Marko Leponen

PRO GRADU
RESILIENSSI KYBER-FYYSISESSÄ SOSIAALISESSA SYSTEEMISSÄ – TARKASTELUSSA TURVALLISUUSSYSTEEMIN RESILIENSSI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Leponen, Marko
Resilienssi kyber-fyysisessä sosiaalisessa systeemissä – tarkastelussa turvallisuussysteemin resilienssi
Jyväskylä: Jyväskylän yliopisto, 2019, 68 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja: Seppänen, Ville

Tässä tutkimuksessa käsitellään kyber-fyysisen sosiaalisen systeemin teoriaa ja sen resilienssiä. Tutkimuksen teoriaosuuden tarkoituksena oli selvittää, miten sosiaalisen systeemiteorian avulla voidaan kuvata turvallisuusjärjestelmää kyber-fyysisenä sosiaalisena systeeminä ja miten resilienssi voidaan määritellä tällaisessa systeemissä. Tutkimuksen empiirisessä osuudessa tutkittiin turvallisuussysteemin resilienssiä ja siihen liittyviä tekijöitä systeemiin kohdistuvassa moniulotteisessa iskussa. Tutkimuksen aihe on tärkeä, koska sen avulla voidaan havainnollistaa turvallisuusjärjestelmän toimintaa kokonaisuutena ja sillä saadaan tietoa systeemin kestävyyteen ja sietokykyyn vaikuttavista tekijöistä. Kirjallisuustutkimus suoritettiin kirjallisuusanalyysiä käyttäen. Empiirisessä osiossa käytettiin skenaarioanalyysiä, sekä asiantuntijahaastattelua. Tutkimuksen teoriaosuudessa havaittiin, että turvallisuussysteemi pitää sisällään sekä fyysisen-, että kyberulottuvuuden että sosiaalisen pääoman. Resilienssin kannalta systeemin merkittävimmät ominaisuudet olivat lujuus, sopeutuvuus ja kyky muuttua. Tutkimuksen empiirisessä osiossa havaittiin, että kyber-fyysisen sosiaalisen turvallisuussysteemin resilienssin kehittymisen kannalta monivaikutteisessa iskussa tärkeimpiä ominaisuuksia olivat systeemin kyky kehittää toimintaansa, sekä oppia aiemmista tapahtumista.

Asiasanat: Systeemiteoria, kyber-fyysinen sosiaalinen systeemi, turvallisuusjärjestelmä, resilienssi

ABSTRACT

Leponen, Marko
Minithesis Resilience in Cyber-Physical Social System - Review the Resilience of the Security System
Jyväskylä: University of Jyväskylä, 2019, 68 p.
Major subject, Master's Thesis
Supervisor: Seppänen, Ville

This study discusses the theory of the Cyber-Physical Social System and the Resilience in it. The purpose of the theoretical part of the study was to find out how the theory of Social System can describe the security system as a Cyber-Physical Social System and how resilience can be defined in such a system. In the empirical part of the study the resilience of the security system and related factors were investigated in a multidimensional attack to the system. The subject of the study is important because it can be used to describe how the security system works as a whole and provides information on factors affecting the resistance of the system and its resilience. Literature research was conducted using literary analysis. In the empire research were used scenario analysis and expert interview. In the theoretical part of the research, key findings was that the security system includes both physical and cyber dimensions as well as social capital. The most important characteristics of the system resilience were strength, adaptability and ability to change. In the empirical part of the research, it was found that the most important characteristics of the cyber-physical social security system's resilience in the multidimensional attack were the system's ability to develop activities and learn from previous events.

Keywords: System theory, Cyber-Physical Social System, National Security Authoritaty, Resilience

KUVIOT

KUVIO 1: Systeemin eri avoimuuden tasot....16
KUVIO 2: Avoimen systeemin toimintamalli....17
KUVIO 3: Kyber- ja fyysisen maailman suhde....22
KUVIO 4: Kyber-fyysisen järjestelmän havainnollistaminen ja toiminta National Science Foundationin mukaan....23
KUVIO 5: Kyber-fyysisen sosiaalisen systeemin kuvaus....25
KUVIO 6: Systeemin resilienssin kehitysprosessi....36
KUVIO 7: Skenaariotyöskentelyn vaiheet Rubinin mallin mukaan....40
KUVIO 8: Deduktiivisen tutkimuksen skenaarioanalyysin prosessikaavio....43
KUVIO 9: Deduktiivinen skenaarioanalyysi prosessina....43
KUVIO 10: Vaikuttimien analysointi prosessina....55

TAULUKOT

TAULUKKO 1: SWOT-analyysin sisäiset attribuutit....49
TAULUKKO 2: SWOT-analyysin ulkoiset attribuutit....50
TAULUKKO 3: Uhkien tunnistamiseen tarkoitettu ajatusmalli....51
TAULUKKO 4: PEST+V -Analyysi....53
TAULUKKO 5: Skenaario 1. Toivottu skenaario....57
TAULUKKO 6: Skenaario 2, negaatio....59
TAULUKKO 7: Skenaario 3, kyberhyökkäykset....61
TAULUKKO 8: Skenaario 4, luvaton tunkeutuminen ja informaatiovaikuttaminen....63

