlaajuisesti 1982–2018 seuraavia kybertapahtumia tapahtumatyypin ollessa sabotaasi, vakoilu, tietovarkaus, tiedustelu ja kiristys, ja toimijan ollessa sisäinen tai ulkoinen (Desarnaud, 2018):

- haittaohjelma SCADA-järjestelmässä
- virus ohjausjärjestelmässä
- hätävaroitusjärjestelmän aktivointi kaappaamalla sitä ohjaava tietokone
- jakelua ohjaavan paneelin haltuunotto
- virhe SCADA-järjestelmän tietokannan kehitystyössä
- tunkeutuminen järjestelmäoperaattorin sisäverkkoon
- parametrinäytön sammuttaminen madolla
- tietokoneiden hallintajärjestelmän päivityksestä johtuva tuotannonohjausjärjestelmän virhe
- mato laitteistonohjausjärjestelmässä
- tietomurto projektitietokantaan
- vahingollinen koodinosa verkossa
- pitkäaikainen tekninen tiedonsiirto (yritysvakoilu)
- tietojen muuttaminen, poisto tai varastaminen
- kovalevyjen tuhoaminen

- laitteen, komponentin tai ohjausjärjestelmän haltuunotto etähallintaan
- palvelun estäminen palvelunestohyökkäyksellä
- laitteiden, tuotantokomponenttien tai -kokonaisuuksien suunnitelmien, kuvausten, käyttöohjeiden tai mittaustiedon varastaminen
- sähköasemien irtikytkentä verkosta, tuotannonohjausjärjestelmän vahingoittaminen.

On oletettavaa, että kybertapahtumat monipuolistuvat edelleen teknologioiden kehittyessä ja samanaikaisesti uusien haavoittuvuuksien ilmetessä. Kybertapahtuma vaikuttaa aina tilannekuvan saatavuuteen ja tilanneymmärryksen muodostumiseen havainnoinnin kautta. Kyberturvallisuus on myös sosiaalinen haaste inhimillisiin heikkouksiin kohdistuvina manipulointeina, mutta myös järjestelmien suunnittelupuutteina (Mujinga, Kroeze & Elof, 2017). Turvaketju ei ole aukoton, mikäli käyttäjät eivät pysty tulkitsemaan oikein virheilmoituksia tai varoitusviestejä, tai heillä on mahdollisuus ohittaa suojausmekanismeja.

Hyökkäyksen tavoitteena voi olla järjestelmän tai palvelun toimivuuden keskeyttäminen, luottamuksellisuuden heikentäminen tietoihin pääsemiseksi, tietojen saatavuuden estäminen, tai tietojen eheyden rikkominen muuttamalla laitteiston tai järjestelmän toimintaa tai poistamalla komponentteja toiminnasta (Desarnaud, 2018). Hyökkääjä voi toimia taloudellisista tai (geo)poliittisista lähtökohdista, jolloin motiivina voi olla tiedonhankinta kilpailuasetelmasta, kyvykkyyksistä, huoltovarmuudesta sekä samalla myös resilienssistä (resilienssiä on käsitelty tarkemmin seuraavassa pääkappaleessa). Motiivi vaihtelee toimijan mukaisesti, joka voi olla valtio, yksittäinen ihminen tai rikollisryhmä. Kaikki tavoittelevat omaa etua, joko kasvattamalla omaa tietopääomaa ja salaamalla omaa toimintaa, tai julkisena voimannäyttönä.

Erilaisten hyökkäystyyppien torjumiseksi tulee soveltaa useita samanaikaisiakin keinoja. Kyberturvallisuusteknologialla voidaan suojautua vain tiettyyn tasoon asti hyökkäyksen nopeuden tai laajuuden vuoksi. Tehokas torjunta muodostuu myös inhimillisestä toimin-

nasta ja hyvästä turvallisuuskulttuurista. Tietojenkalastelua (phishing) ei voida täysin torjua pelkällä teknisellä haittaohjelmien suodatuksella. Lisäksi on huomioitava, että suurin osa haittaohjelmatartunnoista tapahtuu hallinta- ja valvontatasolla operaattoreiden työasemien ja käyttöliittymien kautta. Kyberhyökkäysprosessin (ICS Cyber Kill Chain) ensimmäisen vaiheessa hankitaan tietoa havainnon avulla (reconnaissance) sekä tutkimalla kohdetta avoimen lähdekoodin tiedonkeruutyökaluilla tai hakemalla tietoa julkisista lähteistä. Tiedonkeruu voidaan tehdä etäohjatusti salakuuntelemalla tai -kuvaamalla elektronisia viestintävälineitä (ml. älykellot ja -puhelimet) (Westerdahl, 2019). Hyökkääjän tavoitteena on paljastaa heikkoudet ja tunnistaa ne tiedot, jotka tukevat hyökkääjää hyväksikäyttämään kohteena olevan järjestelmän osia. Hyökkääjää hyödyttävät tiedot käyttäjistä, verkosta, palvelimista, käyttäjähallinnasta ja tileistä sekä tiedot prosesseista, protokollista, toimintatavoista ja menettelyistä, teknisten haavoittuvuustietojen ohella. Tiedustelussa voidaan käyttää valtavaa tietomäärää kohteen sitä havaitsematta. (Assante & Lee, 2015)

Vuonna 2017 tehdyssä kyselyssä hieman yli kaksi kolmasosaa tietotekniikan toimijoista katsoivat ICS-järjestelmiin kohdistuvien uhkien olevan vakavia tai kriittisiä. Erityistä huolta aiheuttivat teollinen internet (Industrial Internet of Things) sekä informaatio- ja toimintateknologioiden lähentyminen. Huomiota on kiinnitettävä älyverkoiksi kutsuttujen tietoverkkojen standardien ja protokollien yhteentoimivuuteen ja niiden omaksumiseen, teknisiin riippuvuuksiin ja järjestelmien monimutkaisuuteen. (Kovanen, Nuojua & Lehto, 2018)

On arvioitu, että voi vanhentuneiden järjestelmien haavoittuvuuspäivitykset ja haittaohjelmien käyttöönotot voivat aiheuttaa käytössä olevien laitteistojen toiminnan keskeytymisen tai toiminnan muuttumisen jopa viidesosalla yhteensopimattomuusvirheiden vuoksi. Em. syystä tuotantoriskien torjumiseksi on mahdollista, että laitteistoja ja järjestelmiä päivitetään harvoin. Eräs kuuluisimmista esimerkeistä tulee Japanista 2011 onnettomuuden kohdanneesta Fukushiman ydinvoimalasta, jonka operaattorille (Tokyo

Electric Power Company TEPCO) annettiin 2015 kehotus päivittää 48 000 vanhentuneella käyttöjärjestelmällä (Windows XP) edelleen toimivaa työasemaa. (Desarnaud, 2018)

Energiatuotantoon ja jakeluun kohdistuvien hyökkäyksen seuraukset ovat arvioitavissa tutkimalla energian tuotannon ja jakelun häiriöiden vaikutuksia kansallisilla tasoilla. Massiiviset sähkökatkokset, kuten New Yorkissa 14.–15. elokuuta 2003, haastavat kansakunnan sietokyvyn. Tämä kaksi päivää kestänyt sähkökatkos kasvatti kuolleisuuden määrää noin neljänneksellä (n=90) kyseisen elokuun aikana. Kuolemat johtuivat pääasiassa sairauksien hoidossa käytettävien lääkinnällisten laitteiden rajoitetusta käytöstä ja hitaammasta ensihoidon vasteajasta. (Kovanen, Nuojua & Lehto, 2018)

Sähkönjakeluhäiriöt voivat olla mittavia, esimerkiksi Saksassa korkeajännitelinjan irtikytkentä 2006 aiheutti sähkökatkoksen kuudessa (6) maassa 15 miljoonalle ihmisille. Ukrainassa 23.12.2015 toteutettu kyberhyökkäys alueellisille sähköverkko-operaattoreille aiheutti usean tunnin kestävän sähkökatkoksen yli 200 000 ihmiselle. Operaattorit joutuivat menemään sähköasemille fyysisesti paikan päälle, sillä etäohjaus ei toiminut tietoliikenneyhteyksien ollessa poikki. Fyysisen läsnäolon tarve asemilla kesti useiden viikkojen ajan hyökkäyksen jälkeen. Hyökkäyksellä katkaistiin virta noin kolmestakymmenestä (30) asemasta ja se toteutettiin hyödyntämällä tietojenkalastelua ja käyttämällä syvällistä tietoutta teollisuuden ohjausjärjestelmistä (ICS). Ukrainan tapahtuma oli ensimmäinen, jolla oli fyysisiä käytännön vaikutuksia sähkönjakeluun. Kyberhyökkäyksen taloudelliset vaikutukset voivat olla merkittävät ja mm. USA:ssa hyökkäyksen kustannusten on arvioitu olevan noin 2,5 miljoonasta dollarista yhteen triljoonaan dollariin. (Desarnaud, 2018)

Irlantilainen sähkönsiirtoverkonhaltija EirGrid joutui elokuussa 2017 kyberhyökkäyksen kohteeksi. Hyökkäys toteutettiin reitittämällä verkkoliikenne uudelleen. Verkko-operaattori Vodafone ja Irlannin kansallinen Kyberturvallisuuskeskus arvioivat hyökkäyksen toteuttajana olleen valtiollisen toimijan. (Kovanen, Njuojua & Lehto, 2018)

Ukrainan energialaitoksiin kohdistetuista hyökkäyksistä on lukuisia esimerkkejä tälläkin ajanhetkellä Venäjän yrittäessä heikentää Ukrainan selviytymistä ja huoltovarmuutta erityisesti talvikaudella. Poliittisen motivaation omaavien kyberhyökkäysten määrä kasvaa edelleen samalla kuin valtiollisten toimijoiden, erityisesti Venäjän, Kiinan, Iranin ja Pohjois-Korean tiedustelu haavoittuvuuksien etsimiseksi kriittisestä infrastruktuurista lisääntyy (Mission Support Center, 2016, viittaa Clapper, 2016)

Suomen suojelupoliisin (2024) mukaan kriittinen infrastruktuuri on jatkuvasti altis erityisesti tiedustelun ja vaikuttamisen uhalle Venäjän taholta. Myös Svenska Kraftnät´n (2024) uhkakuvan mukaan ulkovaltojen (erit. Kiina, Venäjä) tiedonkeruu on suurin uhka Ruotsin sähkönsaannille terrorismin ja järjestäytyneen rikollisuuden toiminnan lisäksi. Energiaalan toimijoilla tulee olla avoimiin lähteisiin perustuvaa jaettavaa tietoa toimintaympäristön muutoksista tarvittavien varautumistoimenpiteiden toteuttamiseksi.

Energiatoimialan haavoittuvuutta lisää erityisesti se, että erilaiset alihankinta- ja toimitusketjut ovat sekä laajoja että vain muutaman kriittisen päätoimittajan varassa esim. komponenttivalmistuksen ja huollon suhteen ulottuen oman maan rajojen ulkopuolelle. Tällaisen toimittajan joutuessa esim. kyberhyökkäyksen kohteeksi aiheutuu kerrannaisvaikutusta monelle samasta toimittajatahosta riippuvaiselle osapuolelle. Lisäksi on mahdollista, että uhkatoimija ns. soluttautuu toimitusketjuun mukaan esim. osaomistajana tai alihankinnan kautta, jolloin hyökkäysala kasvaa. Hyökkäysalaa muodostaa myös energiahuollon fyysinen infrastruktuuri, mikä voi vaurioitua esim. räjähdehyökkäyksen oheisvauriona varsinaisen kohteen ollessa toinen. Tähän uhkaan herätty Ruotsissa järjestäytyneen rikollisuuden ja jengien aiheuttamien uhkien vuoksi. (Westerdahl, 2019)

5 Uhkahavainnoinnin tiedonkäsittelyn tukeminen

Järjestelmäratkaisujen toiminnallisuuksien tulee edellä kuvatun mukaisesti tukea uhkatilannekuvan muodostamista ja visualisointia, monenvälistä ja ajantasaista tilannetiedon jakamista, uhka- ja riskianalyysia vaikutustenarviointeineen, heikkouksien ja haavoittuvuuksien tunnistamista, turvallisuustilanteen arviointia, turvallisuus- ja valmiustilan asemointia sekä torjunta- ja kontrollitoimien seurantaa. Näille edellä kuvattujen muutos-, uhka-, riski-, tilanne-, tapahtuma- ja vastehallinnan ulottuvuuksien toiminnoille luodaan dokumentoitavat, vakiinnutettavat ja ylläpidettävät menettelyt, politiikat ja ohjeistukset. Työvoimaan, välineisiin ja talouteen liittyvät resurssit varataan ja valtuutetaan toteutusta varten. Hallintaulottuvuuksien toimintojen tehokkuutta seurataan ja arvioidaan. (U.S. Department of Energy, 2022)

Vuonna 2016 tehdyn tutkimuksen (RSA Research) mukaan kansainvälisistä yrityksistä vain noin viidennes kykeni nopeaan tai erittäin nopeaan kyberhyökkäysten havainnointiin, sillä ne eivät joko kokoa tarvittavia tietoja tai hyödynnä keräämiään tietoja (Yoran, 2016) . Tämän pääluvun alaluvuissa tarkastellaan edellä mainitun valossa uhkiin varautumista resilienssin näkökulmasta, tilannekuvan ja ennakoinnin välistä suhdetta, uhkatiedon hankintaa ja jalostamista tietotuotteeksi järjestelmäteknisissä ratkaisuissa sekä yhteistoimintaa ja harjoittelua osana uhkiin varautumista.

5.1 Uhkatiedon merkitys varautumiseen

Informaatio on tietyssä muodossa, merkityssisällössä ja käyttöyhteydessä olevaa uutuusarvon omaavaa välitettävää ja tietyssä viitekehyksessä tulkittavaa tietoa (Rantamäki & Jalonen, 2022, viittaa Davenport & Prusak, 1998). Toimijat voivat rakentaa omia tietokantojaan ilmiö- ja uhkatiedon keräämiseen ja käsittelyyn sekä niiden muutosten ja keskinäisten vaikutusten seurantaan (Rubin, 2024). Edellä mainitulla muodostetaan organisaatiolle palautuvuutta ja palautumiskykyä (Nevalainen, Tukiainen & Myllymäki, 2021) sekä kimmoisuutta ja sietokykyä, huolimatta siitä, että kaikkeen ei voi aina varautua. Re-

silienssillä tarkoitetaan kriisinkestävyyttä eli yksilöiden, yhteisöjen ja instituutioiden toimintakyvyn ylläpitoa muuttuvissa olosuhteissa sekä valmiutta kohdata ja palautua häiriöistä ja kriiseistä. Resilienssi ilmentyy jatkuvan varuillaan olon, tarkkailun, ennakoinnin ja kokemuksesta oppimisen kautta. Resilienssiä voidaan määritellä myös sosio-ekologisesti, jolloin kuvataan yhteisöjen ja yhteiskuntien ennakoimattomissa olosuhteissa sekä alati monimutkaistuvassa ympäristössä toteutettaviin vakautta edistäviin itseorganisoitumisen, resurssienhallinnan ja päätöksenteon toimiin hajautetun turvallisuusvastuun periaatteella. Resilienssi ei ole sidottu ainoastaan nykyhetkeen vaan se liittyy myös menneisyyden ja tulevaisuuden tilanteisiin osana sitä, mitä toimenpiteitä toteutetaan ennen kriisitilannetta, jotta resilienssi toteutuu ko. kriisin aikana sekä sen tapahtuma-ajankohdan jälkeen. Resilienssin olemassaolo ei itsessään vähennä uhkia tai niiden toteutumisen todennäköisyyttä, eikä sen suojelemiseksi tai arvioimiseksi ole vielä olemassa muodollista järjestelmää sen kansainvälisen yhteistyönkin ollessa vielä varsin kehittymätöntä. (Moilanen, 2021b, viittaa Kyberturvallisuuden sanasto, 2018, Adger, 2003, Kaufmann, 2017 ja Hyvönen, 2019)

Tietojen hankintaa ja arviointia tulisi toteuttaa mahdollisimman kokonaisvaltaisesti resilienssin ylläpitämiseksi. Tällöin rakennetaan informaatioresilienssin kyvykkyyttä, jossa pyritään varmistamaan organisaatiolle hyödyllisen informaation saatavuus, torjumaan väärän ja harhaanjohtavan informaation aiheuttamia ongelmia toiminnalle sekä rakentamaan ennakointinäkökulmasta proaktiivista varautumiskyvykkyyttä kriisitilanteisiin. Informaatioresilienssillä on suhde myös huoltovarmuuteen, sillä kansallinen huoltovarmuus on samalla myös tiedon huoltovarmuutta. (Rantamäki & Jalonen, 2022)

Energiatoimijat voivat hyödyntää Maailman energiajärjestön (World Energy Council) kehittämää viitekehystä tarkistuslistana resilienssinsä kehittämiseen. Viitekehys erottautuu tavanomaisesta riskienhallinnasta jatkuvan oppimisen periaatteen soveltamisella sen sijaan, että sillä pyrittäisiin hallitsemaan tulevaisuutta vähentämällä epävarmuutta. Toimintaa vahvistetaan systeemitasolla ennakoinnin, vahvan yhteistyön ja kokeilevan vaste-

toiminnan avulla, jolloin muutoksiin reagoinnista tulee dynaamista. Dynaamiselle resilienssille on ominaista verkostoituminen ja liittoutuminen toimialan eri toimijoiden, strategisten kumppaneiden ja lainvalvonnan edustajien kanssa. Tällä kanavien ja mekanismien luonnilla ja niiden valmiina ololla häiriö- ja poikkeustilanteissa voidaan vahvistaa tilannetietoisuutta ja kyvykkyyttä vastatoimiin. Tietojärjestelmätasolla tämä ilmenee esimerkiksi siten, että turvallisuuskontrollit ovat hajautettuja ja kattavat laajalti eri operointialueita, jolloin poikkeus- ja häiriötilanteissa ne voivat automaattisesti siirtyä suojaustilaan. Tähän tarvitaan tietoa muutoksista, niiden automaattista arviointia sekä ennalta määrättyjä toimenpiteitä, jotta toimintaprosessi saadaan sujuvaksi ja katkeamattomaksi. (World Energy Council, 2019)

Resilienssin määritelmä eroaa antihaurauden (engl. antifragility) määritelmästä siinä, että resilientti järjestelmä palautuu entiselleen häiriön kohdatessaan, mutta antihauras järjestelmä vahvistuu häiriön tapahduttua kasvattamalla aina kyvykkyyttään sopeutua niihin (Taleb & West, 2023). Tämän mukaisesti uhkatilanteista oppiminen ja sen hyödyntäminen varautumiseen olisi siten enemmän antihaurautta kuin resilienssiä.

5.2 Tilannekuva ja tilannetietoisuus

Varautuminen ja toiminnan jatkuvuuden varmistaminen edellyttää kyvykkyyttä muodostaa tilannekuva. Tilannekuvalla tarkoitetaan koottua kuvausta vallitsevista olosuhteista, käsillä olevan tilanteen synnyttäneistä tapahtumista, tilannetta koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista sekä eri toimijoiden toimintavalmiuksista (Kokonaisturvallisuuden sanasto; Sanastokeskus TSK 50, 2017). Tilannekuva muodostuu inhimillisestä ymmärryksestä ja tulkinnasta tapahtuneista asioista, niihin vaikuttaneista olosuhteista, eri osapuolten tavoitteista ja mahdollisista kehitysvaihtoehdoista, toimintaan liittyvien päätösten tekemiseksi (Turvallisuuskomitea, 2017). Teknisen tiedon lisäksi tietoisuus ja ymmärrys tilannekuvasta pitää sisällään myös kyvykkyyden arvioida tilanteeseen johtaneita syitä ja kykyä ennustaa tilanteen jatkokehittymistä. Tätä kuva-

taan tilannetajulla, mikä syntyy eri toimijoiden tietotaidon, roolien ja toimintaympäristöjen pohjalta muodostetuista tilannekuvista. Tilannekuvia voi siten olla useampi. (Huovila ja muut, 2010)

Tilannetietoisuus muodostetaan tilannekuvien avulla. Yleinen suomalainen ontologia määrittelee tilannetietoisuuden seuraavasti: "Kuvaus tai käsitys vallitsevasta tilanteesta, sen taustatekijöistä ja tilanteen kehittymisen mahdollisista vaihtoehdoista" (FINTO, 2019). Tilannetietoisuuden käsite on siinä määritelty kuuluvaksi sotatieteen tai työsuojelun ontologiaan. YSO viittaa FAST: iin, joka puolestaan viittaa Wikipedian määritelmään tilannetietoisuudesta ”ympäristötekijöiden havaitsemisena” (FAST, Wikipedia, 2019). Tilannetietoisuus on toimijan kykyä seurata, ymmärtää, arvioida ja jatkuvasti päivittää havaintoja toimintaympäristöstään (Endsley, 2015; 1995). Toisin sanoen tilannetietoisuus on ympärillä olevien tapahtumien tiedostamista ja tietämistä, jatkuvaa ympäristötiedon hankintaa ja yhdistämistä aiempaan tietoon yhtenäisen mielikuvan muodostamiseksi, sekä tämän mielikuvan käyttöä havaintojen ohjaamiseksi ja tulevien tapahtumien ennakoimiseksi (Blasch ja muut, 2006; Endsley, 2000).