SISÄLLYS

TIIVISTELMÄ
ABTRACT
KUVIOT
TAULUKOT

1 JOHDANTO....6
1.1 Tutkimuksen tausta....7
1.2 Menetelmä ja tutkimuskysymys....8
1.3 Tutkimuksen aiheen rajaus....9
1.4 Aiempi tutkimus....9
1.5 Tutkielman rakenne....10

2 SYSTEEMITEORIA JA SYSTEEMIAJATTELU....12
2.1 Mitä on systeemiajattelu?....12
2.2 Avoin systeemi....14
2.3 Kompleksisuus sosiaalisessa systeemissä....17
2.4 Kompleksinen sopeutuva systeemi....18
2.5 Toimijaverkkoteoria....19

3 TURVALLISUUSJÄRJESTELMÄ KYBER-FYYSISENÄ SOSIAALISENA SYSTEEMINÄ....21
3.1 Kyber ja fyysinen - rinnakkaiset maailmat....21
3.2 Kyber-fyysisen sosiaalisen systeemin tekninen rakenne....24
3.3 Päätöksenteko kyber-fyysisessä sosiaalisessa systeemissä....26
3.4 Kyber-fyysinen sosiaalinen turvallisuusjärjestelmä....27

4 KYBER-FYYSISEN SOSIAALISEN SYSTEEMIN RESILIENSSI....28
4.1 Resilienssin määritelmä....28
4.2 Resilienssin yhteiskunnallinen ulottuvuus....29
4.3 Resilienssin piirteet....29
4.4 Diversiteetti resilienssin ominaisuutena....32
4.5 Sosiaalinen resilienssi systeemissä....32

5 YHTEENVETO....34
5.1 Systeemiajattelu turvallisuusjärjestelmän kuvaajana....34
5.2 Resilienssi kyber-fyysisessä sosiaalisessa systeemissä....34

6 METODOLOGIA....37
6.1 Tutkimusmenetelmä....37
6.2 Tutkimusongelma....38
6.3 Tutkimusongelman rajaus....38
6.4 Skenaarioanalyysi....38

6.4.1 Tulevaisuuskuvien rakentaminen....41
6.4.2 Useamman skenaarion rakentaminen....42
6.4.3 Skenaarioanalyysi prosessina....42
6.5 Asiantuntijahaastattelumenetelmä resilienssin analysoinnissa....44
6.5.1 Asiantuntijoiden valinta....44
6.5.2 Haastattelun anonymiteetti....45
6.6 Tutkimuskohde....45
7 TULOKSET....47
7.1 Nykytilan kartoitus....47
7.1.1 Skenaarion laajuuden määrittely....47
7.1.2 Keskeiset toimijat....48
7.1.3 Systeemin tarpeet, toiveet ja odotukset....48
7.1.4 SWOT-analyysi systeemin nykytilasta....48
7.1.5 PEST+V -analyysi....52
7.1.6 Heikot signaalit....54
7.2 Skenaariot....54
7.2.1 Skenaario 1: Toivottu skenaario....56
7.2.2 Skenaario 2: Negaatio....58
7.2.3 Skenaario 3: Kybervaikuttaminen....60
7.2.4 Skenaario 4: Fyysinen isku ja informaatiovaikuttaminen....62
7.3 Resilienssin analysointi....64
7.3.1 Asiantuntijahaastattelun SWOT-analyysin yhteenveto....65
8 JOHTOPÄÄTÖKSET JA POHDINTA....66
8.1 Reliaabiliteetti ja validiteetti....66
8.2 Tulosten pohdinta....67
8.3 Jatkotutkimusaiheet....68
LÄHTEET....69
LIITTEET....74

1 JOHDANTO

Yhteiskunnan turvallisuudesta vastaavilla toimijoilla on varsin merkittävä rooli yhteiskunnan kokonaisturvallisuuden ylläpitäjänä. Näiden toimijoiden harteilla lepää vastuu yhteiskunnan turvallisuudesta ja sen toimivuudesta kaikissa olosuhteissa. Näitä toimijoita ovat yleisesti viranomaiset, sekä muut yhteiskunnalliset järjestöt, jotka yhdessä muodostavat kokonaisturvallisuudesta vastaavan kokonaisuuden. Näiden toimijoiden tehtävänä yhdessä on ylläpitää ja kehittää yhteiskunnan turvallisuutta ja vakautta.

Kokonaisuuteen kuuluvien eri viranomaisten ja muiden toimijoiden kirjo on laaja, vaikka turvallisuustoimijoina yleisesti nähdään vain sisäisen turvallisuuden (poliisi) tai ulkoisen turvallisuuden (puolustusvoimat ja rajavartiolaitos) toimijat. Tässä tutkimuksessa tarkastellaan tämän kokonaisuuden toimintaa abstraktin objektin, systeemin näkökulmasta. Tutkimuksen kohteena on siis yhteiskunnan sisäisen turvallisuuden toimijat systeeminä. Tätä edellä mainittua järjestelmää tutkitaan kyber-fyysisenä systeeminä.

Tutkimuksen teoreettisessa osuudessa tutkitaan systeemiteorian näkökulmasta kyber-fyysistä sosiaalista systeemiä, sekä resilienssin käsitettä tällaisessa systeemimallissa. Empiirisessä osuudessa tutkitaan systeemin resilienssiä, kun systeemiin kohdistetaan monitasoisia iskuja ja samalla tutkitaan sitä, miten se vaikuttaa toiminnassa systeemitasolla. Tutkimuksen tärkeimpänä tavoitteena on löytää ymmärrys siitä, miten systeemi reagoi ja mitä systeemi voi tehdä kehittääkseen resilienssiään.

Yhteiskunnan toiminnan kehittämisen kannalta on merkityksellistä tutkia tällaisen systeemin toimintaa, oppimiskykyä ja kykyä sopeutua, kun ajatellaan mahdollisten yhteiskunnan rakenteisiin kohdistuvien uhkien estämistä, keskeyttämistä taikka yhteiskunnan toimijoiden (mm. viranomaisten) yhteistoimintaa tällaisessa tilanteessa. Systeemin toiminnan jatkuvuuden kannalta on tärkeää, että sen on kyettävä muutokseen säilyttääkseen toimintakykynsä ja mahdollistaakseen toimintansa myös tulevaisuudessa. Sopeutuva ja oppiva yhteiskunta (sekä sen sisällä toimivat systeemit) on merkittävä edellytys sille, että yhteiskunnalla on mahdollisuus oppimalla ja kehittymällä kyetä ennalta ehkäisemään yhteiskuntarauhaa ja sen rakenteita uhkaavien tapahtumien

konkretisoituminen tai oppia vastaamaan niihin riittävän ajoissa, oikeanlaisilla ja -aikaisilla toimenpiteillä.

1.1 Tutkimuksen tausta

Tämän tutkimuksen näkökulmaksi on otettu systeemiajattelu, jossa yhteiskunnan yhden osan toimintaa tutkitaan systeemiteorian näkökulmasta. Systeemitutkimuksen erona verrattuna yksittäisen toimijan tutkimukseen, on kokonaiskuvan saaminen koko järjestelmän toiminnasta. Luvussa 3 kuvataan systeemiajattelun teoriaa tarkemmin. Siinä yhteydessä kuvataan myös, miten systeemiajattelun mukaisesti systeemin koko ja sisältö (mitä elementtejä systeemi pitää sisällään) syntyvät aina siinä hetkessä, jossa systeemiä tarkastellaan (Kast & Rosenzweig, 1972, s. 450). Koska systeemi sisältää myös sen sisällä olevat ihmiset (inhimillinen pääoma), on varsin tärkeää saada tutkimustietoa siitä, miten systeemin henkistä kykyä (tietoisuutta) voidaan lisätä ja mikä merkitys sillä on koko systeemin resilienssin kehittämisessä. Systeemin resilienssin tutkiminen on merkityksellistä, etenkin sen toiminnan kehittämisen kannalta.

Tutkimuksen aihe on erittäin ajankohtainen, sillä oman yhteiskuntamme, että globaali turvallisuustilanne on viimevuosina muuttunut kohti epävarmuuden aikaa. Rauhan- ja kriisiajan väliin on tullut nk. harmaa tila, jossa valtioiden koskemattomuutta voidaan loukata erilaisilla ”epäsuorilla toimilla”, anonymiteetin suojista. Ne saatavat olla toimia, joihin kansainvälinen lainsäädäntö ei suoranaisesti anna vastauksia, jolloin toimet ovat lainsäädännön harmaalla alueella. Väitteitä siitä, että valtiot sotkeentuisivat toisten valtioiden sisäiseen toimintaan on esitetty useampiakin. Todisteiden esittäminen tällaisista operaatioista on haastavaa. Hyvänä esimerkkinä voidaan pitää Yhdysvaltojen presidentinvaaleja 2017, joissa kansainvälisesti epäiltiin Venäjän valtiollisena toimijana informaatio-operaatiolla vaikuttaneen vaalitulokseen.

Suomen Valtioneuvoston puolustuspoliittisessa selonteossa (2017) on katsottu Suomen turvallisuustilanteen muuttuneen ja sotilaallisten jännitteiden lisääntyneen varsinkin Itämeren alueella, sekä yleisen sotilaallisen epävarmuuden yleisesti lisääntyneen. Tämän lisäksi julkisuudessa on esitetty arvioita, että globaali turvallisuustilanne on tällä hetkellä epävakaampi, kuin koskaan kylmän sodan jälkeen. Turvallisuustilanteeseen ovat vaikuttaneet mm. valtioiden väliset poliittiset jännitteet, terrorismin pelko, kyberuhkien lisääntyminen, taloudelliset muutokset, ilmastonmuutos, väestön liikehdintä sekä lisääntynyt informaatio-vaikuttaminen. (Valtioneuvosto 2017, 8-10.)

Suomea koskevassa yhteiskunnan turvallisuusstrategiassa (2017) on myös kirjattu useita suomalaiseen yhteiskuntaan kohdistuvia mahdollisia uhkia.

Siinäkin mainitaan mm. kyberuhat, terrorismi, poliittinen vaikuttaminen, sekä ilmastolliset kriisit. (Turvallisuuskomitea 2017.)

Tutkijan näkökulmasta aihe on varsin mielenkiintoinen. Tutkimuksen kohteena olevaan systeemin kohdistuu yhä enemmän odotuksia ja vaatimuksia, sekä samalla siihen kohdistuu myös enemmän uhkia. Näiden tekijöiden yhteen sovittaminen ja niihin varautuminen edellyttävät yhä enemmän osaamista ja kykyä kehittää sitä.