Tilannetietoisuutta tarvitaan luotettavuuden ylläpitämiseksi sekä tapahtumien ennakoimiseksi ja niihin vastaamiseksi. Ensimmäisen havaitsemisen tason tavoitteena on havaita tiedot tilanteesta, tilanteeseen liittyvistä tekijöistä sekä toimintaympäristön muutoksista liittyen resursseihin, prosesseihin ja muihin merkityksellisiin tarkkailtaviin kohteisiin. Saatujen tilannetietojen ts. tilanteen tunnistamisen pohjalta muodostetaan käsitys tilanteen vaikutuksista omaan toimintaan, jolloin tilanteeseen reagoivat toimenpiteet voidaan toteuttaa ja saada niiden vasteesta uutta tietoa tuleviin tapahtumiin varautumista varten. (NERC 2017, viittaa Endsley 1995)

Uhkien hallinnan kannalta tilannetietoisuutta tulee tukea strategisella tiedustelulla. Strategisen tiedustelun harjoittaminen tuottaa tulevaisuutta koskevaa tietoutta ja arvioita sekä helpottaa johtotason päätöksentekoa (Joint Chiefs Of Staff, 2013). Tiedustelulla py-

ritään vähentämään epävarmuutta erilaisissa uhka- ja konfliktitilanteissa, kuten esim. liiketoimintatiedustelun keinoin kilpailuasetelman vallitessa (Niemelä 2021, viittaa Clark 2020 ja Liebowitz 2006).

Havaintoja tehdään muutoksista ja kehityskuluista sekä ulkopuolisten toimijoiden tarkoitusperistä ja tavoitteista, jotka voivat muodostua suoranaisiksi kyberriskeiksi, tai jotka voivat muutoin merkittävästi vaikuttaa toimialaan. Tulkitut ja arvotetut havainnot viedään päätöksentekoprosesseihin, joilla valmistaudutaan ennakolta häiriö- ja poikkeustilanteisiin. Hajautunut tilannetietoisuus tarkoittaa keskinäisessä vuorovaikutus- ja viestintäprosessissa olevien inhimillisten ja/tai ei-inhimillisten toimijoiden toisiaan täydentävään toimintaan (Franssila, 2020, viittaa Stanton ym., 2006 ja 2007). Inhimillinen ja tekninen kyvykkyys havainnointiin ja tilannetietoisuuteen sekä ihmisen ja koneen vuorovaikutuksen (Human Computer Interaction HCI) tuki ovat edellytyksiä järjestelmän autonomisella toiminnalle (Ailisto, 2018), jossa tietoa hankitaan ympäristöstä. Tietoa täytyy ylläpitää ja päivittää, sillä ympäristö muuttuu ajassa (Franssila, 2020, viittaa Gutwin & Greenberg, 2002). Toimintaympäristön muutoksen seuranta alkaa tarkkailtavien toimijoiden määrittämisellä, jonka jälkeen muutoksen lähde paikallistetaan ja sen tapahtumisen todennäköisyys arvioidaan muutosten vaikutusten ennakoimiseksi (Rubin, 2024).

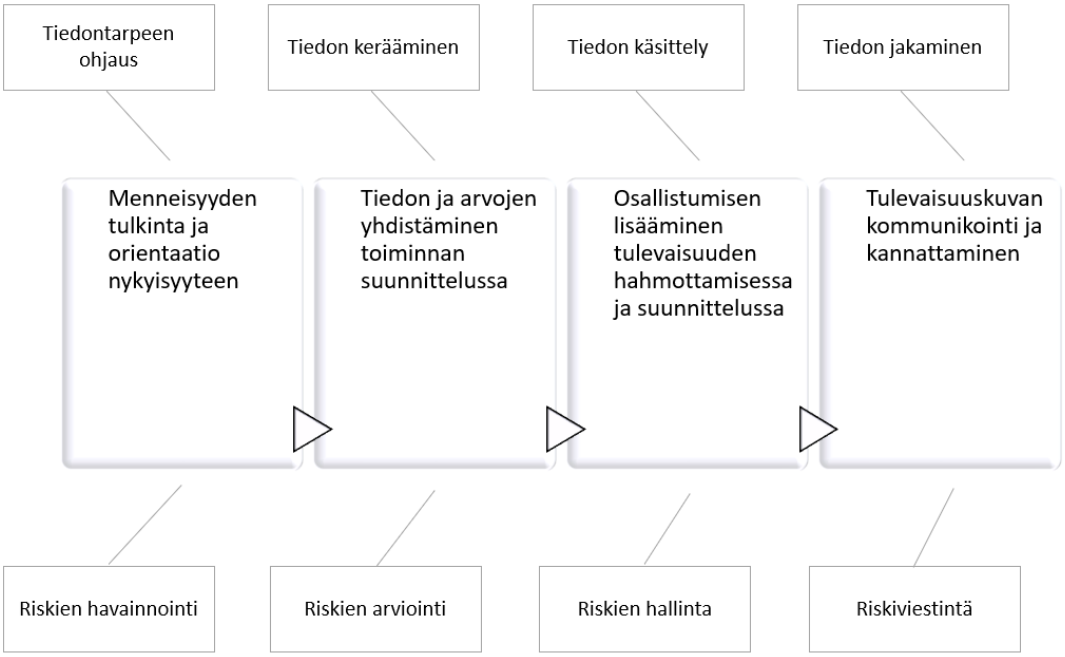
Maa- ja metsätalousministeriön 2019 teettämässä selvityksessä vesihuollon häiriötilanteista osoitettiin, että tilannekuvan muodostaminen häiriötilanteessa on haastavaa. Kaikissa selvityksen esimerkkitapauksissa tilannekuva oli aluksi ollut väärä. Selvityksessä todettiin, että vesihuoltolaitoksen tulisi heti häiriötilanteen alussa panostaa tilannekuvan luomiseen ja korjaavien toimenpiteiden nopeaan aloittamiseen (Belinskij & Saarinen, 2019). Sosiaali- ja terveysministeriön teettämässä selvityksessä sairaanhoitopiirien alueellisesta varautumisesta kävi puolestaan ilmi, että alueellisen valmiussuunnitelman käsite ymmärrettiin eri tavoin (Tuominen, Rapeli & Mussalo-Rauhamaa, 2014). Käsite on tiedon yksikkö tai ajattelun perusyksikkö tai ajatustiivistymä (Tieteen termipankki, 2020), jonka tulkitseminen eri tavoin tai ymmärtäminen väärin heikentää suunnittelua, toimintaa, viestintää ja tehtävien suorittamista. Väyläviraston (2011) tutkimuksessa puolestaan

todettiin, että tilannetietoisuutta ja tilannekuvaa termeinä tai niiden edellytyksiä ei oltu määritetty operatiivisen liikenteenhallinnan näkökulmasta ennen ko. julkaistua tutkimusta, jolloin erot termien käytössä ovat saattaneet heikentää toimijoiden kanssakäymistä ja lisätä väärinkäsityksiä (Väylä, 2011). Kaikki edellä kuvatut toimivat esimerkkeinä siitä, millaisia haasteita tilannekuvaan luomiseen liittyy osana varautumista.

5.3 Aikakäsitys, tulevaisuus ja ennakointi varautumisen lähtökohtana

Edellisessä alaluvussa kuvatun resilienssin, ml. informaatioresilienssin, toteuttaminen vaatii kykyä jäsentää tulevaisuuteen liittyvää tuntematonta eli kykyä ennakoida, jotta tulevaisuutta muokkaavia tapahtumaketjuja ja nykyhetken ilmiöitä voidaan tunnistaa jo varhaisessa vaiheessa ja että niihin voidaan varautua. Varautumisenhallinta muodostuu heikkojen signaalien havainnoinnin kyvystä, kyvystä hankkia ja jakaa kriittistä tietoa sekä kyvystä näiden pohjalta tehdä ja toteuttaa päätöksiä. (Rantamäki & Jalonen, 2022, viittaa Blay, 2020; Brasset & Vaughan-Williams, 2015; Boin & Lodge, 2016; Donovan & Oppenheimer, 2016)

Varautumisessa tarvitaan siten tulevaisuudentuntemusta. Niiniluoto (1999) viitaa Belliin (1997) kuvatessaan tulevaisuuden tutkimuksen tehtäviksi mm. mahdollisten, todennäköisten ja tulevaisuuskuvien tutkimisen. Alla olevassa kuviossa on kuvattu tämän tutkimuksen kontekstissa tulevaisuuden tutkimuksen muiden Bellin nimeämien tehtävien yhteyttä toiminnan suunnitteluun ja tulevaisuuden hallintaan.



Kuvio 7 Tulevaisuuden hallinta, mukaillen Niiniluoto (1999)

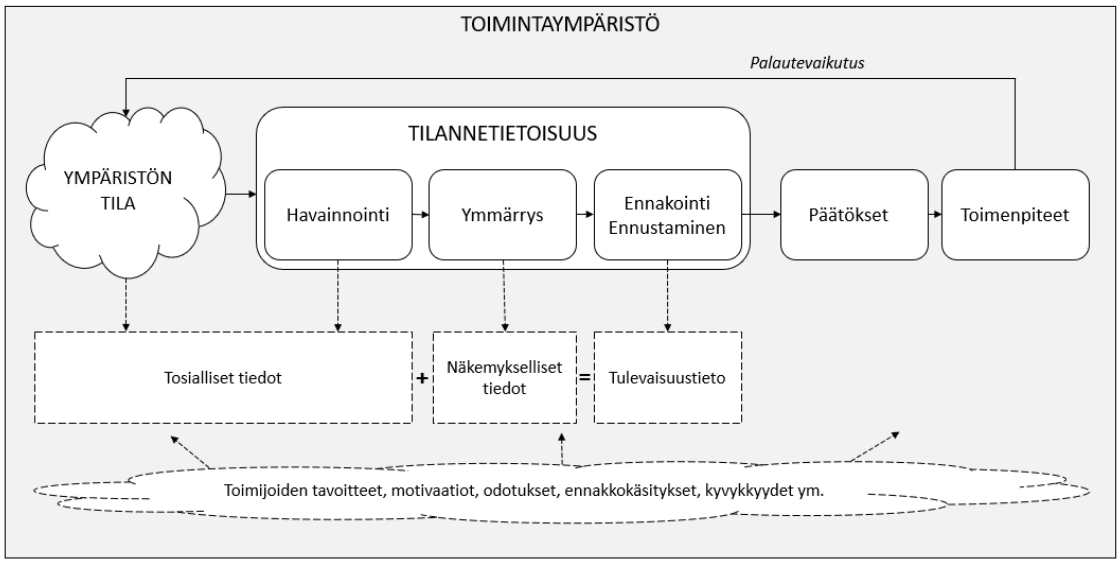
Niiniluoto (1999) kuvaa tulevaisuuden tutkimisen olevan luotaamista sekä oman ja yhteisen toiminnan vastuullista harkintaa, suunnittelua ja rakentamista. Niiniluoto (1999) viittaa edelleen RAND-yhtiön matemaatikkoon Olaf Helmeriin, jonka mukaan kohtalonuskoinen sivustakatsojan käsitys tulevaisuudesta arvaamattomana ja välttämättömänä ei enää päde, sillä olemme oppineet ymmärtämään, että erilaiset tulevaisuudet ovat mahdollisia ja että niihin voi vaikuttaa oman toimintamme väliintuloina. Tulevaisuuden tutkimisen tehtävissä on havaittavissa yhtymäkohtia myös tiedusteluanalyysin (ks. alaluku 3.4) prosessivaiheisiin ja riskienhallinnan prosessin tehtäviin, mitkä nekin tavoittelevat tulevaisuuden hallintaa.

Tulevaisuuden hallinta edellyttää kykyä havaita ennusmerkkejä toimintaympäristössä esiin nousevista tulevaisuuden kannalta merkittävistä asioista tai muutoksista, jolloin tulevaisuuden tutkiminen on muutoksen tutkimista ennusmerkkien avulla. Näitä ennusmerkkejä kutsutaan heikoiksi signaaleiksi, joiden avulla voidaan tunnistaa oletuksia tulevaisuusnäkymistä ja kehityskuluista sekä toimia toivottavan tulevaisuuden saamiseksi.

Heikot signaalit eivät itsessään ole ennusteita, eivätkä ne siten suoraan ainoana vaihtoehtona mitä tulee tapahtumaan. (Dufva & Rowley, 2022, viittaa Hiltunen, 2010)

Toimintaympäristön aikakäsitys muodostuu toiminnan mm. teknologiajärjestelmien, tuotannon ja vuorovaikutuksen rytmeistä. Rytmit tulevat sitä selkeämmiksi, mitä enemmän ja säännöllisemmin niitä noudatetaan, jolloin ne saavat aikaan toiminnan kaavan, johon toimintaympäristön toimijat sopeutuvat ja sitoutuvat. Rytmien muodostamat kaavat mahdollistavat ennustettavuuden. Asioiden visualisoinnin nopeus kuvastuu fyysisten, elektronisten ja digitaalisten järjestelmien kautta, jotka sallivat myös ajan ja paikan riippumattomuuden toimijan yhtäaikaisella läsnäololla useassa eri sijainnissa. Toisistaan eroteltavissa olevien toimintaympäristön tapahtumien rytmien muutokset ilmenevät tapahtumajonojen muodostumisena tai niiden katoamisina riippumatta tapahtuman aiheuttajan tai sen päättäjän fyysisestä tai virtuaalisesti sijainnista. Tietovirrat voivat olla katkeamattomia ja siten samalla ajattomia tai aikamääreistä vapaita niin kutsuttuja hetkittäisiä ikuisuuksia tai temporaalia järjestyksiä ilman järjestystä (Kamppinen, 1999, viittaa Castells, 1996). Saatujen tietojen nopean vanhentumisen vuoksi kyky hallita samanaikaisuutta ja reaaliaikaisuutta on toimijoille kilpailuetu. (Kamppinen, 1999)

Tarve tulevaisuuden ennakoinnille on olemassa seuraavassa kuviossa kuvattujen elementtien mahdollistamana. Ennakointi on huolenpitoa tulevaisuudesta sekä kykyä nähdä asioita ennen niiden tapahtumista (Malaska, 2013, viittaa Oxford English Dictionary 5. painos, 2002). Toimintaympäristön dynaamisuus eli ajallisen tilan ja ympäröivän maailman rakenne sallii intentionaalisen toiminnan ja intressien syntymisen. Muutokset, niiden suunta ja nopeus voidaan tunnistaa etukäteen, jolloin valintojen tekeminen tulee mahdolliseksi. Ennakoinnit ja ennusteet, jotka eivät vastanneet reaalimaailman kehitystä, auttavat tästä huolimatta ymmärtämään toimintaa ja seurauksia. Kokonaisuudesta muodostuu tulevaisuustietoa, joka on luonteeltaan faktuaalista tietoa yleisempää ja monipuolisempaa. (Malaska, 2013)

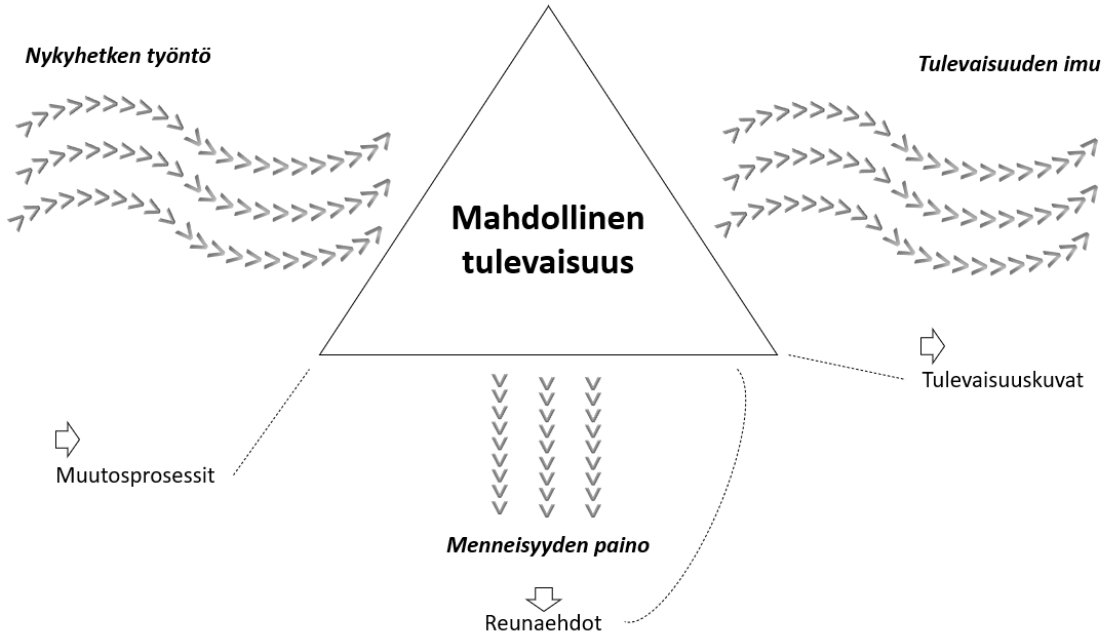


Kuvio 8 Tulevaisuustieto (mukaillen Endsley, 2015; 1995 ja Malaska, 2013)

Tulevaisuustiedon sanoittaminen edellyttää tarkasteltavan kohteen (järjestelmän tai toimintaympäristö) tuntemista (Borg, 2013). Ennakoinnissa merkittäviä ovat tapahtumat, joiden esiintyminen ei ole vielä varmuudella määräytynyt tai vahvistunut, toisin sanoen niiden totuusarvoa ei ole vielä määritettävissä. Tällöin voidaan arvioida tapahtumien ja samalla vaihtoehtoisten tulevaisuuksien todennäköisyyksiä. Todennäköisyyksien arviointi edellyttää puhtaasti laskennallisten menetelmien lisäksi myös luovaa tieteellistä mielikuvitusta, jotta vaihtoehtoiset vielä tuntemattomat tulevaisuudet kyetään kuvaamaan edes jollain tasolla. (Niiniluoto, 1993)

Ennakoinnin tarve perustuu toimintaympäristön (ts. maailman) dynaamisiin ajallisiin, tilallisiin ja rakenteellisiin muutoksiin, jotka tarjoavat tilaisuuksia synnyttäen uusia mahdollisuuksia toimijoiden tarkoituksille, kiinnostuksenkohteille ja tavoitteille valinnan vapauden periaatetta toteuttaen. Edellä kuvatut muutokset niiden kohteineen, suuntaliikkeineen, tekijöineen ja nopeuksineen voivat olla ennakoitavissa. (Malaska, 2013, viittaa Flechtheim, 1966)

Muutoksen syntymistä on pyritty kuvaamaan ns. tulevaisuuskolmiolla, jossa aiempi toiminta asettaa ehtoja tulevalle toiminnalle ja siten myös tulevaisuuden syntymiselle. Reunaehtoja voivat asettaa käyttöön valitut säätely- ymv. järjestelmät. Muutosta voidaan pyrkiä sekä tiedostamatta että tarkoituksellisesti vastustamaan, lieventämään, torjumaan ja estämään. Muutosnopeutta voidaan myös haluta viivästyttää, mutta siitä huolimatta tulevaisuus on jo olemassa. Tästä ilmiötason esimerkkinä on mm. ilmastonmuutos tai tekoälyteknologioiden käyttö. (Dufva & Rowley 2022)



Kuvio 9 Tulevaisuuskolmio, mukaillen Dufva & Rowley, 2022, viittaa Inayatullah, 2008

Edellä kuvatun mukaisesti tarvitaan tietomallien muodostamiseksi dataa menneestä, olemassa olevasta, nykyhetken tilanteesta sekä tulevasta. Ennen kuin uhkatiedon keruuta voidaan ryhtyä suorittamaan, tulee ymmärtää menneisyyden, nykyhetken ja oletetun tulevaisuuden vaikutus mahdolliseen tulevaisuuteen. Uhkien torjunnan kyvykkyys on edellä kuvatun mukaisesti vahvasti sidoksissa aikaan, sillä torjunnallisen toimenpiteen oikea-aikaisuus syntyy toiminnan suhteuttamisesta sekä reagoinnin nopeudesta tapahtumaan (Halonen, 2015, viittaa Hackathon, 2004). Tällöin reagointiviiveellä voi olla arvoa lisäävä tai vähentävä vaikutus.

Uhkatiedon kerääminen palvelee myös riskienhallintaa, sillä tiedon järjestämisen ja käsittelyn avulla voidaan muodostaa tunnuslukuja ja funktioita nimenomaisesti tulevaisuuden arvioiden laskemiseksi. Tämä näkyy erityisesti operatiivisten riskien mittaamisessa ja seurannassa, jolloin puutteellisista tai epäonnistuneista toiminnallisista, inhimillisistä tai järjestelmäprosesseista aiheutuvan menetyksen tai tappion riskille annetaan oletusarvo. (MSO, 2014)

5.4 Teknologinen analyysikyvykkyys uhkien hallinnassa

Jo vuosituhannen alkupuolella havaittiin (Mayer, Steinecke & Quick, 2011, viittaa Fuld, 2003), että valtaosa organisaatioista yllättyi toimintaympäristön muutosten voimakkuudesta ja vaikutuksista omaan toimintaan puutteellisen tiedonkeruun tai tiedon hyödyntämisen seurauksena. ICT-järjestelmien, erityisesti analyysi- ja analytiikkajärjestelmien vaatimusmäärittelyissä ei kenties ole osattu ottaa huomioon tietotarpeiden laajuutta ns. 360 asteen tutkanäkymän tapaan tai heikkoja signaaleja ei ole osattu kääntää käytännön indikaattoreiksi. Syy-seuraussuhteet jäävät todentamatta, mikäli tiedonkeruussa ja -prosessoinnissa on jouduttu säästämään esim. kaupallisten tietokantojen korkeiden lisenssikustannusten vuoksi. Järjestelmien käyttöliittymät ja rajapinnat ovat voineet olla puutteellisesti suunniteltuja, jolloin käyttöaste jää matalaksi tai visualisoitua tietoa on vaikeaa jatkojalostaa. Datatieteelliset ja matemaattiset tulosesitykset voivat olla epäyhteneviä suhteessa heuristisiin ja asiantuntija-arvioihin, mikä vaikeuttaa päätöksentekoa. Mahdollisuudet ja uhat tulisi saattaa samalle näkymälle ts. samaan portfolioon arvioinnin ja päätöksenteon helpottamiseksi. Järjestelmäratkaisuissa olisi tuettava myös skenaarioiden visualisointia. Luotettavuuden kannalta erityisen tärkeää on harjoittaa retrospektiivistä tietojen ja tulosten tarkastelua sekä varmistaa tarkastelun kattavuus tietojen riittävän laajan jakamisen kautta. (Mayer, Steinecke & Quick, 2011)

Tunnistamalla omassa toiminnassaan edellä kuvatut haasteet ja hyödyntämällä tiedon käsittelyyn ja toiminnan turvallisuuteen liittyviä viitekehyksiä, voivat toimijat muodostaa tietomalleja digitaalisen tietojenkäsittelyn pohjaksi. Tietomalleja voidaan hyödyntää

aiemmissa alaluvuissa esitetyn mukaisesti ennustavina sisältäen tietoa tulevista tapahtumista, ohjaavina tukemaan optimointia ja päätöksiä toteutettavista toimenpiteistä sekä kognitiivisina informoimaan ja visualisoimaan esim. koneoppimiseen pohjautuvien teknologioiden avulla sellaisesta, mitä ei vielä tiedetä.