1.2 Menetelmä ja tutkimuskysymys

Tutkimuksen pohjaksi on kerätty kirjallista aineistoa aiemmista systeemi- ja resilienssitutkimuksista, tieteellisistä julkaisuista, artikkeleista sekä aiheeseen liittyvästä kirjallisuudesta. Kirjallisuuskatsauksen tarkoituksena on kerätä mahdollisimman laaja-alainen kuvaus kyber-fyysisestä sosiaalisesta systeemistä, sekä systeemin resilienssin käsitteestä. Tämän tutkimuksen lähdemateriaaliksi on valittu kirjallisuutta laaja-alaisesti sosiaalisen systeemiteorian pohjalta. Sosiaalisen systeemin teoriaan on yhdistelty teoriaa kyber-fyysisestä systeemistä. Kirjallista aineistoa on kerätty eri lähteistä kokonaiskuvan luomiseksi kyber-fyysisestä systeemistä. Lopuksi kirjallisuuskatsauksessa on tarkasteltu resilienssin käsitettä ja tarkasteltu, miten sen määritelmä sopii kyber-fyysiseen sosiaaliseen systeemiin. Aineistoa on pyritty löytämään tutkimuksista ja julkaisuista, jotka tarkastelevat aihetta eri näkökulmista. Tutkimukseen on kerätty eri systeemimalleja kuvaavaa kirjallisuutta, kyber-fyysisen systeemimallin kokonaisuuden hahmottamiseksi. Aineistoa on kerätty eri kirjastojen tietokannoista, sekä Google Scholar -hakukoneella eri sähköisistä tietokannoista.

Tutkimuksen empiirisessä osuudessa yhteiskunnan turvallisuusjärjestelmää tutkitaan systeemiteorian näkökulmasta, jossa järjestelmää itsessään kuvataan kyber-fyysisenä sosiaalisena systeeminä. Tutkimuksessa keskitytään edellä mainitun systeemin määrittämiseen sekä sellaisen systeemin resilienssin tutkimiseen systeemin kohdistuvassa monivaikutteisessa iskussa. Tutkimus on laadullinen tutkimus, jonka tarkoituksena on tuottaa tietoa kyber-fyysisen sosiaalisen systeemin toiminnasta ja sen resilienssistä sekä etsiä siihen laadullista vastausta määrällisen sijaan. Hirsjärven, Remeksen ja Sajavaaran (2011) mukaan laadullisen tutkimuksen tarkoituksena on tutkia kohdetta kokonaisvaltaisesti ja kuvata todellista elämää. Tutkimuksen kantavana tutkimuskysymyksinä ovat: *Millainen on kyber-fyysinen sosiaalinen turvallisuussysteemi? Mitä tarkoitetaan resilienssillä turvallisuussysteemissä?*

1.3 Tutkimuksen aiheen rajaus

Tässä tutkimuksessa turvallisuussysteemiä tutkitaan kyber-fyysisenä sosiaalisena systeeminä, joka sisältää useita samantasoisia tai eri tasoisia systeemejä, sekä kaikkia niitä systeemin elementtejä, joita tällainen systeemi pitää sisällään. Useammat systeemin sisäiset systeemit tai elementit voivat olla yhteydessä toisiinsa, niiden toiminta voi olla osin riippuvaista toisistaan, niillä voi olla rajapintoja toistensa kanssa, mutta ne toimivat aina systeemin sisällä itsenäisesti. Tutkimuksessa on rajattu pois suljettua systeemiä koskeva kirjallisuus ja keskitytty adaptiivista, avointa sosiaalista systeemiä koskevaan aineistoon, koska juuri se kuvaa tutkimuksen kohteena olevaa sosiaalista systeemimallia parhaiten. Suljettu systeemi on rajattu pois sen vuoksi, että sen ominaisuuksiin ei kuulu vuorovaikutus ympäristönsä kanssa, jonka voidaan katsoa olevan perustavaa laatua oleva ominaisuus turvallisuusjärjestelmässä.

Tutkimuksessa ei myöskään tutkita minkään viranomaisen toimintaa taktisten menetelmien näkökulmasta, vaan tutkimuksessa pitäydytään toiminnassa systeemitasolla. turvallisuussysteemi käsitteenä pitää sisällään kaikki ne viranomaiset ja muut toimijat, jotka tutkimuksen kuvaamassa tilanteessa, nimenomaisella hetkellä toimisivat turvallisuussysteemiksi kutsutun systeemin sisällä. Näillä systeemin sisällä toimivilla viranomaisilla on useita eri tehtäviä ja vastuita, joita kansallinen tai ylikansallinen lainsäädäntö on niille asettanut. Niillä on myös omat toimialueensa, mutta näiden toimialueiden erillinen tutkiminen ei ole merkityksellistä tutkittaessa koko turvallisuussysteemin resilienssiä.

Tutkimuksessa on rajattu ulkopuolelle systeemin päätöksentekoon liittyvät yhteiskunnan poliittiset päätöksentekijät ja heidän tekemät valinnat. Tutkimus keskittyy sen hetkisen systeemin toiminnan tutkimiseen, ilman poliittista ohjausta. Poliittinen ohjaus on rajattu pois, koska tutkimuksessa keskitytään systeemin sisäiseen toimintaan.