Liiketoiminta-analytiikka on lähtökohtaisesti eräs yleisimmistä yritystoimijan tiedon käsittelyyn liittyvistä käsitteistä. Se on perinteisesti jaettu kuvailevaan, ennakoivaan ja ohjaavaan analytiikkaan. Kuvailevan liittyessä menneen ja nykytilan raportointiin tuotetaan ennakoivalla analytiikalla tietoa siitä, mitä on tapahtumassa ja mistä syystä. Ennakoivaa analytiikaa toteutetaan tiedon-, sisällön- ja medianlouhinnan teknologioin, mm. tunneanalyysin (engl. sentiment analysis[3]) tai mielipidelouhinnan keinoin. Viimeksi mainittua sovelletaan erityisesti markkinoinnissa ja asiakaspalvelussa sekä viestintämedioissa luokittelemalla koneoppimisen kielimallien avulla ilmaisuja esim. myönteisiksi, kielteisiksi tai neutraaleiksi. Näin voidaan järjestelmällisesti tunnistaa ja analysoida kokemuksellisia tietoja sekä sidosryhmien tunnetiloja, mielipiteitä ja asenteita. Ohjaavan ylimmän tason analytiikan simuloivilla ja optimoivilla sekä päätöksentekoa mallintavilla välineillä pyritään organisaation kannalta parhaisiin mahdollisiin päätöksiin ja toimenpiteisiin. Analyysikyvykkyys muodostuu edellä kuvatun yhteistoiminnasta kerätä ja käsitellä sekä organisaatiosta itsestään että sen toimintaympäristöstä peräisin olevaa monimuotoista ja nopeasti muuttuvaa laajaa tietomassaa. (Sharda, Delen & Turban, 2018)

Edellä kuvattua analytiikkaa toteuttavien sosioteknisten järjestelmien painopiste on enemmän tietämysteknologissa kuin tuotantoteknologissa ratkaisuissa. Järjestelmien tulee tarjota ratkaisuja työssä kohdattavien poikkeavuuksien käsittelyyn sekä tehtävienhallinnan että analyysin keinoin. Tämä ilmentyy organisaation järjestelmäkokonaisuudessa sen elementtien keskinäisen vuorovaikutusten diagnosoivina ja analysoivina toiminnallisuuksina. Järjestelmän ympäristössä on tunnistettava toimintaan vaikuttavat keskeiset tekijät, tyypilliset ongelmat, elementtien näkyvimmät vuorovaikutussuhteet,

[3] Finto https://finto.fi/mesh/fi/page/D000090042?clang=en ja https://finto.fi/mesh/fi/page/D000090042

organisaation merkittävimmät vahvuudet suhteessa sen ympäristöön sekä sen ilmeisimmät heikkoudet. (Appelbaum, 1997, viittaa Perrow, 1967)

Uhan ollessa mikä tahansa mahdollisesti toimintaa, tavoitetta tai resursseja haittaava vaikutus, olosuhde tai tapahtuma, käynnistyy niiden tunnistaminen sekä niihin vastaaminen aina torjunnan kannalta hyödyllisten tietojen keräämisellä luotettavista lähteistä. Kerättyä tietoa tulkitaan organisaation ja sen toiminnan kontekstissa, ja uusilla tiedoilla arvioidaan sekä täydennetään aiemmin luotuja uhkaprofiileja. Uhkaprofiilissa uhka on luonnehdittu ja tyypitelty sen todennäköisen aikomuksen, kyvykkyyden, haittavaikutuksen ja kohteen perusteella. Profiloinnin avulla vaikutetaan uhkien tunnistamiseen, riskianalyysiin sekä tilannekuvan rakentamiseen. Uhkien hallinnan ensimmäisenä edellytyksenä on sisäisten ja ulkoisten tiedonlähteiden tunnistaminen ja yksilöinti vähintään tapauskohtaisesti. Uhasta kattavasti tietoa tuottavia tietolähteitä kohdellaan ensisijaisina ja niitä seurataan aktiivisesti. Uhkatietoa kerätään ja tulkitaan järjestelmällisesti uhkien ja kohteidensa tunnistamiseksi, analysoimiseksi ja asettamiseksi tärkeysjärjestykseen. Uhkien vaikutukset toiminnalle osoitetaan ja organisaation toiminnan kannalta merkityksellisten uhkien vastatoimet määritetään. Uhkavaste sisältää ennalta määrättyjen vastatoimien toteuttamisen. Uhkaprofiili muodostetaan uhkien tunnistettujen ominaisuuksien, kuten uhkatoimijatyyppien, motiivien, tavoitteiden, kyvykkyyksien ja uhkien kohteiden avulla, ja sitä päivitetään toimintaympäristön tapahtumien ja järjestelmämuutosten pohjalta. Tiedot uhista suojataan ja niitä vaihdetaan turvallisella ja mahdollisimman ajantasaisella tavalla eri sidosryhmien ja analysointikeskittymien kanssa nopean ja kattavan reagoinnin mahdollistamiseksi. (U.S. Department of Energy, 2022)

Tilannetietoisuutta rakennetaan dynaamisessa toimintaympäristössä uhkien ajantasaisen havaitsemisen ja uhkavasteen pohjalta, jossa ennalta määrätyt reagointitoimenpiteet ovat sovitettu suhteessa toimintaympäristössä tapahtuviin muutoksiin. Kyvykkyys liikkua joustavasti reagoinnin eri tilojen ja toimien välillä takaa tehokkaan ja oikeansuhtaisen vasteen tuottamisen uhkiin. Reagoinnin kehittämiseksi toimintaympäristön uhka-

tapahtumia seurataan ja lokitetaan eli koostetaan niistä ajantasaista ja aikajärjestyksellistä tietoa. Tietoa kartutetaan tapahtuman ajankohdasta, aiheuttajista ja vaikutuksen laajuudesta, jotta pystytään tietämään mitä tapahtui, kenen toimesta ja milloin sekä ymmärtämään tapahtuman tarkoitusperiä ja juurisyitä (Kyberturvallisuuskeskus, 2024a). Keskitetysti kerätyn ja hyödynnettävän tiedon avulla parannetaan mahdollisuutta havaita tiedon osista muodostuvasta suuremmasta tietokokonaisuudesta keskenään korreloivaa asiayhteyttä, erottaa poikkeavat tapahtumankulut normaaleista ja havaita pitkän aikavälin kehitystä (Kyberturvallisuuskeskus, 2024a). Seurannan tulee perustua uhkaprofiileihin toimenpiteiden kohdistamiseksi tärkeimmiksi valittuihin kohteisiin. Seurattavien tietojen ajanmukaisuutta ja kattavuutta sekä tietojen pohjalta luotujen tiedotusten (hälytykset) tarkoituksenmukaisuutta tarkastellaan ja arvioidaan säännöllisesti. Tapahtumahälytysten (esim. kynnysarvojen ylitys ym.) ja varoitusten asetuksia päivitetään uhkien havaitsemisen ja tunnistamisen vaatimusten mukaisesti. Toimintaympäristön muutosta ja poikkeamaa osoittavat tiedot (indikaattorit) määritetään ja niitä päivitetään havaittujen kehityskulkujen ja suoritettujen uhka- ja riskianalyysien pohjalta järjestelmällisesti. (U.S. Department of Energy, 2022)

Tilannetiedon saatavuus varmistetaan määrittämällä tiedontarve sekä jakamisen menetelmät, kanavat ja vastuut sekä sisäisten että ulkoisten sidosryhmien kesken. Tiedonjakamisen käytännöistä sovitaan normaali- ja poikkeusolot sekä hätätilat huomioiden. Jaettavaa tilannetietoa yhdistetään ja koostetaan siten, että sen pohjalta on mahdollista muodostaa kokonaiskuva seurannan sekä yhteisymmärrys toiminnan ja vasteen tiloista. Suojaavat turvatoimet vakiinnutetaan luottamuksellisten, arkaluontoisten ja turvallisuusluokitettujen tietojen välitystä varten. Tiedot esikäsitellään siten, että niiden keskinäiset ristiriitaisuudet, huonolaatuisuus tai tietopuutteet tulevat huomioiduksi analyysissa. Tiedon analyysiin on osoitettu riittävät inhimilliset ja tekniset resurssit. Tiedon visualisointi ja raportointi toteutetaan mahdollisimman lähellä reaaliaikaisuutta (*near-real-time*) olevan tiedon tuottamisen ja toimittamisen tarpeita vastaavasti. Tiedon esittämisessä päätöksentekijöille hyödynnetään tilannekuvaan pohjautuvia työpöytänäkymiä. (U.S. Department of Energy, 2022)

Organisaation keräämää monilähteistä tietoa hyödynnetään toimintaympäristöön kohdistuvaan tiedustelulliseen analyysiin. Tietoa kerätään monipuolisesti tuotanto- ja toimitusketjusta kattaen taloudelliset, poliittiset, sosiaaliset ja ympäristöön liittyvät ulottuvuudet. Tiedonhankintaa toteutetaan eri muotoisena inhimillisestä havaitsemisesta kuvien, signaalien ja avointen lähteiden tietojen käsittelyyn. Hankittu tieto jalostetaan sisäisille ja ulkoisille sidosryhmille jaettaviksi tietotuotteiksi mahdollisimman kattavaa uhkien- ja riskienhallintaa varten. (NIST, 2020)

Toimintaympäristön ja itselle tärkeiden kohteiden tietojen keräämistä, käsittelyä ja jakamista tehdään tiedonkäsittelyn ja tietoliikenteen teknologioiden mahdollistamana kaikkialla ja kaikkien toimesta ja siten ei yksinomaan esim. muiden toimintaympäristön toimijoiden tai eriytettynä tiedustelun ja turvallisuuden erityisalojen ja näiden omien organisaatioiden toimesta. Tämä aiheuttaa myös datan määrän jatkuvaa kasvua suhteessa inhimilliseen tiedonkäsittelykykyyn. Se mitä aiemmin tehtiin käsityönä ja inhimillisen päättelyn, intuition tai heuristiikkojen avulla, on osattava määritellä digitaalisiksi tehtäviksi koneellisten ja laskennallisten analyysien mallintamiseksi. Mikäli digitaaliset mallit eivät olekaan kattavia tai yhteensopivia ihmisen mentaaliseen malliin, jää hyöty uusien teknologioiden, kuten tekoälyn, soveltamisesta riittämättömäksi. Huolimatta siitä, että mallien muodostamisessa onnistuttaisiin, jää riski monimuotoisen ja -lähteisen datan käsittelyyn ja noutamiseen käyttöön aina tarvittaessa tilanteen vaatiessa useilla erilaisilla tietoteknisillä ratkaisuilla, sillä yksi järjestelmä ei taivu kaikkeen. Tämä toisaalta puoltaa tiedon keräämistä, käsittelyä, jakamista ja tärkeysjärjestykseen asettamista hajautetusti, kohdekohtaisesti tai erikoistuneiden toimintayksikköjen toimesta. Järjestelmäratkaisuissa täytyy kuitenkin tällöin olla vahva tuki datan luokittelulle ja indeksoinnille, varastoinnille sekä ajanmukaiselle visualisoinnille tietojen koostamista ja yhdistämistä varten. (Vinci, 2020; Katz, 2020a ja Katz, 2020b)

Suurten ja toisistaan poikkeavien datamassojen hyödyntämistä voi lisäksi haitata toimijoiden riippuvuus vanhoista (engl. legacy) tietojärjestelmistä, tietämättömyys uusista tiedon hyödyntämisen käytännöistä ja teknologioista sekä joidenkin yksittäisten toimintojen priorisointi tai osaoptimointi (Pherson & Pherson, 2017). Pelkän teknologisen analyysikyvykkyyden varaan ei voi kuitenkaan jättäytyä inhimillisen analyysiresurssin kustannuksella, sillä laadukas analyysi pohjautuu kriittiseen inhimilliseen ajatteluun, asiayhteyteen ja arviointiin päätöksentekoa varten, joilla torjutaan teknistä analyysitulosta vääristävää tai sen laatua heikentävää epämääräistä, epäluotettavaa, epätäydellistä, vanhentunutta, virheellisesti syötettyä tai tulkittavissa olevan data vaikutusta (Pherson & Pherson, 2017).

Suurten datamassojen käsittely ei myöskään suoraan paljasta asioiden tai tekijöiden syyseuraussuhteita, monimutkaisuutta, tarkoitusperiä tai aikomuksia, vaikka se paljastaakin korrelaatioita. Välitön arvo tulee siitä, että datamassojen käsittelyllä voidaan vastata kysymykseen "mitä", eikä niinkään pyrkimällä saamaan vastausta kysymykseen "miksi". (Katz 2020b)

Inhimillistä osaamista tarvitaan mallissa sovellettavien tietokenttien tunnistamiseen, tiedon puhdistamiseen sen laadun ja käyttövalmiuden varmistamiseksi sekä tuloksellisten algoritmien laadintaan. Datakokonaisuuden heikot kohdat ja uudet käyttömahdollisuudet täytyy osata tunnistaa ja niistä osata viestiä teknistä rakentamista varten. Eri teknologioiden, kuten mm. datanlouhinta ja -fuusio, luonnollisen kielen käsittely, kuvan ja puheentunnistus, sosiaalisen median analysointi, todennäköisyys- ja kvanttilaskenta sekä koneoppiminen, osaamisesta tulee kilpailuvaltti (Vinci, 2020). Koneoppimista ja automatisointia hyödyntävät itsenäiset järjestelmät toteuttavat analyysiprosessia tai vähintään sen keskeisiä osia, jolloin niiden merkitys teknisten asiaintuntijaroolien (esim. datatieteilijät, integraatio-, tietokanta- ja koneoppimisasiantuntijat ymv.) ja toiminnallisten asiantuntijaroolien (analyytikot, liiketoimintavastaavat ymv.) yhteensaattajina ja vuorovaikutuksen edistäjinä kasvaa. (Katz, 2020a)

5.5 Uhkien havaitsemista tukevan tietotuotteen kehittämisessä huomioitavia seikkoja

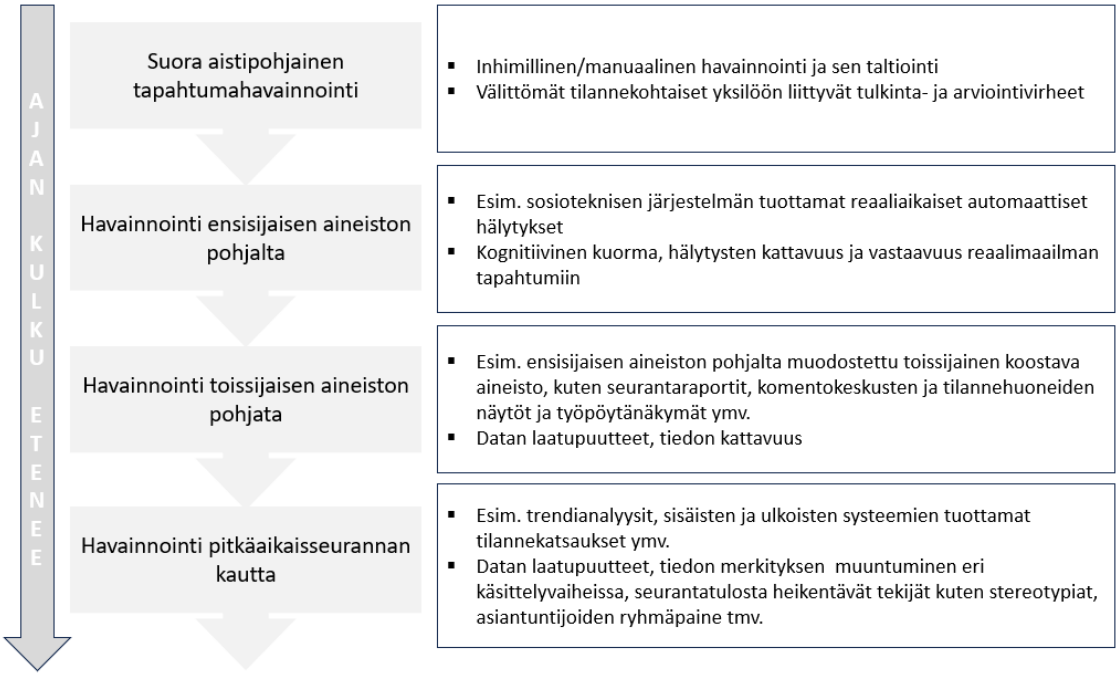
Tilannetietoisuuden muodostamiseksi on välttämätöntä kerätä tietoa riittävän laajalti, kuten edellä tuodaan useaan otteeseen esille. Monialaisten ja -ulottuvuuksisten kyberuhkien seuranta ja analysointi edellyttää suurten tietojoukkojen käsittelyä ja visualisointia. Painotus on ollut paljolti teknisessä ulottuvuudessa perinteisten kyberturvallisuusmenetelmien keskittyessä fyysiseen ja virtuaaliseen infrastruktuuriin (mm. laitteistot, koodit). Uhkien sosiaaliset, poliittiset, taloudelliset ym. ulottuvuudet on kuitenkin otettava enenevässä määrin huomioon kokonaiskäsityksen saamiseksi uhkatilanteesta.

Uhkien havaitsemisen ja toimintaympäristön tuntemisen kyvykkyyksillä on suora yhteys organisaation menestymiseen ja selviytymiseen. Mitä enemmän käytetään erilaisia pistemäisiä ja toisistaan erillään olevia hajautettuja järjestelmäteknisiä ratkaisuja eri kohdealueiden tietojen keräämiseen ja visualisointiin, sitä enemmän tulee haasteellisemmaksi sovittaa tietoa yhteen sekä laadullisesti että määrällisesti tai muodostaa niille merkitystä ja painoarvoa laajan datamassan kokonaisuudessa manuaalisin tai toisistaan erillään olevien käsittelyprosessein. Tästä syystä fuusioalustaratkaisu, joka tarjoaa tietojen nopean koostamisen, yhdistämisen ja visualisoinnin yhteiset toiminnallisuudet automatisoituna, helpottaa monilähteisen ja -ulottuvuuksisen tiedon tulkintaa ja luo edellytyksen toimintaympäristön ajantasaiselle ymmärtämiselle. (Sharda, Delen & Turban, 2018)

Erilaisten tietotyyppien kerääminen ja analysointi kultakin eri ulottuvuudelta aiheuttaa mittavia toiminnallisia ja metodologisia haasteita, joita voidaan ratkaista datan fuusiomenetelmien hyödyntämisellä. Datafuusiolla tarkoitetaan tietojen yhdistämisen prosessia, jossa useita erilaisia tietolähteitä yhdistetään sellaisen analyysin ja ymmärryksen tason saavuttamiseksi, joka ei olisi mahdollista yhdellä datapisteellä. Fuusiotekniikat sekä nopeasti kehittyvät jäsenneltyä ja jäsentämätöntä tietoa käsittelemään pystyvät dataanalytiikan ja visualisoinnin alustat tarjoavat uusia mahdollisuuksia kyberavaruuden uh-

kien teknisten, sosiaalisten ja poliittisten ulottuvuuksien tutkimiseen. Tietojen yhdistäminen on monitasoinen ja -tahoinen prosessiksi, joka käsittelee useista lähteistä peräisin olevia tietoja automaattisen havaitsemisen, yhdistämisen, korrelaation ja arvioinnin menetelmin. Data-termin asemasta voidaan käyttää tieto-termiä (engl. information fusion), jolloin fuusion merkitys kattaa sen teorian, tekniikat ja työkalut useiden lähteiden (esim. sensorit, tietokannat, ihmisten tuottamat tiedot ymv.) muodostaman synergian tuottamiseksi siten, että toiminnan tulos on parempi tai yhteisöllinen merkitys suurempi kuin hyödynnettäessä vain yhtä lähdettä. Näin ollen fuusiomenetelmät kattavat useita erilaisia omat määrityksensä ja terminologiansa omaavia tieteenaloja. (McMahon, Rohozinski & Canada, 2013, viittaa U.S. Department of Defence, 1991 ja Dasarathy, 2001)

Tällaisella tietolähteitä ja visualisointeja yhteen kokoavalla kognitiivisella arkkitehtuurilla pyritään simuloimaan inhimillisen havaitsemisen ja tulkinnan rakennetta datan jalostamisessa tietoudeksi ihmisen ja koneen välisessä vuorovaikutuksessa havaittavuuden, hallittavuuden ja tilannetietoisuuden kontekstissa (Fernandez ja muut, 2017). Alla olevassa kuviossa on tutkijan oma karkea tulkinta siitä, miten havainnointi jakaantuu inhimilliseen aistipohjaiseen ja konepohjaiseen havaitsemiseen.