1.4 Aiempi tutkimus

Systeemitutkimusta on tehty systeemiteorian kehittämisen jälkeen melko laajasti ja systeemiteoriaa onkin käytetty useamman tieteenalan tutkimuksen teoriapohjana. Systeemitutkimusta on tehty myös resilienssin näkökulmasta. Kyber-fyysinen systeemi terminä on tieteellisessä tutkimuksessa otettu käyttöön vasta 2010-luvulla. Erityisesti voidaan mainita ekologisen systeemin resilienssiin ja kestävään kehitykseen liittyvä tutkimus, jota on tehty kasvavassa määrin liittyen ilmaston muutokseen ja ekologisen systeemin kestävyyteen (mm. Leichenko 2011; Adger 2000).

Wang (2010) on kuvannut sosiaalisen ominaisuuden (inhimillisen pääoman) lisäämistä perinteiseen kyber-fyysiseen systeemin, sekä sen merkitystä systeemin toiminnalle. Sosiaalisella elementillä on tutkimuksessa havaittu olevan systeemin älykkyyttä (tietoisuutta) lisäävä merkitys. Wang on käyttänyt termiä "*Intelligence*", joka voidaan tässä yhteydessä kääntää suomeksi älykkyydeksi. Tutkimuksen mukaan sosiaalisen tietoisuuden lisääntyminen, lisää samalla systeemin päätöksenteon kompleksisuutta. (Wang 2010, s. 85-86.)

Xiong ym. (2015) ovat tutkineet älykästä kuljetusjärjestelmää kyber-fyysisen sosiaalisen systeemin näkökulmasta. Xiongin ym. tutkimuksessa on lähdetty ajatuksessa, että ihmisellä on merkittävä rooli kyber-fyysisen systeemin kehittäjänä ja käyttäjänä. Vaikka kyber-fyysisessä sosiaalisessa systeemissä laitteet voivat keskustella toistensa kanssa, on ihmisellä kuitenkin merkitystä systeemin hallinnan ja päätöksenteon kanssa. (Xiong ym., 2015.)

Systeemin resilienssiä on tutkittu mm. Puupposen, Paloviidan, Kortetmäen ja Silvastin (2017) tutkimuksessa maatalouden ja ruokatuotannon näkökulmasta. Tässä tutkimuksessa maatalouden resilienssiä on tutkittu osana elintarvikejärjestelmää ja maatalouden kykyä sopeutua erilaisiin muutoksiin (huoltovarmuus). Systeemin resilienssiä on tutkittu myös käskyvalta-organisaation, militaristisen systeemin, näkökulmasta Liun (2011) tutkimuksessa, jossa systeemiä on tarkasteltu johtamisen ja sen hallittavuuden kannalta. Tutkimuksessa systeemiä on tarkasteltu päätöksenteko-prosessin näkökulmasta, kun johdettavana on sekä ihmisiä, että koneita ja johtamisessa käytetään useita eri kommunikointi menetelmiä.

Ympäristön ja ekologisen systeemin tieteellisessä tutkimuksessa juuri resilienssin tutkiminen on merkittävässä roolissa. Adgerin (2000) ja Leichenkon (2011) tutkimukset keskittyvät ekologisessa systeemissä tapahtuvien muutosten sietokyvyn tutkimiseen. Adgerin (2000) tutkimus määrittelee sosiaalisen ja ekologisen systeemin resilienssin suhdetta toisiinsa ja niiden merkitystä ekologisen systeemin resilienssiä mitattaessa. Leichenkon (2011) tekemä resilienssitutkimus keskittyy ilmastonmuutoksen ja alueellisen resilienssin tutkimiseen ja kehittämiseen yhteiskunnallisen jatkuvuuden varmistamiseksi. Tutkimuksen tärkeimpiä huomioita on, että mahdollistaakseen jatkuvuuden, alueiden on kyettävä sopeutumaan tuleviin muutoksiin ja kyettävä kehittämään uusia menetelmiä selviytyäkseen.

1.5 Tutkielman rakenne

Tutkielma sisältää järjestyksessä johdannon, teoriaosuuden ja empiirisen osion. Tutkimuksen kannalta keskeisimmät käsitteet kuvataan ja määritellään sen teoriaosuudessa, sekä kuvataan kyber-fyysisen sosiaalisen systeemin teoriaa, että resilienssin käsitettä. Empiirisessä osiossa tutkintaan sosiaalisen kyber-

fyysisen systeemin resilienssiä monivaikutteisessa iskussa skenaarioanalyysiä käyttämällä. Tutkielman lopuksi asiantuntijathaastattelun avulla, asiantuntijat arvioivat tutkimuksella saatuja tuloksia.

Systeemiteoriaa, systeemiajattelua, sekä siihen liittyvää kompleksisuutta kuvataan luvussa kaksi. Kolmannessa luvussa kuvataan kyber-fyysistä systeemiä ja turvallisuussysteemiä kyber-fyysisenä sosiaalisena systeeminä. Luvussa neljä kuvataan resilienssin määritelmää, sekä resilienssiä systeemin ominaisuutena. Luvussa viisi on yhteenveto kirjallisuuskatsauksesta ja kyber-fyysisen sosiaalisen systeemin resilienssistä. Empiirisessä osuudessa tutkitaan systeemin resilienssiä skenaarioanalyysin avulla ja asiantuntijahaastatteluilla. Empiriisien osuuden tutkimusmenetelmät on esitetty luvussa kuusi. Luvussa seitsemän esitettään skenaarioanalyysi ja sen tulokset, sekä peilatataan skenaarioanalyysillä saatuja tuloksia asiantuntijahaastattelun tuloksiin. Luvussa kahdeksan on esitetty tutkimuksen johtopäätökset, sekä jatkotutkimusaiheet.

2 SYSTEEMITEORIA JA SYSTEEMIAJATTELU

Tämän luvun tarkoituksena on esitellä lukijalle teoria, jolle kyber-fyysinen sosiaalien systeemi perustuu. Luvussa esitellään tutkimuksen viitekehykseksi valittuja systeemiteorian malleja, ohjataan lukijaa systeemiajattelumalliin, sekä syvennetään systeemiajattelua lisäämällä siihen uusia ulottuvuuksia kuten kyber-maailma. Luvun tarkoituksena on rakentaa pala palalta kyber-fyysisen sosiaalisen turvallisuussysteemin kuvaus. Lisäksi luvussa esitellään lyhyesti sellaisia systeemiteorian ulottuvuuksia, joita tutkimuksessa on tutkimuksellisista syistä rajattu pois ja perustellaan, miksi nämä systeemimallit eivät sovi tässä tutkittavaan systeemimalliin.

Kyber-fyysinen sosiaalinen systeemi koostuu useista eri elementeistä, jotka systeemi omistaa. Tässä luvussa kuvataan kyber-fyysisen sosiaalisen systeemin elementtejä ja niiden ominaisuuksia. Tämän tutkimuksen teoreettinen viitekehys, systeemiteoria, rakentuu saksalaisen sosiologi Niklas Luhmannin kehittämälle systeemiajattelulle ja sen kompleksisuuden tarkastelulle. Tässä luvussa tarkastellaan erilaisia systeemimalleja, joiden avulla kuvataan tutkimuksessa tarkasteltu systeemimalli. Tämän luvun teorian kuvauksen perusteella luodaan kuva siitä, millaisesta näkökulmasta tutkimuksen systeemiä tarkastellaan ja millaiselle teoriapohjalle se muodostuu. Näiden systeemimallien sekä niiden tulkintojen valitsemista tutkimuksen viitekehykseksi perustellaan alla olevissa luvuissa.

2.1 Mitä on systeemiajattelu?

Modernin sosiaalisen systeemin teoria perustuu Luhmannin (1995) kehittämän sosiaalisen systeemiteorian pohjalle. Teoria perustuu siinä tehtyyn olettamukseen, että *on olemassa systeemejä*. Luhmann onkin omassa sosiaalisen systeemin teoriassa käyttänyt juuri tätä olettamusta teoriansa perustana. Systeemiteoria ei itsessään vahvista systeemin olemassa oloa, vaan teoria perustuu edellä mainitulle oletukselle niiden olemassa olosta ja rakentuu tämän oletuksen päälle. Vaikka teoria perustuukin olettamukselle, on teorialla kuitenkin viittaus reaalimaailmaan. Olettamus systeemistä vastaa Luhmannin

mukaan jotain olemassa olevia reaalimaailman systeemiä (mm. ekologinen systeemi) vastaavia malleja. (Luhmann, Bednarz & Baecker, 1995, s. 13.)

Veermer (2006) kuvaa Luhmannin teorian pohjautuvan vahvasti olettamuksille, joita tieteellisessä tutkimuksessa voidaan hänen mukaansa pitää teoriaa esittävinä pätevinä toteamuksina (Veermer, 2006, s. 12). Skyttner (2005) lähestyy systeemimallia samasta ajatuksesta, kuin Luhmann ym. (1995) ja Vermeer (2006). Skyttnerin mukaan systeemiajattelu on tapa hahmottaa maailmaa tai jonkin toiminnan kuvausta, eikä se edellytä että systeemin tarvitsee *"fyysisesti olla olemassa"* vaan se voi olla abstrakti käsitys jostain olemassa olevasta kokonaisuudesta. Systeemimalli on siis abstraktio jostain olemassa olevasta, ja sen tehtävänä on mahdollistaa järjestelmän tutkiminen objektina. (Skyttner, 2005, s. 57.)

Systeemiteorian mukaan kaikki ovat systeemejä ja systeemit elävät ympäristössään. Kyseessä on kuitenkin filosofinen paradigma, sillä systeemiteorian mukaan myös ympäristö on systeemi ja systeemi rajautuu ympäristöönsä. Systeemin ja ympäristön suhde on abstraktio ja se tulee myös nähdä sellaisena. Systeemin ja ympäristön määrittäminen on teorian mukaan hankalaa. Systeemi rajautuu ympäristöönsä, jolloin se samalla määrittää itse oman rajauksensa suhteessa ympäristöönsä. Se ei kuitenkaan määrittele ympäristö-systeemin rajoja, koska teorian mukaan mikään toinen systeemi ei voi rajata toista systeemiä. Systeemin ympäristö määrittyy itsenäisesti omana systeeminä, sen suhteesta systeemiin. Jokainen ympäristö on uniikki, eikä se koskaan näyttäydy muille systeemeille samanlaisena. Ympäristö on samalla myös systeemi ja se sisältää myös kompleksisuutta (kuten kompleksisia systeemejä). Systeemiä ei ole olemassa ilman ympäristöään, mutta ympäristö ei kuitenkaan määritä systeemiä. (Luhmann ym., 1995, s. 15-19, 182.)