Kuvio 10 Havainnoinnin ajalliset tasot ja mahdolliset vaikeudet

Havaitsemista tukevat erityyppiset visualisoinnit sisältävät ns. yhdellä silmäyksellä nähtävää tai yleiskatsauksenomaista tietoa tilasta, attribuuteista ja tarkkailtavan ympäristön dynamiikasta, ja vastaavat kysymyksiin ”Mitä ympäristössä on tapahtumassa?” (Sharda, Delen & Turban, 2018). Suurien organisaatioiden valvomot voivat käsitellä jopa tuhansia teknisiä hälytyksiä vuorokaudessa. Näistä kaksi kolmasosaa voi olla jatkotoimia aiheuttamattomia noin kolmasosan edellyttäessä inhimillistä arviointia. Tietokuormitus johtuu teknisten järjestelmien puutteellisista kyvyistä suodattaa hälytysten laukeamisen aiheuttavaa oleellista tietoa havaituista poikkeavuuksista. (Francis, 2017)

Automatisoidun tiedonkäsittelyn sekä analyysijärjestelmäpuutteiden tuottamien väärien hälytysten ohella tiedonkulkua ja havaitsemista voivat haitata viiveet hälytysten toimittamisessa ja vastaanottamisessa, tiedon visualisoinnin ongelmat, puuttuvat sisältötiedot ja puutteet niiden päivitys-, muutos- ja korjaustoiminnallisuuksissa sekä varoittamisen ja tilanne- ja riskiarvion perustuminen pelkkään ennusteeseen huomioimatta itse havaintoa (Huovila ja muut, 2010). Lisäksi havaitsemiseen vaikuttavat oleellisesti tiedon

kattavuus (tietolähteiden määrä ja laatu) sekä tietovirtojen käsittelyn ja havainnollistamisen tekninen tehokkuus. Havaitsemista vaikeuttavat puutteet havaintotiedon laadussa ja saatavuudessa, ylimääräinen samanaikainen tiedon kuormitus (esim. suoranainen häirintä), ennakkoasenteet ja havaitsemista ohjaavat odotukset sekä puutteet tarkkailun ja seurannan kohdistamisessa. Nämä voivat saada aikaan havaintovääristymiä, olennaisten havaintojen erottelukyvyn menetystä sekä keskeisen havaintotiedon jäämistä pimentoon, mitkä johtavat tilannetietoisuuden menettämiseen. (Himanen, 2013, viittaa Endsley, 1988 ja 1995, Jones & Endsley, 1996, Oksamaa, 2012 ja TSTJSOM, 2010)

Työskentely tilannekeskusten, kuten energiantuotantolaitosten valvomoiden ja organisaatioiden operatiivisten johtokeskusten kaltaisissa ympäristöissä on luonteeltaan monimutkaista ja dynaamista johtuen jatkuvista muutoksista havaintoympäristössä. Käyttäjien on reagoitava nopeasti ja tehtävä päätöksiä ajan paineessa. Tilannekuvan on oltava täydellinen ja tarkka. Tilannetietoisuus muodostuu havaitsemiskyvystä eli esimerkiksi varoitussignaalien kuulemisesta tai hälytysmerkkien näkemisestä näytöllä. Lisäksi käyttäjän on kyettävä keskittämään huomionsa havaittuun tietoon ja tulkitsemaan tilanteen muutoksia. Käyttäjän on saatava mielikuva tilanteesta ja ylläpidettävä sitä sekä kyettävä arvioimaan mahdollisia muutoksia ja odottamattomia tapahtumakulkuja (SKYbrary, 2019). Käyttäjän kognitiiviset toiminnot on tunnistettava tietyn vaaditun tehtävän tai työn suorittamiseksi sekä varmistettava, että työympäristö on sopiva tehtävävaatimuksiin. (Kalakoski, 2016)

Tilannetietoisuuden päätehtävät koostuvat kognitiivisista tehtävistä, kuten seurannasta ja havaitsemisesta, tilanteen arvioinnista, reagoinnin suunnittelusta ja reagoinnin toteuttamisesta. Seuranta ja havaitseminen puolestaan koostuvat toiminnoista, jotka liittyvät tiedon saamiseen ympäristöstä. Nykyisissä prosessijärjestelmissä näitä tehtäviä tuetaan erilaisten anturien ja signaalinkäsittelymenetelmien avulla, joiden avulla poimitaan tietoa järjestelmien dynaamisesta ympäristöstä. (Naderpour, Nazir & Lu, 2015, viittaa O´Hara ja muut, 2011)

Sensoriteknologiaa hyödyntävien järjestelmien ja laitteiden käytön lisääntyessä tuotetaan samalla lisää hälytystoiminnallisuutta, jolloin käyttäjä voi väsyä toistuviin hälytyksiin (Gaba, Lau & Desaulniers, 2013). Hälytysväsymyksellä tarkoitetaan käyttäjän siedättymistä hälytysärsykkeeseen, mikä aiheuttaa aistikuormitusta ja johtaa hälytysvasteen ts. reagoinnin viivästymiseen tai puuttumiseen (West, Abbott & Probst, 2018).[4]

5.6 Tiedonhankkimistekniikoita

Uhkien ja myös riskien hallinnassa tiedon saatavuuden merkitys on suuri. U.S. National Institute of Standards and Technology (NIST) ja the North American Electric Reliability Corporation (NERC) energiatoimialalle (sähköntuotanto) kehittämän riskienhallintamallin mukaisesti organisaation liiketoimintatavoitteiden saavuttamisen yhtenä edellytyksenä on kyberturvallisuusriskien hallinta. Ko. riskienhallintamalli korostaa sitä, että nimenomaan tietopohjaisella, organisaation läpikattavalla päätöksenteolla voidaan tehostaa resurssijakoa, toiminnallista tehokkuutta sekä uhkiin ja riskeihin varautumista ja vastetta. (NIST, 2012)

Uhkamallintaminen tuottaa tietoa riskienhallinnan lisäksi myös liiketoiminnan päätöksentekoa tukevaan analytiikkaan, johon tulee kerätä monipuolista tietovarantoa uhkiin varautumisesta sekä riskienhallinnasta organisaation sisältä ja sen toimintaympäristöstä (MSO, 2014). Uhkamallinnusprosessi etenee uhkatoimijaan ja sen toiminnan tunnistamiseen ja määrittämiseen liittyvästä tiedonkeruusta uhan arviointiin ja lopulta torjuntatoimien suunnitteluun (OWASP, 2024).

Tiedonhankkimiseen liittyviä menetelmiä, viitekehyksiä ja käsitteitä on lukuisia, mm. potentiaali-, kilpailija- tai toimija-analyysi. Asiakkaan tunteminen ja tunnistaminen (engl.

[4] Vrt. esim. sairaalaympäristössä tehdyn tutkimuksen mukaan hoitohenkilökunta ei vastannut 70 %:iin lääkinnällisten laitteiden ja järjestelmien hälytyksistä (n=400 hälytystä). Kolmestakymmenestäneljästä merkittävästä, mahdollisesti henkeä uhkaavasta tilanteesta ilmoittavasta hälytyksestä 41 %:iin ei vastattu välittömästi. ECRI Institute; Clinical Alarms, 23.12.2013, Healthcare Risk, Quality, & Safety Guidance – Guidance, 23 December 2013. https://www.ecri.org/components/HRC/Pages/CritCare5.aspx?tab=2

Know Your Customer, KYC) on erityisesti finanssialalla sovellettu menetelmä sidosryhmien riskienhallintaan (FCA, 2024). e-KYC viittaa sähköisten menetelmien avulla suoritettaviin asiakkaan tunnistamisen digitalisiin todentamisprosesseihin (FATF, 2017). Suomessa asiakkaan tuntemista ohjaa erityisesti Laki rahanpesun ja terrorismin rahoituksen estämisestä 28.6.2017/444, jonka kolmannessa luvussa kuvataan tuntemiseen ja tunnistamiseen liittyviä toimijoiden velvoitteita (Finlex, 2024).

Sähkömarkkinatoimijat keräävät mm. markkinointi- ja asiakkuustietoa mm. asiakkaidensa kanssa käytävien puhelinkeskustelujen, verkkokyselyiden, sosiaalisen median, sähköpostiviestinnän ja muiden kontaktipisteiden kautta. Asiakasviestintää voidaan tukea myös energiatuotteiden ja -palveluiden käytön automaattisen tiedonkeruun (mm. älysähkömittarit) avulla. Toimintaympäristön tietoekosysteemi on siten suuri eri sidosryhmien tuottaessa tietoa. Energiatoimialan muutosnopeuden vuoksi markkinakilpailuasetelma on korostunut toimintamahdollisuuksien houkutellessa yhä enemmän uusia liiketoimintariskejä ottavia toimijoita. (Sharda, Delen & Turban, 2018)

Toimintaympäristön muuttuessa mm. edellä mainitun kilpailuasetelman vahvistumisen myötä tulee uhkatiedon hallinnasta vakiintunut osa liiketoimintatiedon hallintaa, mikä puolestaan muodostuu liiketoiminta-analytiikasta eli liiketoiminnan päätöksentekoa tukevasta tiedonkäsittelyn tavasta faktapohjaisten järjestelmien avulla (Meretvuo, 2021, viittaa Dresner, 2015). Uhkatietoa hankitaan tiedustelullisin keinoin organisaation johdon ohjaamana, sen analysoinnista ja sen jakelusta päätöksiä tekevälle taholla, jolloin puhutaan liiketoimintatiedustelusta (Meretvuo, 2021, viittaa Carlisle, 2005).

Uhkatiedustelulla tarkoitetaan tutkimuksellista tietokoostetta uhista, niiden toteuttajista (toimijat) ja käytetyistä menetelmistä ja välineistä, jota hyödynnetään kohteena olevan organisaation uhkavasteessa eli uhkien havaitsemissa ja tehottomaksi tekemisessä ennen kuin uhkatoimija saavuttaa tavoitteensa. Edellä kuvattua laajaa näkökulmaa pyri-

tään enenevässä määrin käyttämään kyberturvallisuuden toimialalla pelkästään teknologiaulottuvuuteen keskittyvän näkökulman asemasta. (McMahon, Rohozinski & Canada, 2013)

Edellä kuvatun mukaisesti voidaan ajatella olevan olemassa myös yrityksiin kohdistuvaa vakoilua sekä sen torjumiseksi toteutettavia estämiseen, havaitsemiseen, harhauttamiseen ja neutralisointiin liittyviä toimia eli vastatiedustelua. Yritysvakoilun havaitsemisessa pyritään tunnistamaan tapahtunut asia sekä siihen liittyvät henkilöt, organisaatiot, olinpaikat ja sijainnit, ja keräämään todisteet tästä. Havaitsemiseen sisältyy myös vastatarkkailua eli pyritään havaitsemaan henkilöstöön ja toimitiloihin kohdistuva ulkopuolinen tarkkailu mm. yritys-/organisaatioturvallisuuden toteuttamin keinoin. Kontrolli- ja estämistoimien tehtävänä on myös osoittaa toimien läpäiseminen. Nämä faktatiedot, ml. myös esim. rikospaikkatiedot, rakentavat uhkatiedonhallinnan kokonaisuutta. (Meretvuo, 2021, viittaa Prunckun, 2012)

Yritysvakoilun kohteena oleminen voidaan havaita esim. seuraamalla pimeän verkon anastettuja liiketoimintatietoja ja -salaisuuksia kauppaavilla markkinasivustoilla. Toimintaympäristön muutostilanteet, kuten esim. menetetty kilpailuasema, pienellä erolla hävityt kilpailutukset, osake- ja markkinaosuusheilahtelut, henkilöstön siirtyminen kilpailijalle, kilpailijan viestinnällinen samankaltaisuus tai katoavat asiakkaat voivat kertoa yritysvakoilun kohteena olemisesta. (Meretvuo, 2021)

Edellä olevan mukaisesti tiedon hankinta on laajaa ja tiedonhallinnan kannalta kapasiteetikas ja kyvykäs tietotekninen ratkaisu on avainasemassa. Fuusiojärjestelmää voi kehittää edelleen järjestelmien järjestelmäksi. Tällä käsitteellä (engl. System of Systems) tarkoitetaan vastaanottavia, ohjaavia, yhteiskäyttöisiä tai virtuaalisia järjestelmäkokonaisuuksia, joiden valvonnan, johtamisen ja tiedonvälityksen elementit toimivat itsenäisesti tukien tilannetietoista päätöksentekoa (Pöyhönen 2020, viittaa U.S. Department of Defense, 2008). Tilannetietoisuuden saavuttaminen riippuu tietolähteiden tuottaman tiedon käsittelykyvystä.

Tiedon keräämistä toimintaympäristöstä ja kybermaailmasta voidaan toteuttaa eri menetelmillä datan lähteestä, tyypistä ja sisällöstä riippuen. Fyysisen kerroksen muodostavista tietokoneista, palvelimista ja muista tietoliikenneverkon rautainfrastruktuurista on saatavilla tunniste- ja vuorovaikutustietoja esim. geograafisesti visualisoitavaksi. Tietoliikennepakettien seurannan ja lokitiedostojen avulla voidaan tunnistaa toimintaympäristöjen toimijaosapuolten verkkokäyttäytymistä, minkä lisäksi toimijoiden toimintakulttuurista ja sosiaalisesta käyttäytymisestä on saatavilla tietoa sosiaalisen median ja muiden palvelukanavien välityksellä tapahtuvan vuorovaikutuksen kautta. (McMahon, Rohozinski & Canada, 2013)

Eri lähteistä kerätty monimuotoinen data työstetään koneellisesti tai manuaalisesti käsiteltävään muotoon nimeämällä, luokittelemalla, ryhmittelemällä ja puhdistamalla sitä. Datan ja sen lähteen luotettavuutta, todenperäisyyttä ja todennäköisyyttä arvioidaan sekä asetetaan se tärkeys- tai merkitysjärjestykseen. Näin saatua datatulosta tarkastellaan edelleen ja asetetaan sen perusteella testattavia hypoteeseja. Dataa voidaan analysoida monin eri menetelmin näkökulmasta tai ulottuvuudesta riippuen ja nykyjärjestelmät tai analytiikka-alustat[5] tarjoavat jo sekä mm. tilasto-, verkosto-, geokoodaus-, geografiikka-, tila-, aika- ja kontekstianalyysityökaluja tai jopa API-rajapintapalveluita niihin. Erityisesti temaattisesti, ajallisesti ja maantieteellisesti yhdistelty ja visualisoitu data auttaa havaitsemaan tiettyyn toimintaympäristöön tai toimijoihin liittyvien tapahtumien, trendien ja uhkien kehittymistä. Automatisoidussa verkkoaineistojen sisältöanalytiikassa uudet luonnollisen kielen tekoälymallit sisältömoottoreineen helpottavat tapahtumatietojen keräämistä ja tukevat toimintaympäristön kehityskulkujen tulkintaa. Monipuolisia työkaluja tarjoavien analytiikka-alustojen käyttö edellyttää organisaation ja toimintaympäristöjen muutosten seurannan kannalta tarkoituksenmukaisen ontologian määrittämistä sekä kyvykkyyttä rikastuttaa kertyvää tietoutta ja omaa uhkatietovarantoa uusien

[5] Esimerkiksi tuotenimet: Apache (tuoteperhe), Palantir, i2 Analyst's Notebook, Maltego, Pajek, Gephi, GRAS, ymv.

datalähteiden yhdistämisen myötä. Alustaratkaisu tarjoaa yhteiskäyttöisen virtuaalisen ympäristön eri analyytikkorooleille ja lisää näin analyysitoiminnan kattavuutta. Asianmukainen järjestelmäratkaisu tukee myös päättelyn, johtopäätösten ja analyysin jäljitettävyyttä sallimalla läpinäkyvyyden eri prosessivaiheisiin aina tiedonkeruusta ja ensimmäisten hypoteesien tuottamisesta tulosten raportointiin asti. (McMahon, Rohozinski & Canada, 2013)

Toimintaympäristön tietojen keräämistä toteutetaan myös ns. avointen lähteiden tiedustelulla (engl. Open Source Intelligence OSINT) esim. perinteisestä julkisesta mediasta ja avoimesta tietoverkosta, millä osaltaan varmistetaan aiemmin havaitsematta jääneiden uhkien havainnoimista (Pöyhönen, 2020, viittaa Lee ja Shon, 2016). Mediamonitoroinnin lisäksi organisaation sisäisillä lähteillä, kuten esim. markkina- ja kilpailija-analyyseilla ja asiakas- ja sidosryhmäpalautteilla täydennetään uhkatietovarantoa.

Mitä enemmän erityisesti anonyyminä toimivaan uhkatoimijaan on liitettävissä määreitä ja lisätietoa, sitä enemmän saadaan tuotua esiin toimijan aikaan, paikkaan ja toimintaverkostoon liittyvää tietoa. Kyvyllä sitoa yksittäisiä tietoja toisiin tietoihin kasvatetaan havainnointikyvykkyyttä. Vahingoittamistarkoituksessa toimivat toimijat mukautuvat nopeasti ja tilannekohtaisesti suojautumis- ja torjuntatoimiin, minkä vuoksi on tärkeää lisätä uhkatoimijoita ja uhka-alaa koskevaa akateemista, valtiollista ja toimialayhteistyöverkostojen toteuttamaa tutkimusta. (Mission Support Center 2016, viittaa Clapper, 2016)

Tietojen käsittelyyn ja visualisointiin voidaan soveltaa myös erilaisia tekoälyteknologioita, joita jo nyt käytetään tukemaan mm. energian käytön ennusteissa sekä tuotannon, jakelun ja varastoinnin hallinnassa. Seuraamalla, keräämällä ja analysoimalla toimintaympäristöstä saatavaa tietoa sekä ennakoimalla tulevia tarpeita ja vallitsevia olosuhteita, voidaan tekoälyllä saada aikaan esim. energiankulutuksen vähentymistä ja siten myötävaikuttaa kestävään kehitykseen teollisuuslaitoksissa, yrityksissä ja kotitalouksissa. Integroi-

malla tekoälyä kiinteistö-, laitos- ja teollisuusautomaatiojärjestelmiin saadaan hyödynnettäväksi seurantatietoa suuria määriä toiminnan ja järjestelmien vakaannuttamiseen, optimointiin ja ennakointiin sekä poikkeama- ja häiriötilanteiden hallintaan. Esimerkiksi uusiutuvan, erityisesti sääolosuhteista riippuvan tuuli- ja aurinkoenergian tuottajat voivat hyödyntää tekoälyavusteisesti kerättyä ja analysoitua sää- ja satelliittitietoa tuotannon ennustamiseen, varastoinnin optimointiin sekä tarjonnan ja kysynnän tasapainottamiseen. (Rozite, Miller & Oh, 2023)

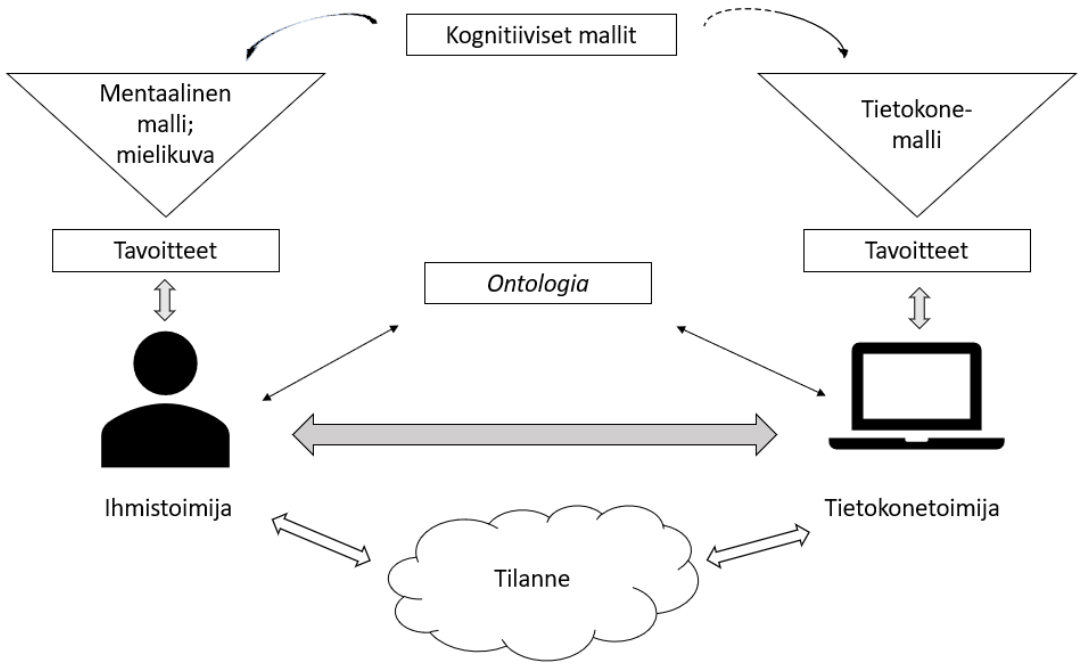
Tällaisessa toimintaympäristössä, missä tuotetaan inhimillisen käsittelykyvyn ylittäviä tapahtumamääriä taltiointia, seurantaa, lokitusta, hälyttämistä ja varoittamista varten, tulee haasteeksi riittävä ja tarkoituksenmukainen reagointi teratavuluokkaa olevan tietopaljouden vallitessa. Teknisiä taktiikoita, työkaluja, menetelmiä ja prosesseja tulee kehittää edelleen, jotta analyytikkojen inhimilliseen analysointiin jäisi enemmän aikaa ja analyysiresurssit kohdentuisivat tehokkaammin. Ihmisanalyytikoille ohjautuvaa datan määrää, muotoa ja laatua tulee optimoida, sillä koneen suorittamat analyysit eivät tällä ole vielä toiminnallisuudeltaan ja kattavuudeltaan riittäviä. Analysointi edellyttää ennen kaikkea ajattelemista omalle toiminnalle uhkaa tai vahinkoa aiheuttavan toimijan tavoin sekä luonteeltaan taistelullisen ja ketterästi tilanteisiin ja tapahtumakenttään sopeutuvan ajattelutavan omaksumista. (Johnson, 2019)