Systeemiajattelun tarkoituksena on kuvata määritellyn järjestelmän tai kohteen rakennetta, mallia, organisoitumista tai toimintaa. Voidaan myös käyttää termiä kokonaisuuden kuvaaminen. Systeemiajattelu perustuukin sellaisten kokonaisuuksien tutkimiseen ja havainnointiin, joita ei voi luonnollisesti jakaa osiin ilman, että ne lakkaavat olemasta (eli menettävät oman identiteetin). Tämän voidaan Skyttnerin (2005) mukaan ymmärtää tarkoittavan sitä, että osiin jakamalla, jäljellä jääneet osat eivät olisi järjestäytynyt systeemin osa, vaan palasia irroitettuna kokonaisuudesta. Vaikka nämä osat Luhmannin ym. (1995) mukaan voisivatkin muodostaa systeemin, ei niillä olisi tuolloin Skyttnerin (2005) teoriassa edellyttää identiteettiä, jolloin niitä voisi kutsua systeemiksi. Sosiaalisen systeemin kokonaisuuden rajaus perustuu systeemin identiteettiin ja sen kykyyn sisäiseen päätöksentekoon. Tällä tarkoitetaan systeemin kykyä havaintoihin, perspektiivin tai tilanteen määrittelyyn, jonka perusteella systeemin sisällä syntyy päätös sen sisältämistä elementeistä ja sen

koosta. Systeemin kokonaisuus määrittyykin siinä hetkessä, jossa sitä tulkitaan. (Skyttner, 2005, s. 50.)

Luhmannin sosiaalisen systeemin teorian mukaan jokainen systeemi omistaa oman sisäisen maailmansa. Sisäinen maailman määritys perustuu edellä mainittuun rajaukseen kokonaisuudesta. Systeemin sisäisen maailman lisäksi sillä on ympäristö, jossa systeemi sijaitsee ja jonka kanssa (avoin) systeemi on vuorovaikutuksessa. Vuorovaikutus voi olla datan, informaation, tiedon, energian tai tuotoksen siirtymistä ympäristön ja systeemin välillä. Systeemi syntyy siinä hetkessä ja tilassa, missä se sijaitsee tai missä sille ilmenee tarve olla olemassa. Toisin kuin rakenteita (organisaatiot), (sosiaalisia) systeemejä ei perusteta, vaan systeemit syntyvät systeemin sisäisestä tarpeesta muodostaa sellainen. (Veermer, 2006, s. 11-13.)

Mentäessä systeemin rakenteessa syvemmälle havaitaan, että jokaisella sosiaalisella systeemillä on oma sisäinen järjestyksensä. Sillä on sisäinen päätöksenteko ja rakenne, jonka avulla se toimii. Systeemiä voidaan tällöin kuvata sosiaalisesti järjestäytyneeksi ja organisoituneeksi. Sosiaalisen systeemin teoria perustuu Luhmannin ym. (1995) mukaan systeemin sisäiselle ja systeemien väliselle kommunikaatiolle. Kommunikaatio on yksi Luhmannin sosiaalisen systeemin teorian kulmakivistä. Kommunikaatio saa systeemin sisällä aikaan toimintaa ja johtaa myös systeemin muutoksen. Kommunikoinnin ja toiminnan lisääntyminen lisäävät systeemin kompleksisuutta. (Kihlstrom, 2012, s. 289; Luhmann ym., 1995, s. 146, 171.)

Sosiaalisen systeemin varsin merkitsevä ominaispiirre on sen sosiaalinen aspekti. Luhmannin teorian mukaan sosiaalinen systeemi omistaa inhimillisen elementin. Luhmann itse käyttää siitä nimitystä ihminen (*human being*). Ihminen on systeemin pysyvä elementti. Yksilönä (*individual*) ihminen on yksi toimija systeemin sisällä, mutta useamman yksilön joukko muodostaa systeemin sisäisen yhteiskunnan (*society*). Yhteiskunnan muodostuminen yksilöistä on myös omiaan lisäämään systeemin kompleksisuutta. (Luhmann ym., 1995, s. 211-212.)