5.7 Tietoyhteistyöverkostot uhkien havaitsemisen apuna

Jaettua tilannetietoisuutta tuetaan toimintaympäristön toimijoiden välisellä tietojenvaihdolla, jota voidaan toteuttaa paikallisesti, alueellisesti tai globaalisti suojattujen tietoverkkojen ja - tietoliikenteen sekä autorisoitujen käyttäjien kautta. Toimijat tuottavat ja saavat kollektiivisesti uhkatietoa yli maantieteellisten rajojen tarvittaessa myös toimialoilta. Tämä kehittää puolustuksellista kyvykkyyttä tehokkaammin kuin pelkästään yksin eriytettynä toimien. Jaetun tilannetietoisuuden ratkaisuissa tulee päättää seurattaviin kohteisiin liittyvän datan keräämisestä, käsittelystä ja jakamisesta sekä datan luottamuksellisesta ja turvallisesta välittämisesti. (Mission Support Center, 2016)

Tietoyhteistyöverkoston toimijoiden keskinäinen vuorovaikutus tuottaa systeemitason tilannetietoisuutta. Franssila (2020) tutki hajautuneiden energiansiirtojärjestelmien (verkot) ohjaustyötä, jossa merkittävimmät haasteet liittyvät ympäristön tilasta tehtävien havaintojen keräämiseen ja kokoamiseen, sekä (Hakala, 2021) tiedon jakamisen esitystapaan ja tiedon määrään suhteessa tiedon ymmärrettävyyteen ja selkeyteen. Tiedot toimijoiden identiteetistä, sijainnista, toiminnan kohteesta sekä tehtävistä tulisi visualisoida havaitsemisen helpottamiseksi osana tilannetietoisuuden muodostumista. Tietopuutteiden tulkittiin estävän ongelmanratkaisun koordinoimista ja tuottamista käytännön tasolla. (Franssila, 2020)

Ympäristöstään havaintoja keräävän järjestelmän tiedot ovat osa järjestelmäkokonaisuuden ontologista tietämysrakennetta. Sovellusalueen käsitteiden ja niiden välisten suhteiden tietämysrakenteella mallinnetaan sovellusalueen tietoja eri kuvaustekniikoin (YSO, 2023). Ihmiset ja koneet tuottavat tilanteista malleja, jotka voidaan viestittää muille toimijoille jaetun ontologian eli jaetun ymmärryksen ja tietämyksen avulla, kuten seuraavassa kuviossa esitetään. Tavoitteet määrittävät käsiteltävien tilanteiden rajat. (Kokar & Endsley, 2012)



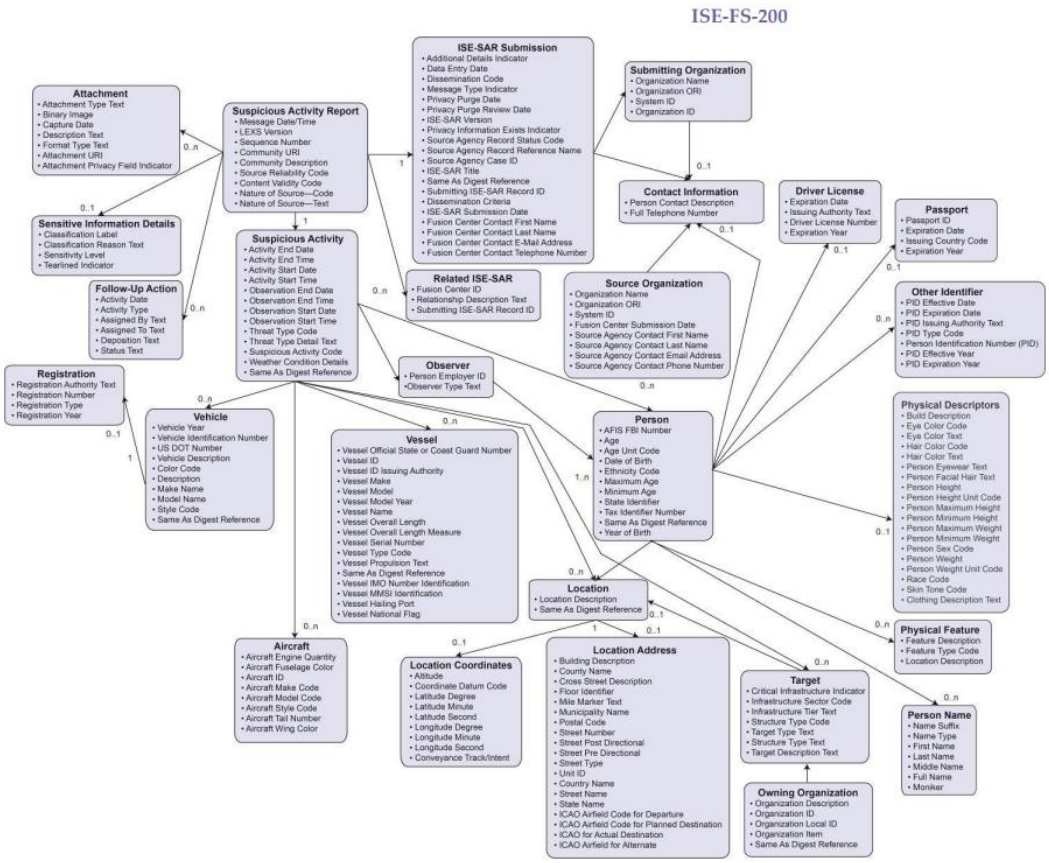
Kuvio 11 Tilanteen käsittely ihmisen ja koneen välillä (mukaillen Kokar & Endsley, 2012)

Uhkatiedon ja kriisitilanteiden hallinnassa käsitteiden merkityksen selventäminen, mallintaminen ja standardisointi on oleellista, jotta tietojärjestelmät saadaan toteuttamaan yhteisesti ymmärretyn tiedon jakelua ja vaihtoa. Tätä mallinnusta on tehty mm. W3C-työryhmässä "Emergency Information Interoperability Framework Incubator Group[6]" (Huovila ja muut, 2010). Automaattiseen ja rakenteelliseen tiedonjakoon kyberuhista voidaan hyödyntää esim. OASIS-yhteisön (2017–2024) kehittämää uhkatietokieltä (STIX) sekä tiedonvälitysmekanismia (TAXII).

Yhdysvaltain kotimaan turvallisuusvirasto (Homeland Security) on kehittänyt ISE-SAR -standardin (Information Sharing Environment - Suspicious Activity Report) tiedon tuottamiseen ja jakamiseen liittovaltiotasolla eri virastojen kesken rikollisesta ja mahdollisesti terrorismiin liittyvästä toiminnasta. Tapahtumatietoa, johtolankoja tai muuta vihje- ja liitetietoa raportoidaan yhteiselle tiedonkäsittelyalustalle lainvalvontaviranomaisen, analyytikon tai tutkijan toimesta jaettavaksi muiden

[6] https://www.w3.org/2005/Incubator/eiif/XGR-Framework-20090806/

sidosryhmien tietoon. Raportti sisältää useisiin uhkatoimijaan liittyvien tietokenttien lisäksi tietoa myös tehdyistä ja tarvittavista jatkotoimista, sijaintitietoja, havainnoitsijatietoa (mm. tunniste, organisaatio) sekä tiedon tuottamiseen, jakeluun ja hallintaan liittyviä perustietoja. Standardissa huomioidaan myös kriittistä infrastruktuuria ja energiatoimialaa määrittäviä tietoja, joihin liittyvää tapahtumaraportointia voidaan tarkentaa vapailla tekstikentillä. Seuraavassa kuviossa on esitetty standardin tietomalli.

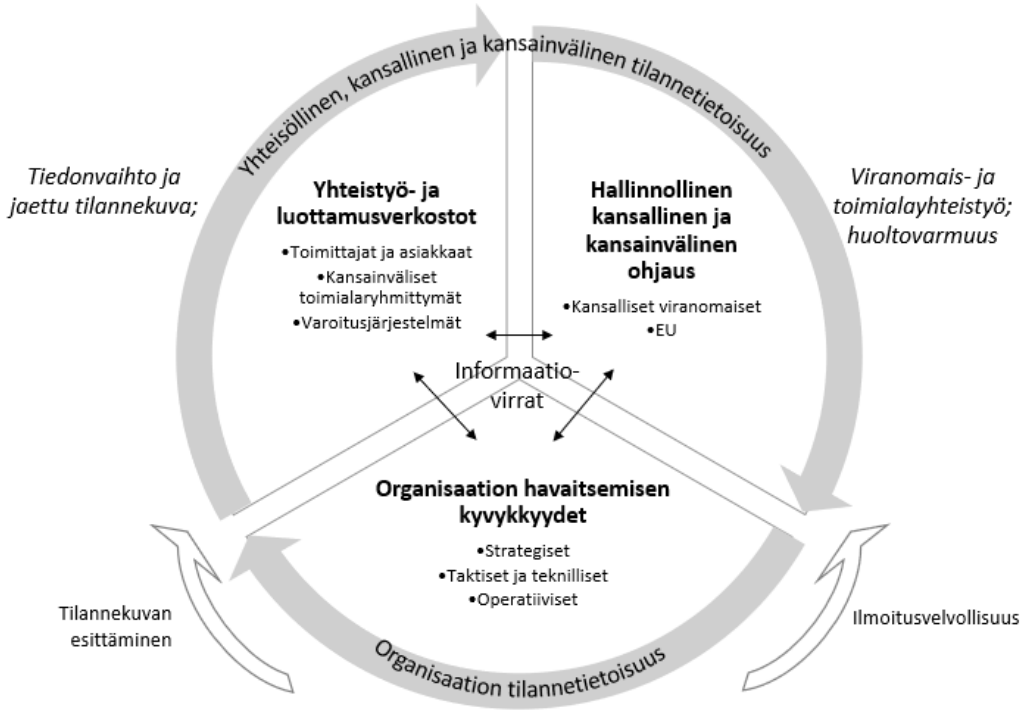


Kuvio 12 ISE-FS-200 tietomalli (ISE-SAR Functional Standard, 2015)

Tietomalli sisältää uhkakuvauksen tarkennettuna uhan muodolla (esim. asiakaspalautteen kautta saatu uhkaus, jauhekirje tmv) tarkkoine tietoineen, epätavallisen toiminnan (esim. poikkeuksillinen kiinnostus kohteeseen) kuvauksen sekä havainnoinnin kuvauksen (esim. yksittäisen kansalaisen uhkatapahtuman havaitsemistilanne). (Homeland Security, 2022)

Uhkien ja kriisien hallinnassa riittävien ja tarkoituksenmukaisten toimenpiteiden valinta tapahtuu seurauksena tilannekuvaymmärryksestä ja tilannekohtaisesta analysointikyvystä, ollen osa organisaation päätöksentekoprosessia riski- ja vakavuusluokitteluineen. Eri sidosryhmien (esim. analysointikeskukset ja keskitetyt asiantuntijaverkostot) kautta tapahtuva havainto-, ennakkovaroitus- ja arkaluonteisten tietojen vaihtaminen, parhaiden käytäntöjen jakaminen ja muu luottamusverkostoyhteistyö kehittää tilannekuvaymmärrystä ja tilannekohtaista analysointikyvykkyyttä. Tämän tietoyhteistyön rakennetta kuvataan seuraavassa kuviossa, jossa organisaatio muodostaa vuorovaikutukseen perustuvaa tilannekuvaa. Tietoyhteistyöverkostoja[7] hyödynnetään tilannekuvapalveluina sekä proaktiiviseen, ennakoivaan ja varautuvaan analyysi- ja turvallisuustoimintaan. (Pöyhönen, 2020)

[7] Esimerkiksi Energy Expert Cyber Security Platform EECSP https://energy.ec.europa.eu/publications/energy-expert-cyber-security-platform-eecsp-expert-group_en ja KRIVAT https://www.erillisverkot.fi/palvelut/krivat/ sekä European network of Cybersecurity centres and competence Hub for innovation and Operations ECHO https://echonetwork.eu/welcome-to-echo/ ja Pan-European Network to Counter Hybrid Threats https://euhybnet.eu/



Kuvio 13 Tietoyhteistyön kehikko (mukaillen Pöyhönen, 2020)

Sosiaaliset tietoyhteistyöverkostot mahdollistavat osaltaan informaatioresilienssiä vuorovaikuttamalla yhteiskunnassa ja sen yhteisöissä tiedon rakentamisen, sen merkityksellistämisen ja jakamisen kautta. Näin muodostetuissa fyysisissä, sosiaalisissa ja virtuaalisissa tietoympäristöissä toimijat voivat etsiä, tuottaa, käyttää, tulkita ja välittää informaatiota sekä muodollisten ennalta sovittujen käytäntöjen että vapaan vuorovaikutuksen prosessien mukaisesti. Tietoympäristöissä tuotetaan näin monitahoisesti uutta tietoa ja ymmärrystä sekä vahvistetaan samalla päätöksenteon tietopohjaa. (Rantamäki & Jalonen, 2022, viittaa Lloyd, 2015 ja 2014; Vårheim 2017; Shankar ym., 2016; Scholl & Patin, 2014; Savolainen, 2020; Andersson, 2015; Lloyd & Wilkinson, 2019; Tabasso, 2019; Brassett & Vaughan-Williams, 2015; Athayde ym., 2017; Hopp & Ferrucci, 2020; Torfing, 2019; Raisio, 2018)

EU:n tasolla pyritään vahvasti yhteisiin tiedonkäsittelypalveluihin. EU:n datastrategian tavoitteena on varmistaa Euroopan maailmanlaajuinen kilpailukyky ja datasuvereniteetti.

Yhteisillä eurooppalaisilla data-avaruuksilla varmistetaan, että saataville tulee enemmän dataa käytettäväksi taloudessa, yhteiskunnassa ja tutkimuksessa, samalla kun dataa tuottavat yritykset ja yksityishenkilöt pysyvät hallinnassa. Komissio tukee yhteisten eurooppalaisten data-avaruuksien kehittämistä strategisilla ja yleistä etua koskevilla aloilla, millä taataan datan saatavuus ja yhteiskunnallinen hyödynnettävyys. Jaetun tilanneymmärryksen periaatetta noudattavat keskitetyt tiedonjako- ja analyysikeskukset sekä luottamusverkostot, kuten esimerkiksi European Energy Information Sharing & Analysis Centre EE-ISAC[8] ja Pan-European Network to Counter Hybrid Threats[9] edistävät useilla tasoilla energia- ja kriittisen infrastruktuurin turvallisuutta ja resilienssiä. (Euroopan komissio, 2020)

Euroopan komissio on esim. tiedonannossaan 1.2.2008 määritellyt yhteisen ympäristötietojärjestelmän (Shared Environmental Information System SEIS) periaatteet, joilla pyritään tietojen integroitavuuteen sekä tietojen keruun, vaihdon ja käytön tehokkuuteen ympäristöpoliittisten toimien suunnittelussa ja toteuttamisessa. Periaatteen mukaisesti järjestelmän tietoja hallinnoidaan hajautetusti, mutta ne kerätään vain kerran ja annetaan kaikkien osapuolien käyttöön. Tietojen käsittelyn tulee perustua yleisiin ja vapaisin avoimen lähdekoodin välineisiin. Eduiksi on kuvailtu tietovirtoihin ja tiedottamiseen liittyvien menettelyjen yksinkertaistumista, tietojen saatavuuden ja tehokkaan hyödyntämisen tehostumista sekä myös kansalaisten vaikutusmahdollisuuksien sekä kyvykkyyden parantumista nopeaan toimintaan erityisesti kriisitilanteissa. (EU EUR-Lex, 2011)

Suomessa suomalaisiin huoltovarmuuskriittisiin yrityksiin ja organisaatioihin kohdistuvien uhkien havainnointiin ja niistä varoittamiseen on luotu Liikenne- ja viestintävirasto Traficomin hallinnoima HAVARO-palvelu. Havaitseminen toteutetaan teknisesti tarkkailemalla sensoreiden avulla palvelun hankkineiden yritysten tietoliikennettä. Tietoliikennepoikkeamat analysoidaan palvelun toimesta ja yritystä varoitetaan uhasta. Palvelulla

[8] https://ee-isac.eu

[9] https://euhybnet.eu/about/

tuetaan kansallista kyberturvallisuustilannekuvaa samalla huoltovarmuutta varmistaen. (Kyberturvallisuuskeskus, 2024b).

Tiedonvälitysverkostojen mahdollistamalla sidosryhmäyhteistyöllä, kuten esim. toimialan sisäisillä liittoumilla sekä yhteyksillä lainsäädännön ja sääntelyn kehittäjiin ja strategisiin kumppaneihin tehostetaan varautumista. Yhteistyön kautta vakiinnutetuilla viestintäkanavilla pidetään yllä tilannetietoisuutta ja mahdollistetaan nopea uhkavaste, mikä rakentaa dynaamista resilienssiä. Dynaaminen resilienssi muodostuu kyvykkyydestä jatkuvaan tilannetietoisuuteen, ketteryyteen ja nopeuteen vasteen muodostamisessa, kyvystä ennakointiin sekä sopeutumis-, uusiutumis- ja joustamiskyvyistä suunnitella ja reagoida päivittyvien tietojen mukaisesti. USA:ssa on mm. muodostettu energiatoimialan kyberosaajien verkosto (the Cyber Mutual Assistance Program) tarjoamaan yrityksille ja organisaatioille asiantuntijatukea uhka- ja häiriötilanteissa. (World Energy Council, 2019)

Yhdysvalloissa toimii lisäksi Energiaviraston alaisuudessa kyber- ja energiaturvallisuutta sekä kriisivastetta koordinoiva virasto (Office of Cybersecurity, Energy Security, and Emergency Response in U.S. Department of Energy CESER), jonka toimialalla energiasektorin kyberturvallisuus on yksi kolmesta päätoimialueesta. Tilannetietoisuuden ylläpito, tiedonjako ja riskianalyysi ovat viraston varautumis- ja valmiussuunnitteluun kuuluvia tehtäviä. CESER tekee kiinteää yhteistyötä energiasektorin toimijoiden kanssa uhkien ja riskien havaitsemiseksi ja niiden torjumiseksi. Se auttaa toimijoita luomaan uhkien hallintaan ja arviointiin liittyvää kyvykkyyttä tarjoamalla asiantuntemustaan operatiivisten uhkatyökalujen kehittämisessä ja käytössä. CESER tekee yhteistyötä myös tiedusteluyhteisön kanssa erityisesti uhka- ja tiedustelutiedon jakamisessa. Se tuo myös esille valtion (hallituksen) ja yksityissektorin yhteistyön merkitystä uhkien hallinnassa nykyisessä dynaamisessa teknologia- ja uhkaympäristössä, jota uhkien vakavuus, kohde ja luonne voidaan nopeasti määritellä sekä toteuttaa tarvittavat torjuntatoimet. (U.S. Department of Energy, 2024)

Yhdysvaltain energiavirasto koordinoi myös sähköalaan liittyvän tiedon jakamista Electricity Information Sharing and Analysis Center (E-ISAC) -keskuksen avulla. E-ISAC toteuttaa kyberturvallisuusriskien tiedonjaon ohjelmaa (The Cybersecurity Risk Information Sharing Program CRISP), jonka tarkoituksena on saattaa ajankohtainen uhkatieto energiasektorin toimijoiden saataville sekä kehittää tilannekuvatyökaluja ja edistyksellisiä sensori- ja uhka-analyysitekniikoita. Myös tässä ohjelmassa tehdään yhteistyötä kansallisen tiedusteluyhteisön kanssa. CRISP-ohjelmaan osallistuu noin 75 % kaikista Yhdysvaltojen mannermaisista energia-alan toimijoista. (U.S. Departmen of Energy, 2024)

Lisäksi Yhdysvaltain energiaviraston alaisuudessa on kehitetty CyOTE- ja CCE-metodologiat yhteistyössä Idahon kansallisen laboratorion (Idaho National Laboratory INL) kanssa. CyOTE:n eli Cybersecurity for the Operational Technology Environment -metodologian keskeisenä tavoitteena on mahdollistaa energia-alan toimijan uhkien havaitseminen ja lieventämistoimenpiteiden käynnistäminen. CCE:n eli Consequence-driven Cyber-informed Engineering -metodologialla tavoitellaan strategisten suojaavien ja uhkia lieventävien keinojen toteuttaminen. CyOTE:n metodologiassa ensimmäisessä havaitsemiseen liittyvissä vaiheessa lähdetään siitä, että inhimillinen toimija tunnistaa tietoisesti käynnistävän alkutapahtuman, joka voi olla automaattinen hälytys tai varoitus, ihmisen käyttäytymismalli tai poikkeama liiketoimintaprosessissa. CyOTE:ssa on luotu useita erityyppisiä työkaluja mm. tapahtumienhallintaan ja hyökkäysten mallintamiseen (CyOTE, 2024). (U.S. Department of Energy & Idaho National Laboratory, 2022)

Yhdysvaltojen energiaviraston alaisuudessa toimivan yhteisen energia-alan sääntelyn komission 3.5.2023 julkaisemassa aloitteessa kehotetaan toimijoita investoimaan yhteisiin kyberturvallisuusteknologiahankkeisiin sekä osallistumaan uhkatiedon jakamiseen liittyviin ohjelmiin. Tällä tavoitellaan mm. yksittäisille toimijoille aiheutuvien seuranta- ja sensoriteknologioiden kehittämiseen ja ylläpitoon liittyvien kustannuksellisten esteiden poistamista. (Federal Energy Regulatory Commission, 2023)

Yhteistyöverkostojen toiminnan seuraamiseen ja yhteistyön hyötyjen arviointiin voidaan hyödyntää erilaisia työkaluja. Myös kyberturvallisuuden kyvykkyyden mittareihin sisällytetään enenevässä määrin myös ympäristön tilannekuvan seurantaa, kuten mm. NCSI-mittarin (National Cyber Security Index[10]) tapahtumien ja kriisinhallinnan osa-alueita toimintaympäristön analysointikyky-indikaattoreineen (Pöyhönen, 2020). Mittaamisessa tarkastellaan myös tietojenvaihtoon, havaitsemiseen ja ennakkovaroittamiseen liittyvien yhteistyöjärjestelyiden ja toimintaverkostoyhteistyön prosesseja (Pöyhönen, 2020).

5.8 Yhteistyöhön perustuva harjoittelu

Keskeisenä kysymyksenä on se, miten tilannetietoisuutta voidaan harjoitella silloin, kun kyse on laajemmasta kontekstista kuin esim. tunkeutumisen havaitsemisesta tietojärjestelmään. Periaatteena tulisi olla, että harjoittelu kattaa myös teknisten riskitilanteiden lisäksi myös mm. markkinoihin, politiikkaan ja ympäristöön liittyviä uhka- ja riskitilanteita, jolloin varaudutaan esim. tuotannon ja kysynnän välisiin häiriötilanteisiin, terrorismin vaaratilanteisiin tai luonnonilmiöiden aiheuttamiin vahinkoihin. Harjoittelusuunnittelua ohjaa myös lainsäädäntö (esim. poikkeusoloihin ja hätä- tai valmiustilaan liittyvät lait) ja muu unioni- ja kansallisen tason sääntely organisaatio-, toimiala-, kokonais- tai kansallisen turvallisuuden alakohtaisine riskimäärittelyineen, -kehikkoineen ja -skenaarioineen. Harjoitteluun tulisi valita sellainen skenaario, mikä muodostaa laajuudeltaan riittävän kattavan otoksen organisaation strategisella, taktisella ja operatiivisella tasolla huomioiden monipuolisesti toimintaympäristön uhkaulottuvuudet.

Tilannekuva- ja valvontajärjestelmien teknisen suorituskyky- ja kuormitustestauksen ohella harjoittelun tulisi sisältää myös inhimillisen havainnointikyvyn testausta kuormitustilanteissa, jotta saadaan kattava käsitys sosioteknisen järjestelmän yhteentoimivuudesta. Tämän lähtökohdan perustelut on esitetty edeltävässä uhkien havaitsemista ja

[10] https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter ja https://ncsi.ega.ee/indicators/

torjuntaa tukevan tietotuotteen ja järjestelmäratkaisun kehittämisessä huomioitavia seikkoja käsittelevässä alaluvussa.

Valitun harjoitteluskenaarion taustatapahtuma voi olla esimerkiksi energiavarantojen käytön, tuotannon tai jakelun estävä luonnonkatastrofi, radioaktiivisten tai kemiallisten aineiden hallitsematon päästö, kyberhaittaohjelma, sabotaasi, vandalismi, terrorismi tai sota, tai mikä tahansa muu reagointi- ja vastatoimia edellyttävä inhimillinen tai luonnon toiminta. Tapahtumia voidaan luokitella niiden vaikutusalaltaan paikallisiksi, kunta- tai aluetasolla ilmeneviksi tai kansallisiksi. Erilaisten säännösten kuvatessa näinkin laajasti toiminnalle aiheutuvia uhkia ja riskejä on luontevaa pyrkiä myös harjoittelussa huomioimaan näihin johtavat tapahtumakulut varautumiskyvykkyyden parantamiseksi.

Energiatoimialalla kyberharjoitusympäristön luominen on haastavaa erityisesti vanhentuneiden laite-, ICT- ja operaatiojärjestelmien vuoksi. Teknisessä kyberturvallisuustestauksessa yksittäisten testattavien komponenttien vastaavuus tuotannossa käytettäviin tulee olla aukotonta, jolloin käytännössä turvallisuusharjoittelussa käytettävä ympäristö on siten kahdennettava reaalimaailmaa vastaavaksi (Baylon, Brunt & Livingstone, 2015)

Organisaation kyvykkyys havainnoida poikkeavaa toimintaa on oleellinen lähtökohta harjoittelulle (Pöyhönen, 2020). Harjoituksilla mallinnetaan ja simuloidaan riskien laukeamista ja sen vaikutuksia sekä niistä toipumista. Harjoitusten avulla voidaan todentaa riskeihin varautumisen kyvykkyyttä. Harjoitus toimii organisaation kohtaamana kriisitilanteena, jonka vaikutuksia ja tapahtuma-ajankohtaa voidaan suunnittelulla hallita. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus yhdessä Huoltovarmuuskeskuksen kanssa (2019) on kuvannut, että harjoittelulla etsitään prosessien ja toimintatapojen heikkouksia, eikä ihmisten heikkouksia. Harjoitusohjeessa todetaan lisäksi, että laaja-alaisesti verkottuneen toimintaympäristön häiriö- ym. tilanteiden vaikutuksia on arvioitava pelkkää teknistä tietojärjestelmätasoa pidemmälle. Harjoittelun päätavoite asetetaan ydintoiminnan turvallisuudelle tärkeästä strategisesta tavoitteesta, josta johdetaan

harjoituksen yksittäiset harjoitustavoitteet. Harjoitustavoitteena voi olla esimerkiksi uhkien havaitseminen tai muu vastaava reagointivalmiuteen liittyvä teema. Kokonaisvaltaisen harjoittelun suunnittelussa sovelletaan moninaisten teemojen lisäksi myös erilaisia harjoitustyyppejä, kuten esimerkiksi yhteis- ja juurisyyharjoituksia. Toimintaympäristön verkostojen toimivuutta ja uhkatilannekuvaa voidaan testata yhteisharjoituksilla, mikä kehittää myös jaetun käsityksen ja yhteisymmärryksen kehittämiseen vahinkoa tuottavan toimijan (hyökkääjä) tarkoitusperistä, toimintatavoista ja tavoitteista. Juurisyyharjoitus soveltuu puolestaan kokonaisvaltaiseen tarkasteluun lauenneiden riskien alkuperäisistä aiheuttajista. Kokonaisvaltaisuus ilmenee myös harjoitusten taustakuvauksina, joilla valotetaan riskien laukeamiseen johtaneita poliittisia, taloudellisia, sosiaalisia ja ympäristöön liittyviä tapahtumia. (Traficom, 2019)

Huoltovarmuuskeskuksen energia-alan toimijoille laatiman harjoitusohjeen (2024) harjoittelun tavoitteina on parantaa valmiutta kohdata häiriöitä, vahvistaa yhteistyötä ja viestintää, tarkastaa materiaalisen varautumisen tila ja kohottaa henkilöstön valmiuksia. Ohjeessa kehotetaan hyödyntämään alueellisten uhkien tunnistamiseen Tuovi-portaalia. Ohjeessa kuvataan organisaatiokohtaisten harjoitusten lisäksi myös paikallisten, alueellisten, alakohtaisten ja kansallisten harjoitusten toteuttamista eri harjoitustyyppeineen sekä harjoituspalautteen keräämisen merkitystä oppina tulevaan. (Huoltovarmuuskeskus, 2024)

Organisaation toimintaympäristön ulottuvuudet kattavalla harjoitustoiminnalla tavoitellaan parempaa turvallisuuskulttuuria, kriisinsietokykyä sekä ymmärrystä vahinko- ja haittatapahtumien laajoista asiayhteyksistä, riippuvuuksista ja vaikutuksista. Suomen kansallisista yhteisharjoituksista saaduissa palautteissa on käynyt ilmi toiveet uudenlaisista harjoitusmalleista ja realistisimmista skenaarioista sekä harjoittelun monimuotoisuudesta ja toiminnan kattavuudesta. Tätä kuvattiin esimerkiksi organisaation toiminnan kannalta kriittisen materiaalin tilaus- ja toimintaketjun häiriöinä, toimitiloihin liittyvinä asioina sekä syvempänä toimialakohtaisuutena (Rousku, 2019)

6 Tulokset

Johdannossa esitetyn mukaisesti tutkielman tavoitteena on vastata siihen, mitä energiaturvallisuus on, millaisista tekijöistä toimintaympäristön uhat voivat muodostua, millaisia tietoja energia-alan toimijan kannattaa kerätä toimintaympäristöstään uhkiin varautumiseksi sekä miten inhimillisen havainnoinnin osuutta esitellään tietojärjestelmäratkaisuissa. Tutkimuksen neljännessä pääluvussa vastataan kysymyksiin energiaturvallisuudesta ja toimintaympäristön uhkatekijöistä. Viidennessä pääluvussa kuvataan uhkiin liittyvien tietojen hankintaa ja käsittelyä vastaamalla kysymykseen tietojen keräämisestä. Toisessa pääluvussa kuvataan läpikäydyn tutkimusaineiston avulla inhimillisen havainnoinnin esille tuontia järjestelmäratkaisuissa.

Energiaturvallisuus on turvallisuuden sektorirajat ylittävää energian saatavuutta, energiantoimituksen ja -jakelun keskeytymättömyyttä, energian tuotannon ja kulutuksen tasapainoa sekä markkinahintojen kohtuullisuutta ja kilpailukykyä. Energiaturvallisuutta on tarkasteltava moniulotteisena ja monitieteellisesti. Huolimatta teknologiakeskeisyyden painoarvon kasvamisesta on varottava yksiulotteista kokonaisuuden sekä syy-seuraustapahtumaketjut huomiotta jättävää tarkastelutapaa. Energiaturvallisuutta varmistetaan useilla kansallisilla sekä yhteisöjen välisillä sopimuksilla, ohjeistuksilla ja säätelyillä, jotta päivittäin tapahtuvien kansallisesti ja alueellisesti ilmenevien uhkatilanteiden hallinnassa onnistuttaisiin hyökkäysalan ollessa suuri. Uhat ovat monitahoisia aina yksittäisistä toimijoista valtiollisiin ja muodostuvat myös itsestään esim. poliittisten tai yhteiskunnallisten linjauksen aikaansaamina. Uhkien havainnoinnin tulee tällöin olla kattavaa käyttäen erilaisia menetelmiä ja välineitä monien uhkaulottuvuuksien seurantaan. Soveltuvien tietojärjestelmäratkaisujen, kuten monilähdetietoja yhdistävien fuusiojärjestelmien, hyödyntäminen sekä verkostoyhteistyö tiedon jakamisessa ja harjoittelussa muodostavat resilienssiä myös informaation osalta.

Yleistävänä kirjallisuuskatsauksesta muodostettuna johtopäätöksenä on, että inhimillisen havainnoinnin asema, merkitys ja yhteensovittaminen teknologioihin toimintaympä-

ristöstään monilähdetietoa keräävissä sosioteknisissä järjestelmissä ansaitsee lisää tarkentavaa ja määrittävää tutkimusta eri tieteenalojen näkökulmista. Erityisesti kyberturvallisuuden tutkimus on vahvasti teknologiapainotteista ja uhkateema näkyy valtaosin siinä.

Aiemmista tutkimuksista koostettu analyysi vastaa tavoitettaan asetetun hakuehdon ja -tulosten mukaisesti. Samalla tämän kuitenkin voidaan havaita heikentävän tutkimustuloksen arvoa, sillä kohdentamalla hakua toisin esim. liiketoimintatiedusteluun tai tiedonhallintaan liittyvään aineistoon olisi tuloksella voinut olla vahvempi asiayhteys havaitsemiseen. Tutkielmassa kuitenkin pyrittiin tarkastelemaan havaitsemisen osuutta osana monilähdetietoa keräävästä sosioteknisestä järjestelmästä tilannetietoisuuden viitekehyksen ja uhkateeman kautta, millä avarrettiin kohdealuetta tavanomaisen liiketoimintatiedonhallinnan, BI:n ja data-analytiikan käsitteiden ulkopuolelle.

Inhimillisen toimijan osuus tiedonhallinnan toteutuksessa on edelleen merkittävä. Tiedon arvoketjun datan havainto- tai hankintavaiheesta kuvataan muodostuvan valitun datan määrältään riittävän tehokkaasta keräämisestä ja teknisestä prosessoinnista, jossa inhimillistä havainto-, tulkinta- ja päättelykykyä (engl. human grey perception ability; fuzzy evaluation) tarvitaan kuitenkin edelleen muodostamaan kokonaiskuvaa tilanteesta ja myös osallistumaan itse analysointiin esim. opetettaessa koneoppimisen malleja (Li ja muut, 2019).

Inhimillisellä tulkinnalla ja päätöksenteolla on merkittävä rooli uuden datan luomisessa eri teknologioiden avulla sekä datan yhdistämisessä, muuntamisessa ja kääntämisessä (engl. datafication) digitaalisista sekä analogisista aineistoista, ja dataksi tuottamisen prosessia tulisikin tutkia myös tästä näkökulmasta (Lercari ja muut, 2021).

Becerran (2021) julkaisussa on huomattavaa, että nimenomaisesti inhimilliseen havainnointiin liittyviä laatukriteereitä, -piirteitä tai -tekijöitä ei kuitenkaan ole erikseen ni-

metty tai ryhmitelty; lähin liittyvä käsite on saavutettavuus (engl. accessibility), jolla viitataan vain mitattavaan kykyyn käyttää saatavilla olevia tietoja nopeasti ja helposti. Tämä voi selittyä sillä, että kyse ei ole tiedon laadusta, vaan havainnoijan omasta piirteestä tai toiminnasta. Toisaalta tiedolla itsessään voi olla ominaisuuksia, jotka edesauttavat havainnointia ja havaintojen käsittelyä. Becerra (2021) esittääkin jatkotutkimusaiheina kognitiivisen taakan ja moniaistiärsykkeiden tutkimista osana tiedon esittämisen vaikutuksia käyttäjän havainnointiin ja päätöksenteon nopeuteen.

Etäaistintaa (engl. remote sensing) kuvataan datafuusiossa valtaosin sensoreiden tai antureiden sekä raakadatan (signaalit) näkökulmasta, eikä inhimillistä osuutta ole sensoreita painottavissa julkaisuissa juurikaan käsitelty. Inhimillistä osuutta tai ns. väliintuloa datafuusioprosessiin esitetään lähinnä tiedon visualisointiin liittyen, jolloin perusteena on inhimillisen havainto- ja käsityskyvyn ylittävä datan määrä. Lisäksi määritellään usein havainto- tai huomiokyvyn häiriöiden olevan syynä vaaratilanteisiin (Benyon, 2011). Inhimillisen käyttäjän jakaantunut huomiokyky useita samanaikaisia tehtäviä suorittaessa voi johtaa reagoinnin ja päätöksenteon vaikeuksiin. Useat yhtäaikaiset ja peräkkäiset hälytykset voivat kuormittaa havaitsemista ja siten aiheuttaa siinä puutteita. Toisaalta jatkuva kuormitus voi saada aikaan ajatusvääristymää, joka ilmenee mm. tapahtumakulkujen toiminnalle haitallisina ennakko-oletuksina tai havaintotietojen valikoimisena. Edellä kuvatulle sopivia tutkimuskohteita ovat moninaiset valvonta- ja tarkkailutehtävät erityistyötiloineen.

Datafuusiojärjestelmien lisääntyessä ja muuttuessa kompleksisimmiksi tarvitaan lisää tutkimusta monimuotoisen ja -lähteisen datan käsittelystä ihmisen ja järjestelmän vuorovaikutuksen sekä kontekstualisoinnin näkökulmista (Wang ja muut, 2023; Karagiannopoulou ja muut, 2022). Datafuusiojärjestelmien, erityisesti verkkoturvallisuuden järjestelmien, algoritmien ja mallien vertailulle ei vielä ole riittävän laadukasta tieteellistä pohjaa standardoitujen data-aineistojen puuttumisen ja sovellutusten tai sovellusalueiden erilaisuuden vuoksi (Li ja muut, 2019).

Aiemman tutkimuksen kirjallisuuskatsauksen aineistossa yllättää virtuaalisen, lisätyn ja immersiivisen todellisuuden vähäinen yhteys, vaikka julkaisut olivat teknologiapainotteisia. Myös tekoälyratkaisujen hyödyntäminen inhimillisten havaintojen tekijänä ja prosessoijana jäi tässä hakutuloksessa erittäin vähäiseksi. Voidaan todeta myös, että toimi- tai sovellusalakohtaista tutkimusta tarvitaan yleisesti ottaen enemmän.

Informaatioon liittyvän uhkien- ja riskienhallinnan kontekstissa uhkien ymmärtämisessä ja tunnistamisessa niiden kaikissa ulottuvuuksissaan on edelleen puutteita, eikä esim. hallintotieteellisessä resilienssitutkimuksessakaan ei ole vielä riittävästi huomioitu informaation merkityksellisyyttä riskien ja uhkien tunnistamisessa tai niihin vastaamisessa (Rantamäki & Jalonen, 2022, viittaa Imperiale & Vanclay, 2020). Kokonaisvaltaisen tilannekuvan saamiseksi tulisi kerätä tietoa uhkatoimijoiden identiteeteistä, motivaatioista ja tavoitteista, strategioista ja kyvykkyyksistä, kuten kyberturvallisuuden semanttisessa uhkaluokittelumallissa (Bromander, Jøsang, & Eian, 2016) esitetään.

Yhteenvetona voidaan todeta, että kirjallisuuskatsauksen tuloksessa korostuu päällimmäisenä tarve lisätutkimukselle. Tässä merkittävinä tekijöinä ovat havaitsemisen tutkimisen monitieteellisyys eri näkökulmien mukaan, uhkatiedonhallinnan sovellutusalueiden kirjavuus sekä yleisen maailmantilanteen aiheuttamat voimakkaat toimintaympäristön muutokset erityisesti energiatoimialalla.

7 Diskussio

Tämän tutkielman johdanto ja neljäs pääluku johdattelivat tutkimusaiheeseen esittelemällä aiheen ajankohtaisuutta ja tärkeyttä tosielämän esimerkein. Johdannossa esiteltiin myös tutkielman tavoite, aineisto, tutkimusmenetelmät ja rajaus. Tutkielman viitekehys muodostui useista asiakokonaisuuksien pääluvuista. Näistä ensimmäisissä (pääluvut 2 ja 3) luotiin katsaus aiempaan tutkimukseen ja teoriapohjaan. Energiatoimialaa ja -turvallisuutta, sen sääntelyä ja ohjausta, informaatio- ja kommunikaatiojärjestelmiä sekä alaan kohdistuvia uhkia käsiteltiin neljännessä pääluvussa. Tutkielman seuraava viides pääluku kuvaa uhkien havaitsemista, havainnoinnin edellytyksiä ja sen tukemista järjestelmäsovellusalueilla. Kirjallisuuskatsauksen tulokset esitellään yhteenvetona kuudennessa pääluvussa. Tutkielman päättää diskussio-pääluku johtopäätöksineen. Tässä diskussiossa tuotetaan myös yhteenveto tutkielman tavoitteiden toteutumisesta, arvioidaan sen luotettavuutta ja pätevyyttä sekä suositellaan lisätutkimuksia.

Tutkijalle on tutkielman tekoaikana muodostunut käsitys, että energiatoimialan murros uusine teknologioineen vahvistaa entisestään toimijoiden, sidosryhmien sekä myös energiapalveluiden ja –tuotteiden välisiä kilpailuasetelmia nykyisessä kauppa- ja tullisotien vallitsemassa maailmassa. Samalla turvallisuuden käsite laajenee perinteisen sodankäynnin ulkopuolelle. Varautumisen ja turvallisuuden ylläpitämisen näkökulmasta uhkien hallinnassa on varottava tyytymästä jo tietoon saatuihin asioihin, vaan toimijoiden pitää pystyä ennakoimaan tulevaa. Tässä tulevaisuuden ennakoinnissa on mahdollista hyödyntää tulevaisuudentutkimuksen keinoja ja menetelmiä. Lisäksi, kuten Euroopan komission suosituksissa tulee esiin, yhteistyötä on tiivistettävä toimijoiden kesken sekä kansallisella että yhteisön tasolla.

Tutkijan käsitys siitä, että energiatoimialalla saattaa edelleen olla puute kokonaisvaltaisen tilannekuvan ja tapahtumaketjujen hahmottamisessa, on edelleen vahvistunut. Tiedustelevia ja ennakoivia turvallisuuden menettelyjä tai käytäntöjä ei juurikaan tuoda esiin osana kokonaisketjua ja näkyvyys eri ulottuvuuksiin on rajoittunutta. Kyberturvalli-

suudessa painotus kohdentuu välittömiin operatiivisiin uhkiin varautumiseen, josta esimerkkinä ovat tunkeutumisen havaitsemisen ja estämisen tekniset järjestelmät. Vahti-, Katakri-, Pitukri[11]- yms. -ohjeistuksissa painotetaan operatiivista ja reaaliaikaista vastepohjaista kyberturvallisuutta. Kyberhyökkäysten torjuntaa harjoitellaan, mutta hallinnolliset rajat ja organisaation toimintayksiköiden siilot ylittävää laajaa uhka-analyysia ei välttämättä opetella tai harjoitella. Kykyä varautua ja valmistautua ennakkoon vahingollisten toimijoiden hyökkäyksiin ei käsitellä julkisuudessa, sillä toimet ovat keskittyneet itse hyökkäysten torjuntaan. Valtiollisten toimijoiden muodostamaan uhkaan on haasteellista varautua. Tiedusteluanalyysin keinojen hyödyntämistä on vaikea todentaa ulkopuolelta.

Järjestelmä- ja komponenttihaavoittuvuudet ovat jatkuvassa kasvussa, sillä uusien teknologioiden käyttöönottojen myötä syntyy samalla uusia haavoittuvuuksia ja uhka-altistumisia. Ei ole syytä olettaa, että tämä kehitys pysähtyisi esim. edistyksellisten torjuntatoimien vuoksi, sillä kyseessä on jatkuva turvallisuusaukkojen tilkinnän prosessi. Kyberhyökkäyksiä tapahtuu koko ajan suuria määriä, joten on aina vain ajan kysymys, milloin vakava häiriötilanne toteutuu tai päädytäänkö jopa energiakriisiin. Huolimatta energiantuotannon hajauttamisesta eri tuotantolaitoksiin, ja tätä kautta huoltovarmuuden toteuttamisesta, muodostaa energiariippuvuus nykyisissä rikkoutuneissa sähkömarkkinoissa suuren riskin.

Edellä kuvatun pohjalta on perusteltua, että tutkielman vaihtoehtoisena toteuttamistapana olisi voinut olla tapahtuma-analyysin tuottaminen ajankohtaisten energia-alaan kohdistuneiden häiriö- ym. tilanteiden kautta, jolloin tapahtumat olisi luokiteltu eri uhkateemojen (sosiaaliset, ympäristöön liittyvät, taloudelliset, kyberturvallisuuteen liittyvät jne.) alle ja analysoitu niitä. Tätä kuitenkin olisi vaikeuttanut se, että niiden pohjalta

[11] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri

muodostunut kokonaiskuva olisi jäänyt puutteelliseksi, sillä kaikista tapahtumista ei turvallisuuskäytäntöjen vuoksi tiedoteta julkisesti, eikä kaikki ulottuvuudet kattavaa tietokantaa ole saatavilla.

Tutkielman tuloksen arvoa heikentää se, ettei siinä ole kyetty kuvaamaan eritellen niitä tietoja, mitä tyypillisesti voidaan havainnoida inhimillisen toimijan toimesta verrattuna teknologiaperusteisesti (esim. kameravalvonta ja sensorijärjestelmät) toteutettavaan automatisoituun havainnointiin. Oletuksena kuitenkin on, että monimutkaisten ja laaja-alaisten toimintaympäristön uhkien havainnointi, analyysi ja tulkinta edellyttävät aina inhimillisen osuuden mukanaoloa. Tutkielman luotettavuutta puolestaan heikentää se, että tutkimusprosessin pitkittyessä osa lähdeaineistosta on nopean kehityksen vuoksi ehtinyt vanhentua. Esim. uutta sääntelyä on tehty ja niiden vaadittamalla tavalla on jo reagoitu. Haastetta tutkimusprosessiin on samalla aiheuttanut se, että uutta näkökulmaa on tarjolla ajankohtaisten tapahtumien, tilannekehitysten ja ilmiöiden myötä niin runsaasti, että tutkielmaraporttia on ollut vaikeuksia rajata kohdeaiheeseen pidättäytyväksi.

Tutkielman luotettavuutta pyrittiin varmistamaan valitsemalla aiemman tutkimuksen aineistoanalyysiin vain vertaisarvioidut tieteelliset artikkelit. Tutkielman pätevyyttä heikentää se, että aineisto on kerätty tutkijan oman teoreettisen päättelyn ja tulkinnan pohjalta ja se ei sellaisenaan ole toistettavissa täsmälleen samoin tuloksin.

Aineistoa ja hakutulokseen sisältyviä julkaisuja läpikäydessä tulee esiin muutamia mahdollisessa jatkotutkimuksessa tarkennettavia käsitteitä. Näitä ovat esim. jaettu tilannetietoisuus (engl. shared awareness) ja yhteistoiminnallinen tiedustelu (engl. collaborative intelligence), joilla on yhteys tämän tutkielman kohteena olevaan inhimilliseen havainnointiin. Jatkotutkimusta voi kohdentaa myös datan ominaisuuksien muutokseen havaintoverkossa (engl. perception network), jossa staattinen data on pysyvää koko analyysin ajan, dynaamisen datan muuntuessa havaintotuloksen syntymisen ja siitä aiheutuneiden toimenpiteiden myötä (Li ja muut, 2019).

Jatkotutkimukseksi ehdotetaan myös tarkastelua liiketoimintatiedustelun aihealueesta ja sen yhteyksistä strategiseen ja operatiiviseen tiedusteluun kaupallisten organisaatioiden tai kriittisen infrastruktuurin toimijoiden uhkahavainnoinnin kontekstissa sekä mahdollisuudesta ns. venyttää liiketoimintatiedustelun käsitettä liiketoiminnallisen tiedon (BI) yli. Tutkimisen arvoista voi olla myös se, miten pienet, keskisuuret tai suuret energia-alan organisaatiot toteuttavat uhkien analysointia, esim. ovatko ne missä määrin investoineet tämän kyvykkyyden kehittämiseen ja miten toteutusvastuut on jaettu sekä organisaation sisällä että ulkoisen tuen turvin. Jatkotutkimusten aineiston hankinnassa on huomioitava, että useimmat tutkimukset edustavat kyberturvallisuusnäkökulmaa, ja että niistäkin on saatavilla julkista tietoa vain rajatusti, kuten Kovanen, Nuojua & Lehto ovat jo aiemmin (2018) todenneet. Lisäksi kokonaan uusi tutkimuskohde voisi avautua ihmisen ja koneen yhdistymisestä havaintotietoja käsitteleväksi hybridiksi, joko transhumanismin hengessä tai esim. robotiikan, puolustus- tai sotilasteknologian kyvykkyyksien tarkastelun kautta.

Lähdeluettelo

Ailisto, H. (2018), Tekoälyn käsitekartta. VTT Oy. Noudettu 19.9.2021 osoitteesta https://tietokayttoon.fi/documents/1927382/2158283/Teko%C3%A4lyn+k%C3%A4sitekartta/a5c4b469-d8ae-4ce1-a5fc-f12981bae796

Albert, C. D., Baez, A. A., Hunter, L. Heslen, J. & Rutland, J. (2023). Epidemiological intelligence fusion centers: health security and COVID-19 in the Dominican Repub-lic. Intelligence and National Security, 38:1, 90–110, Noudettu 10.8.2024 osoitteesta DOI: 10.1080/02684527.2022.2095601

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. *Management Decision* 35/6 [1997] 452–463. © MCB University Press. ISSN 0021-1747, 2014. Noudettu 13.5.2024 osoitteesta https://www.researchgate.net/publication/235266179

Assante, M. J. & Lee, R. M. (2015, lokakuu). The Industrial Control System Cyber Kill Chain. SANS Institute. Noudettu 10.2.2021 osoitteesta https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf

Baylon, C., Brunt, R. & Livingstone, D. (2015). Cyber Security at Civil Nuclear Facilities - Understanding the Risks, Chatham House Report. ISBN 978 1 78413 079 4. Chatham House, the Royal Institute of International Affairs. Noudettu 14.9.2020 osoitteesta https://www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneExecSumUpdate.pdf

Becerra, M. A., Tobón, C., Castro-Ospina, A. E. & Peluffo-Ordóñez, D. H. (2021, 8. kesäkuuta) Information Quality Assessment for Data Fusion Systems. *Data 2021*, 6, 60. Noudettu 10.8.2024 osoitteesta https://doi.org/10.3390/data6060060

Belinskij, A. J. (2019). Selvitys vesihuollon häiriötilanteista: Lainsäädännön mukaisten vaatimusten täyttäminen ja toimenpidesuositukset. Maa- ja metsätalousministeriö. Noudettu 19.9.2020 osoitteesta https://stm.fi/documents/1271139/1371655/Selvitys vesihuollon h%C3%A4iri%C3%B6tilanteista raportti 8_2019.pdf/c4dac2da-8f90-ff72-a396-b327ca8d02c9

Benyon, D. 2011. Designing Interactive Systems: A comprehensive guide to HCI and interaction design. Pearson Education Limited 2nd edition 2011.

Blasch, E., Kadar, I., Salerno, J., Kokar, M. M., Das, S., Powell, G. M., Corkill, D. D. & Ruspini, E. H. 2006. Issues and Challenges in Situation Assessment (Level 2 Fusion). *Journal of Advances in Information Fusion*, Vol 1, 2 December 2006. Noudettu 14.10.2020 osoitteesta https://www.academia.edu/8939577/Issues_and_Challenges_in_Situation_Assessment_Level_2_Fusion_

Bolado-Lavin, R., Gracceva, F., Zeniewski, P., Zastera, P., Vanhoorn, L. & Menqolini, A. (2012). European Commission, Joint Research Centre, Institute for Energy and Transport. JRC 68735, EUR 25227 EN, ISBN 978-92-79-23118-6 (pdf), ISSN 1831-9424 (online). doi: 10.2790/44771. Luxembourg: Publications Office of the European Union, 2012.Noudettu 10.2.2022 osoitteesta https://ec.europa.eu/energy/sites/ener/files/documents/jrc68735_best_practices_and_methodological_guidelines_for_conducting_gas_risk_assessments.pdf

Borg, O. (2013). Tulevaisuuksista tietämisen lähtökohdat. Tulevaisuudentutkimuksen tiedeidentiteetti ja suhde muihin tieteisiin. Teoksessa Kuusi, O., Bergman, T. & Salminen, H. *Miten tutkimme tulevaisuuksia?* 3. uudistettu painos, kappale 5, s. 43–56. Helsinki. Tulevaisuuden tutkimuksen seura ry.

Bromander, S., Jøsang, A. ja Eian, M. (2016, marraskuu). Semantic Cyberthreat Modelling. 11th International Conference on Semantic Technologies in Intelligence, Defense, and Security (STIDS 2016), Fairfax VA, USA, November 2016.

Csernatori, R. & Martins, B. O. (2023, 19. kesäkuuta). Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination. *Geopolitics*. Noudettu 10.8.2024 osoitteesta DOI: 10.1080/14650045.2023.2224235

Daskalakis, E., Remoundiou, K., Peppes, N., Alexakis, T., Demestichas, K., Adamopoulou, E. & Sykas, E. (2022, 25. toukokuuta). Applications of Fusion Techniques in E-Commerce Environments: A Literature Review. *Sensors 2022*, 22, 3998. Noudettu 10.8.2024 osoitteesta https://doi.org/10.3390/s22113998

Desarnaud, G. (2018, tammikuu). Cyber Attacks and Energy Infrastructures - Anticipating Risks, Études de l´Ifri. ISBN: 987-2-36567-724-0. Ifri Center for Energy.

Noudettu 14.9.2020 osoitteesta https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf

Dorsser, C. von, & Taneja, P. (2019). An integrated three-layered foresight framework. *Foresight*, Vol 22 No 2 2020, pp. 250-272. Emerald Publishing Limited, ISSN 1463-6689. Noudettu 10.8.2024 osoitteesta http://dx.doi.org/10.1108/FS-05-2019-0039

Dufva, M. & Rowley, C. (2022, 2. tammikuuta). Heikot signaalit 2022. Noudettu 13.4.2024 osoitteesta https://www.sitra.fi/julkaisut/heikot-signaalit-2022/#esipuhe

Endsley, M. R., 2000. Theoretical underpinnings of Situation Awareness: A critical review. In Endsley, M. R. & Garland D., J. (Eds.): Situation Awareness Analysis and Measurement. PDF document. Noudettu 15.2.2020 osoitteesta https://www.researchgate.net/publication/230745477_Theoretical_underpinnings_of_situation_awareness_A_critical_review

Energiavirasto / Energy Authority. (2023, 16. tammikuuta 2023). Risk Preparedness Plan of Finland. In accordance with Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. 1393/443/2021. Noudettu 17.11.2024 osoitteesta https://energiavirasto.fi/documents/11120570/12722768/Risk+Preparedness+Plan+of+Finland+public.pdf/e4c9880b-e8cb-f5aa-dfb0-597b0ad2ea33/Risk+Preparedness+Plan+of+Finland+public.pdf?t=1675325213136

Energiavirasto. (n.d.). Toimitusvarmuus. Riskeihin varautuminen sähköalalla. Noudettu 17.11.2024 osoitteesta https://energiavirasto.fi/toimitusvarmuus

Euroopan komissio. (2019, 14. kesäkuuta). Euroopan parlamentin ja neuvoston asetus (EU) 2019/941, annettu 5 päivänä kesäkuuta 2019, riskeihin varautumisesta sähköalalla ja direktiivinen 2005/89/EY kumoamisesta. Noudettu 17.11.2024 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32019R0941

Euroopan komissio. (2022, 14. kesäkuuta). Komission lausunto, annettu 14.6.2022, riskeihin varautumisesta sähköalalla ja direktiivin 2005/89/EY kumoamisesta an-netun asetuksen (EU) 2019/941 mukaisesti Suomen toimivaltaisen viranomaisen Euroopan komissiolle toimittamasta riskeihinvarautumissuunnitelmasta. Noudettu 17.11.2024 osoitteesta https://energy.ec.europa.eu/document/download/96384e58-72d0-49bb-8b83-142610bf114f_fi?filename=C_2022_3863_1_FI_ACT_part1_v2 Finland.pdf

European Comission. (2014, 28. toukokuuta). Communication from the Comission to the European Parliament and the Council - European Energy Security Strategy, SWD(2014) 330 final(COM(2014) 330 final). Brussels. Noudettu 13.9.2020 osoitteesta https://www.eesc.europa.eu/resources/docs/european-energy-security-strategy.pdf

European Comission. (2019, 3. huhtikuuta). Commission recommendations of 3.4.2019 on cybersecurity in the energy sector, C(2019) 2400 final(SWD(2019) 1240 final). Brussels. Noudettu 12.9.2020 osoitteesta https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

European Comission. (2020, 14. syyskuuta). Long-term strategies. Noudettu 14.9.2020 osoitteesta https://ec.europa.eu/info/energy-climate-change-environment/overall-targets/long-term-strategies_en

European Comission. (2020). Regulation on risk-preparedness in the electricity sector. Noudettu 26.9.2020 osoitteesta https://ec.europa.eu/energy/topics/energy-security/security-electricity-supply_en?redir=1

European Union Agency for Cybersecurity. (2020). Threat Landscape through the years, 2020. Noudettu 2.12.2022 osoitteesta https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

FATF. (2013-2017). Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion - With a supplement on customer due diligence. FATF Guidance,

November 2017, Paris. Noudettu 19.4.2024 osoitteesta www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

FCA. (2024). Overview of KYC Screening Types. Noudettu 19.4.2024 osoitteesta https://financialcrimeacademy.org/overview-of-kyc-screening-types/

Fernandez, F., Sanchez, A., Velez, J. & Moreno, B. (2017). A Cognitive Architecture Framework for Critical Situation Awareness Systems. IWINAC 2017. Part I, LNCS 10337, pp. 53–62, 2017. Springer International Publishing AG 2017. DOI: 10.1007/978-3-319-59740-9 6. Noudettu 18.11.2020 osoitteesta https://publik.tuwien.ac.at/files/publik_266621.pdf

Finlex.(2017). Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444. Noudettu 19.4.2024 osoitteesta https://finlex.fi/fi/laki/ajantasa/2017/20170444#L3

Fjäder, C. (2019). Security of supply in Finland and the role of the National Emergency Supply Agency. October 2019. Noudettu 10.10.2020 osoitteesta https://puolustusvoimat.fi/documents/2182132/16308001/20191031+NESA.pdf/37fc0c01-17e7-f5ae-2194-7719466febb0/20191031+NESA.pdf

Franssila, H. (2020, maaliskuu). Jaetun tilannetietoisuuden ylläpidon käytännöt hajautuneen työn yhteisöissä. Tampereen yliopisto, yhteiskuntatieteiden tiedekunta. Pro gradu. Maaliskuu 2020. Noudettu 10.3.2022 osoitteesta https://trepo.tuni.fi

Freedman, L. (2013). Strategy : a history. Oxford University Press, USA. EBSCOhost, e-kirja.

Gaba, D. M., Lau, N. & Desaulniers, D. (2013). Human Factors and Human Reliability in Healthcare and Nuclear Power. Risk and Reliability in Healthcare and Nuclear Power, AAMI. Noudettu 3.9.2020 osoitteesta https://www.nrc.gov/docs/ML1301/ML13017A267.pdf

Gruszczack, A. (2022). Intelligence Fusion for the European Union's Common Security and Defence Policy. *Politeja*, No. 4(79), 2022, pp. 131–150. Noudettu 10.8.2024 osoitteesta https://doi.org/10.12797/Politeja.19.2022.79.08

Hakala, J. (2021, huhtikuu). Tilannetietoisuuden muodostuminen ja merkitys johtamisessa ja päätöksenteossa. Johtamisen ja talouden tiedekunta, turvallisuushallin-

non maisteriohjelma. Pro gradu. Huhtikuu 2021. Noudettu 10.3.2022 osoitteesta https://trepo.tuni.fi

Halonen, H. (2015). Tiedolla johtamisen näyttämö ja kulissit. teoksessa: Tiedolla johtaminen hallinnossa: teoriaa ja käytäntöjä, s. 40–68. Tampereen yliopistopaino. Noudettu 30.10.2023 osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/ongelmanasettelu/teorian-muodostaminen

Hevner, A. R., Salvatore, T. M., Park, J. & Ram, S. (2004, maaliskuu). Design Science in Information System Research. *MIS Quarterly*, Vol. 28 No. 1, pp. 75-105/March 2004.

Himanen, P. (2013). Ilmavoimien taistelujohtajan tehtäväanalyysi – tilannetietoisen päätöksenteon tarkastelu Critical Decision Methodin avulla. Pro gradu. Maan-puolustuskorkeakoulu.

Homeland Security. (2022, 7. heinäkuuta). ISE-SAR Functional Standard. ISE-FS-200, v. 1.5.5, 23.2.2015. Noudettu 21.11.2024 osoitteesta https://www.dhs.gov/publication/ise-sar-functional-standard

Homeland Security Systems Engineering and Development Institute HSSEDI™. (2018, huhtikuu). Cyber Threat Modeling: Survey, Assessment, and Representative Framework. April 7, 2018. Toim. Deborah J. Bodeau, Catherine D. McCollum, David B. Fox.

Huoltovarmuuskeskus. (2020). Kyberhäiriötilanteet - Varautuminen ja toiminta. (Digipooli, Toim.) Huoltovarmuuskeskus. Noudettu 18.9.2020 osoitteesta https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/01/24095937/HVK-suosituksia-kyberh%C3%A4iri%C3%B6tilanteessa.pdf

Huovila, H., Korpi, J., Kortström. J., Kotovirta, V., Molarius, R., Nissilä, M., Mikkonen, P., Mäntyniemi, P., Rauhala, J., Tourula, T., Wessberg, N. & Yliaho, J. (2010). Uhkatilanteiden hallinta. Hälytys-, tilannekuva- ja varoitusjärjestelmän kehittäminen. VTT tiedotteita 2543. VTT. Noudettu 20.9.2020 osoitteesta https://cris.vtt.fi/en/publications/managing-the-emergencies-developing-an-alarm-common-operational-p https://www.vtt.fi/inf/pdf/tiedotteet/2010/T2543.pdf

Johnson, M. (2019, 20. toukokuuta). DISA seeks automated tools to identify potential cyber threats, conduct analysis. DISA Strategic Communication and Public Affairs. Noudettu 20.10.2024 osoitteesta https://disa.mil/NewsandEvents/2019/automated-tools-cyber-threats-analysisJoint Chiefs Of Staff. (2013). Joint publication 2-0, joint intelligence. Noudettu 15.10.2024 osoitteesta https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

Järvenpää, A-M., Kunttu, I. & Mäntyneva, M. (2020, heinäkuu). Using Foresight to Shape Future Expectations in Circular Economy SMEs. TIM Technology Innovation Management Review. Noudettu 10.3.2021 osoitteesta https://timreview.ca/article/1374

Järvinen, P. (2021). Improving guidelines and developing a taxonomy of methodologies for research in information systems. University of Jyväskylä, 2021. JYU Dissertations. ISSN 2489-9003; 414, ISBN 978-951-39-8789-3. Noudettu 10.3.2024 osoitteesta http://urn.fi/URN:ISBN:978-951-39-8789-3

Kalakoski, V. 2016. Cognitive ergonomics. Finnish Institute of Occupational Health. Noudettu 7.10.2020 osoitteesta https://oshwiki.eu/wiki/Cognitive_ergonomics

Kamppinen, M. (1999). Enkelten aika: eri kulttuurien aikakäsitykset. Futura 1/99. UTU Moodle. Artikkeli esitetty 13.1.1999 Tieteen päivillä ja julkaistu Tieteen päivien yhteenvetojulkaisussa ”Matkalla tulevaisuuteen”.

Karagiannopoulou, A., Tsertou, A., Tsimiklis, G. & Amditis, A. (2022, 4. maaliskuuta). Data Fusion in Earth Observation and the Role of Citizen as a Sensor: A Scoping Review of Applications, Methods and Future Trends. *Remote Sens. 2022*, 14, 1263. Noudettu 10.8.2024 osoitteesta https://doi.org/10.3390/rs14051263

Katz, B. (2020a, lokakuu). The Analytic Edge - Leveraging Emerging Technologies to Transform Intelligence Analysis. *CSIS Briefs.* October 2020. Noudettu 15.10.2020 osoitteesta https://www.csis.org/analysis/analytic-edge-leveraging-emerging-technologies-transform-intelligence-analysis

Katz, B. (2020b, huhtikuu). The Intelligence Edge - Opportunities and Challenges from Emerging Technologies for U.S. Intelligence. *CSIS Briefs*. April 2020. Noudettu

15.10.2020 osoitteesta https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence

Kitler, W. (2021). National Security Theory and Practice. The Publishing House of the Society of Defence Knowledge. Warsaw 2021. ISBN 978-83-960228-3-7. Noudet-tu 14.8.2024 osoitteesta https://www.researchgate.net/publication/351117604

Kokar, M. & Endsley, M. (2012). Situation Awareness and Cognitive Modeling. *IEEE Intelligent Systems*, Volume: 27, Issue: 3, May-June 2012, p. 91 – 96. The IEEE Computer Society. Noudettu 12.3.2020 osoitteesta https://doi.org/10.1109/MIS.2012.61

Koppa (2009, 28. huhtikuuta, 2010, 25. helmikuuta, 2015, 23. huhtikuuta). Menetelmäpolku. Jyväskylän yliopisto, Digipalvelut, Korppi, Avoimen yliopiston Koppa. Noudettu 17.8.2020 osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku ja https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/valmiit-dokumentit-ja-tuotetut-dokumentit

Korhonen, A. (2024, 31. lokakuuta). Nyt se sanotaan suoraan: Venäjä on Suomen energiayhtiöitä päivittäin riivaavien verkkohyökkäysten taustalla – muukin vakoilu yhä yleisempää. MTV Uutiset 31.10.2024 klo 06:39. Noudettu 1.11.2024 osoitteesta https://www.mtvuutiset.fi/artikkeli/nyt-se-sanotaan-suoraan-venaja-on-suomen-energiayhtioita-paivittain-riivaavien-verkkohyokkaysten-taustalla-muukin-vakoilu-yha-yleisempaa/9037988#gs.hnhot8

KORP Kielipankki (2024). Konkordanssihaku termistä "uhka". Noudettu 20.11.2024 osoitteesta https://www.kielipankki.fi/tuki/korp/

Kovanen, T., Nuojua, V. & Lehto, M. (2018, 8.–9. maaliskuuta). Cyber Threat Landscape in Energy Sector. Toimittaja W. D. National Defense University. Proceedings of the 13th International Conference on Cyber Warfare and Security Kokoaja University of Jyväskylä. Noudettu 12.9.2020 osoitteesta https://www.researchgate.net/publication/338215941_Cyber_Threat_Landscape_in_Energy_Sector_Cyber_Threat_Landscape_in_Energy_Sector

Kovanen, T. (2021). Cyber-threat aspects in a complex system-of-systems environment: A case study in remote pilotage. University of Jyväskylä, 2021. JYU Dissertations. ISSN 2489-9003; 409, ISBN 978-951-39-8771-8 (PDF). Noudettu 10.2.2022 osoitteesta http://urn.fi/URN:ISBN:978-951-39-8771-8

Kuusisto-Niemi, S. & Saranto, K. (2009). Sosiaali- ja terveydenhuollon tiedonhallinta - Paradigma tieteenalan perustana. Health and Human Services Informatics - Paradigmatic basis. Kuopion yliopisto, Terveyshallinnon ja -talouden laitos, Sosiaali- ja terveydenhuollon tietohallinto. *FinJeHew* 2009; 1(1), s. 19–23.

Kyberturvallisuuskeskus (2023, 6. maaliskuuta). Näin keräät ja käytät lokitietoja. Noudettu 6.3.2023 osoitteesta

KvantiMOTV (n.d.). Menetelmäopetuksen tietovaranto. Tampere. Yhteiskuntatieteellinen tietoarkisto. Noudettu 2.10.2024 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/

Lehto, M. (2019, 26. huhtikuuta). Kybermaailman ilmiöitä ja määrittelyjä. Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisu. 26.4.2019, v10.0, 13.

Lercari, N., Jaffke, D., Campiani, A., Guillem, A., McAvoy, S., Delgado, G.J., Bevk Neeb, A. (2021, 15. lokakuuta). Building Cultural Heritage Resilience through Remote Sensing: An Integrated Approach Using Multi-Temporal Site Monitoring, Datafication, and Web-GL Visualization. *Remote Sens. 2021*, 13, 4130. Noudettu 10.8.2024 osoitteesta https://doi.org/10.3390/rs13204130

Li, Y., Huang, G., Wang, C. & Li, Y. (2019). Analysis framework of network security situational awareness and comparison of implementation methods. *EURASIP Journal on Wireless Communications and Networking* (2019) 2019:205. Noudettu 10.8.2024 osoitteesta https://doi.org/10.1186/s13638-019-1506-1

Luis, A., Garnett, K., Pollard, S. J. T., Lickorish, F., Jude, S. & Leinster, P. (2021, 25. toukokuuta). Fusing strategic risk and futures methods to inform long-term strategic planning: case of water utilities. *Environment Systems and Decisions* (2021) 41:523–540. Noudettu 10.8.2024 osoitteesta https://doi.org/10.1007/s10669-021-09815-1

Luukkainen, K. (2020, 7. syyskuuta). Verkostoissa kyberturvallisuuden haasteita ratkotaan yhdessä. Suomi: Kyberturvallisuuskeskus. Noudettu 16.9.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkostoissa-kyberturvallisuuden-haasteita-ratkotaan-yhdessa

Malaska, P. (2013). Tulevaisuustietoisuudesta ja tulevaisuudesta tietämisestä: Tulevaisuus mielenkiinnon kohteena. Teoksessa Kuusi, O., Bergman, T. & Salminen, H. *Miten tutkimme tulevaisuuksia?* 3. uudistettu painos. Helsinki. Tulevaisuuden tutkimuksen seura ry, s. 14–22.

Mayer, J., Steinecke, N. & Quick, R. (2011). Improving the Applicability of Environmental Scanning Systems: State of the Art and Future Research. University of St. Gallen. Darmstadt University of Technology. M. Nüttgens et al. (Eds.): *Governance and Sustainability in IS*, IFIP AICT 366, pp. 207–223, 2011. © IFIP Interna-tional Federation for Information Processing 2011

McMahon, D., Rohozinski, R. & Canada, B. (2013, heinäkuu). The Dark Space Project. Scientific Authority Rodney Howes DRDC Centre for Security Science Contractor. Report DRDC CSS CR 2013-007 July 2013. The Minister of National Defence.

Mission Support Center (2016, elokuu). Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. Analysis report. Idaho National Laboratory. August 2016.

Meretvuo, M. (2021). Yritysvakoilu: tilannekuva, menetelmät ja estäminen. Jyväskylän yliopisto, 2021. Turvallisuus ja strateginen analyysi, pro gradu -tutkielma.

Moilanen, P. (2021a). Turvallisuuden käsite ja sen muutos. Luento. Moodle. Jyväskylän yliopisto.

Moilanen, P. (2021b)). Kompleksisuus ja resilienssi. Videoluento 28.4.2021. Jyväskylän yliopisto.

Mujinga, M., Kroeze, J. H. & Eloff, M. (2017). A socio-technical approach to information security. Conference paper August 2017. Noudettu 14.4.2020 osoitteesta https://www.researchgate.net/publication/320288245

MSO Management Solutions (2014). Operational risk management in the energy industry.

Mäklin, E. (2024, 17. marraskuuta). Olkiluoto 3:n sähköntuotanto keskeytyi. Yle uutisartikkeli 17.11.2024 klo 18.07. Noudettu osoitteesta https://yle.fi/a/74-20125188

Naderpour, M., Nazir, S. & Lu, J. (2015, syyskuu). The Role of Situation Awareness in Accidents of Large-scale Technological Systems. *Process Safety and Environmental Protection,* Volume 97, September 2015, Pages 13-24. Noudettu 28.11.2020 osoitteesta https://www.sciencedirect.com/science/article/abs/pii/S0957582015001032?via%3Dihub

Nazir, H. M. J. & Han, W. (2022, 25. tammikuuta). Proliferation of Cyber Situational Awareness: Today's Truly Pervasive Drive of Cybersecurity. Hindawi *Security and Communication Networks*, Volume 2022, Article ID 6015253, 16 pages. Noudettu 10.8.2024 osoitteesta https://doi.org/10.1155/2022/6015253

Nevalainen, R., Tukiainen M. ja Myllymäki, R. (2021). *Resilienssi – Palaudu paremmaksi järjestelmäksi, organisaatioksi tai yhteiskunnaksi*. Ketterät Kirjat Oy. Kirja.

Niemelä, T. (2021). Strategisen tiedustelun tukeminen tiedonlouhinnalla – uutisdatasta tiedustelutiedoksi. Jyväskylän yliopisto, 2021, Kyberturvallisuus, pro gradu -tutkielma. Noudettu 20.10.2024 osoitteesta https://jyx.jyu.fi/handle/123456789/76195

Niiniluoto, I. (1999). Avajaisesitelmä Tieteen päivillä 13.1.1999. Tieteellisten seurain valtuuskunta. Turun yliopisto, Moodle, Tulevaisuudentutkimuksen tieteellinen perusta.

Niiniluoto, I. (2013). Tulevaisuustietoisuudesta ja tulevaisuudesta tietämisestä: Tulevaisuuksista tietämisen lähtökohdat: Tulevaisuudentutkimus - Tiedettä vai taidetta? Luku 3, teoksessa Kuusi, O., Bergman, T. & Salminen, H. *Miten tutkimme tulevaisuuksia*? 3. uudistettu painos. Helsinki. Tulevaisuuden tutkimuksen seura ry. s. 23–30.

National Institute of Standards and Technology NIST. (2012). Risk assessment guidance. NIST Special Publication (SP) 800-30R1. Noudettu 10.11.2024 osoitteesta https://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

National Institute of Standards and Technology NIST. (2020, joulukuu). Security and Privacy Controls for Federal Information Systems and Organizations. Special Publi-

cation 800-53 Revision 5, publication Date September 2020, updates Dec 2020. Noudettu 5.6.2024 osoitteesta DOI https://doi.org/10.6028/NIST.SP.800-53r5

Nitoslawski, S. A., Wong-Stevens, K., Steenberg, J. W. N., Witherspoon, K., Nesbitt, L., & Konijnendijk van den Bosch, C. C. (2021, 16. kesäkuuta). The digital forest: Mapping a decade of knowledge on technological applications for forest ecosystems. *Earth's Future*, 9, e2021EF002123. Noudettu 10.8.2024 osoitteesta https://doi.org/10.1029/2021EF002123

North American Electric Reliability Corporation NERC. (2017, maaliskuu). NERC Reliability Guideline: Situational Awareness for the System Operator 12 Approved by the Operating Committee: March 7, 2017.

Organization for the Advancement of Structured Information Standards OASIS. (2017-2024). STIX. TAXII. The OASIS Cyber Threat Intelligence (CTI). Noudettu 17.11.2024 osoitteesta https://oasis-open.github.io/cti-documentation/

Ortamo, S. (2024, 21. huhtikuuta). Venäjä näyttää nyt tekevän kyberiskuja länsimaiden vesilaitoksiin – Mikko Hyppönen: ”Aikamoinen uutinen”. Yle uutisartikkeli, 21.4.2024 klo 10.30. Noudettu 21.4.2024 osoitteesta https://yle.fi/a/74-20084689

OWASP. (n.d.). Threat Modeling. The Open Worldwide Application Security Project. Noudettu 20.10.2024 osoitteesta https://owasp.org/www-community/Threat_Modeling

Pantsu, P. (2023, 15. maaliskuuta). Itä-Suomi ei ehkä jääkään tuulivoimapaitsioon – selvitysmies löysi keinoja sallia voimaloita: Awacs-tutkakone, sensoreita, mallia Britanniasta. Yle uutisartikkeli 15.3.2023 klo 14.49, päivitetty 16.3.2023 klo 8.47. Noudettu 20.3.2023 osoitteesta https://yle.fi/a/74-20022237

Peffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, Winter 2007-8. Vol. 24, No. 3. M. E. Sharpe Inc. 45-77.

Peters, M. A., Jandric, P. & Hayes, S. (2021, 11. tammikuuta). Biodigital Philosophy, Technological Convergence, and Postdigital Knowledge Ecologies. *Postdigital Science*

and Education (2021) 3:370–388. Noudettu 10.8.2024 osoitteesta https://doi.org/10.1007/s42438-020-00211-7

Pherson, K. & Pherson, R. (2017). Critical Thinking for Strategic Intelligence (2nd ed.). Kindle Edition. Thousand Oaks. SAGE Publications and CQ Press. Second Edition. ISBN 978-1-5063-1688-8. s.24.

Pilgrim, T. (2021, 25. huhtikuuta). MI6 checking nations 'play fair' over climate change commitments. The Standard, uutisartikkeli 25.4.2021. Noudettu 26.4.2021 osoitteesta https://esdating.standard.co.uk/news/uk/richard-moore-mi6-china-times-radio-whitehall-b931605.html

Pöyhönen, J. (2020). Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa, Systeemiajattelu. ISBN 978-951-39-8258-4 (PDF). JYU Dissertations 270. Noudettu 20.11.2020 osoitteesta http://urn.fi/URN:ISBN:978-951-39-8258-4

Rantamäki, A. & Jalonen, H. (2022). Hallinnan informaatioresilienssiä etsimässä – Tutkimusmatka käsitteen juurille. Hallinnon Tutkimus 41 (1), 35–51, 2022.

Rimppi, S. & Kivisaari, E. (2024, 30. lokakuuta). Uhkaako kolmas maailmansota? Näin asiantuntijat arvioivat. Iltalehti 30.10.2024 klo 08:08. Noudettu 1.11.2024 osoitteesta https://www.iltalehti.fi/ulkomaat/a/bce86330-2de3-41f2-a37b-d08b19c8b02c

RiskIntelligence (2024). Understanding the difference between risk and threat. Noudettu 8.10.2024 osoitteesta https://www.riskintelligence.eu/background-and-guides/understanding-the-difference-between-risk-and-threat

Rousku, K. (2019). Taisto19-harjoitusraportti ja yhteenveto. JUDO. Digi- ja väestötietovirasto.

Rozite, V., Miller, J. & Oh, S. (2023, 2. marraskuuta). Why AI and energy are the new power couple. International Energy Agency IEA. Noudettu 10.12.2023 osoitteesta https://www.iea.org/commentaries/why-ai-and-energy-are-the-new-power-couple

Rubin, A. (n.d.) Toimintaympäristön muutosten tarkastelu. TOPI – tulevaisuudentutkimuksen oppimateriaali. Tulevaisuuden tutkimuskeskus, Turun kauppakorkea-

koulu, Turun yliopisto. Noudettu 10.11.2024 osoitteesta https://tulevaisuus.fi/menetelmat/toimintaympariston-muutosten-tarkastelu/

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Verkkojulkaisu, Tampere, Yhteiskuntatieteellinen tietoarkisto. Noudettu 14.11.2024 osoitteesta https://www.fsd.uta.fi/menetelmaopetus/

Sharda, R., Delen, D. & Turban, E. (2018). Business Intelligence, Analytics, and Data Science: A Managerial Perspective. 4th edition. Pearson.

Svenska Kraftnät. (2024, 15. toukokuuta). Öppen antagonistisk hotbild för svensk elförsörjning. Ärende nr: Svk 2024/2196 Datum: 2024-05-15. pdf. Noudettu 15.5.2024 osoitteesta https://www.svk.se/siteassets/3.sakerhet-och-beredskap/sakerhetsskydd/dokument/oppen-antagonistisk-hotbild-for-svensk-elforsorjning.pdf

Taleb, N. N., & West, J. (2023). Working with Convex Responses: Antifragility from Finance to Oncology. *Entropy* (Basel), 2023 Feb 13;25(2):343. Noudettu 20.10.2024 osoitteesta doi: 10.3390/e25020343

TEPA-termipankki. (2020). Tilannekuva. Erikoisalojen sanastojen ja sanakirjojen kokoelma. Sanastokeskus TSK. Noudettu 4.12.2020 osoitteesta http://www.tsk.fi/tepa/fi/haku/tilannekuva

Thiele, L. P. (2020, 5. syyskuuta). Integrating political and technological uncertainty into robust climate policy. *Climatic Change* (2020) 163:521–538. Noudettu 10.8.2024 osoitteesta https://doi.org/10.1007/s10584-020-02853-9

Tieteen termipankki. (2020). Käsite. https://www.tieteentermipankki.fi/wiki/Nimitys:käsite

Tieteen termipankki (2024, 26. helmikuuta). Taloustiede: innovaatio. Noudettu 14.3.2024 osoitteesta https://tieteentermipankki.fi/wiki/Taloustiede:innovaatio

Tieteen termipankki (2016). Nimitys: sosio-tekninen järjestelmä. Noudettu 18.7.2024 osoitteesta https://www.tieteentermipankki.fi/wiki/Nimitys: sosio-tekninenjärjestelmä

Tieteen termipankki. (2020). Käsite. Noudettu 19.9.2020 osoitteesta https://www.tieteentermipankki.fi/wiki/Nimitys:käsite

Tieturi Oy. (2013, 15.–17. huhtikuuta). Vaatimusten määrittely ja hallinta. V. 6.5.

Traficom. (2019). Kyberharjoitusskenaariot 2020. Skenaarioesimerkkejä harjoituksen järjestäjälle. Traficomin julkaisuja 121/2019. Toimittaja Huoltovarmuuskeskus. Noudettu 16.8.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusskenaariot2020.pdf

Traficom. (2019). Kyberharjoitusohje - Käsikirja harjoituksen järjestäjälle. 26/2019. ISSN 2669-8757. Toimittaja Huoltovarmuuskeskus. Kyberturvallisuuskeskus.

Tuominen, M., Rapeli, M. & Mussalo-Rauhamaa, H. (2014). Alueellinen varautuminen ja valmiussuunnittelu sairaanhoitopiireissä. STM. Sosiaali- ja terveysministeriön raportteja ja muistioita 2014:37. Noudettu 19.9.2020 osoitteesta http://urn.fi/URN:ISBN:978-952-00-3527-3

Turvallisuuskomitea. (2017). Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 2.11.2017. Valtioneuvosto. Noudettu 19.9.2020 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Turvallisuuskomitea. (2018). Kyberturvallisuuden sanasto. TSK52. Sanastokeskus TSK ry.

Ukkonen, R. & Ruokangas, N. (2024, 20. heinäkuuta). Voimalinjan pitäisi tuoda halpaa sähköä Ruotsista, mutta asiantuntija pelkää, että Suomi jää nuolemaan näppejään. Yle uutisartikkeli, päivitetty 20.7.2024 klo 13.41. Noudettu 20.7.2024 osoitteesta https://yle.fi/a/74-20100435?utm_source=sovial-media-share&utm_medium=social&utm_campaign=ylefiapp

U.S. Department of Energy & U.S. Department of Homeland Security. (2022, kesäkuu). Cybersecurity Capablity Maturity Model C2M2. Version 2.1 June 2022. Noudettu 3.10.2024 osoitteesta https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

U.S. Department of Energy (n.d.). The President’s Critical Infrastructure Protection Board, Office of Energy Assurance. 202/287-1808; 301/903-3777- Noudettu 25.10.2020 osoitteesta https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Vainio, J. (2016). Energiaturvallisuus Baltian maissa – Energiajärjestelmien muutos uudelleenitsenäistymisestä nykypäivään. Pro gradu –tutkielma. Turun yliopisto, Politiikan tutkimuksen laitos, Yhteiskuntatieteellinen tiedekunta, Valtio-oppi. https://www.utupub.fi/bitstream/handle/10024/122832/gradu2016Julia_Vainio_valtio-oppi.pdf?sequence=2&isAllowed=y

Vinci, A. (2020, 31. elokuuta). The Coming Revolution in Intelligence Affairs - How Artificial Intelligence and Autonomous Systems Will Transform Espionage. *The Foreign Affairs*, August 31, 2020. Noudettu 15.10.2020 osoitteesta https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs

Väylä. (2011). Tilannetietoisuus ja tilannekuva. Noudettu 19.9.2020 osoitteesta https://julkaisut.vayla.fi/pdf3/lts_2011-54_tilannetietoisuus_ja_tilannekuva_web.pdf

Wang, M., Song, G., Yu, Y. & Zhang, B. (2023, 19. toukokuuta). The Current Research Status of AI-Based Network Security Situational Awareness. *Electronics* 2023, 12, 2309. Noudettu 10.8.2024 osoitteesta https://doi.org/10.3390/electronics12102309

West P., Abbott, P. & Probst, P. 2014. Alarm Fatigue: A Concept Analysis. *OJNI* Volume 18, Number 2 1 June 2014. WWW document. Noudettu 20.10.2020 osoitteesta https://www.himss.org/alarm-fatigue-concept-analysis

Westerdahl, K. (2019, 30. tammikuuta). Öppen hotbild för elsektorn. Januari 2020/287. Ruotsi. Noudettu 14.9.2020 osoitteesta https://www.energisakerhetsportalen.se/media/10214/oeppen-hotbild-slutlig.pdf

Whitworth, B. (2010, marraskuu). The social environment model: Small heroes and the evolution of human society. Massey University. Artikkeli. First Monday, November 2010. Noudettu 5.6.2024 osoitteesta DOI: 10.5210/fm.v15i11.3173.

World Energy Council (2019). Cyber challenges to the energy transition In Partnership with Marsh & McLennan Companies and Swiss Re Corporate Solutions. Insights brief 2019.

Yleinen suomalainen ontologia YSO. (2019 ja 2020). Tilannetietoisuus. Noudettu 3.8.2020 osoitteesta http://finto.fi/fi/

Yleinen suomalainen ontologia YSO. (2023). Ontologiat (tiedonhallinta). Noudettu 16.5.2024 osoitteesta http://www.yso.fi/onto/yso/p22929

Yoran, A. (2016, maaliskuu). RSA Research. RSA Conference. San Francisco, U.S. Noudettu osoitteesta https://www.rsaconference.com/library/blog/rsa-president-amit-yoran-our-problem-isnt-a-technology-problem

Zhang , J. Feng, H., Liu, B. & Zhao, D. (2023, 27. helmikuuta). Survey of Technology in Network Security Situation Awareness. *Sensors 2023*, 23, 2608. Noudettu 10.8.2024 osoitteesta https://doi.org/10.3390/s23052608