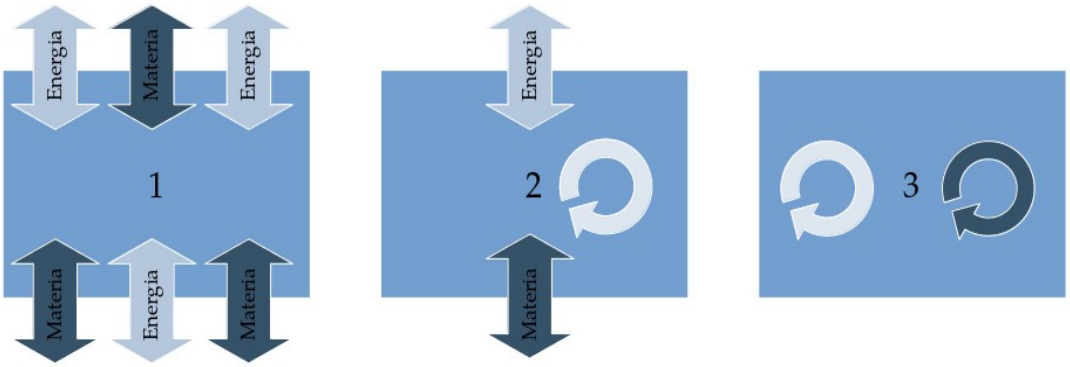
2.2 Avoin systeemi

Kast ja Rosenzweig (1972) ovat omassa tutkimuksessaan tiivistäneet systeemiteorian aiemman tutkimuksen perusteella systeemille tiettyjä merkitseviä ominaispiirteitä. Systeemit voivat olla avoimia (*open system*) tai suljettuja (*closed system*) ja ne koostuvat aina vähintään kahdesta elementistä. Edellisessä luvussa mainittiin, että systeemi koostuu kokonaisuudesta, jota ei voi jakaa osiin. Huomionarvoista kuitenkin on, että ne voidaan Kastin ja Rosenzweigin (1972) mukaan erotella eri elementeiksi. Nämä elementit muodostavat systeemin riippuvuussuhteella toisiinsa ja ovat

vuorovaikutuksessa keskenään, jolloin systeemille kehittyy oma identiteetti. Systeemin osilla on myös hierarkinen suhde toisiinsa. Systeemi voi sisältää alasysteemejä, jotka muodostavat oman hierarkisen rakenteensa. Rakenne voi täten perustua esimerkiksi osien väliseen vuorovaikutukseen tai niiden väliseen johtosuhteeseen. Kastin ja Rosenzweigin (1972) mukaan sosiaaliselle systeemille on vaikea määritellä selkeitä rajoja. Jo aiemmin todettiin, että systeemin rajaus perustuu systeemin sisäiseen päätöksentekoon systeemin koosta ja sen sisällöstä, sekä sen identiteetistä. Kast ja Rosenzweigin (1972) mukaan sosiaalisen systeemin rajat muodostuvat lisäksi vuorovaikutuksessa ympäristönsä kanssa. Systeemin rajaus perustuu siis sen sisäiseen päätökseen siitä, mitä se on, mitä systeemiin sillä hetkellä kuuluu, mutta myös sen ympäristö määrittelee systeemin koostumusta. Tällöin systeemillä ei ole yksinoikeutta sisäisesti päättää koostumuksestaan, vaan se tarvitsee siihen ympäristön hyväksynnän. Systeemin rajautuminen tapahtuu silloin, kun sisäinen ja ulkoinen määritys on tasapainossa. (Kast & Rosenzweig, 1972, s. 450.)

Karkeasti jaotellen systeemiajattelun mukaan systeemi voi olla avoin taikka suljettu. Systeemin avoimuudella tai sulkeutuneisuudella voi olla myös erilaisia asteita. Avoimessa systeemissä, systeemi ottaa ja luovuttaa energiaa ja materiaa vuorovaikutuksessa sisäisesti, sekä ympäristönsä kanssa. Suljettu systeemi vastavuoroisesti on luonnontieteen perspektiivistä tarkasteltuna systeemi, joka voi vaihtaa ympäristönsä kanssa energiaa, mutta ei materiaa. Termodynamiikka muun muassa määrittelee suljetun systeemin vielä tiukemmin. Sen tulkinnan mukaan systeemi ei voi olla vuorovaikutuksessa ympäristönsä kanssa ollenkaan, vaan on täysin eristetty ympäristöstään. (Kast & Rosenzweig, 1972, s. 450.)

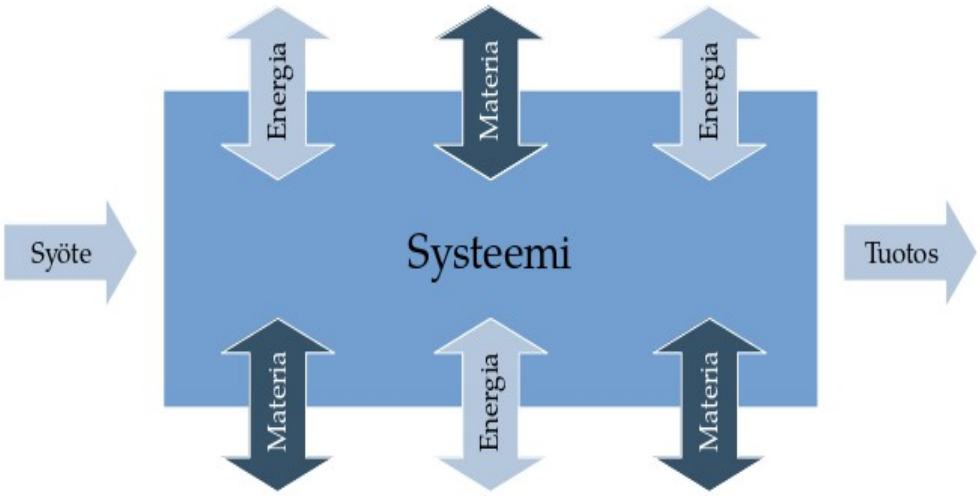
Systeemin eri avoimuuden tasoja on kuvattu alla olevassa kuviossa 1. Kuviossa oleva systeemi numero yksi (1) on täysin avoin systeemi. Se on vuorovaikutuksessa ympäristönsä kanssa ja vaihtaa sen kanssa aktiivisesti materiaa, sekä energiaa. Systeemi numero kaksi (2) on luonnontieteellisen (fysiikan) mallin mukainen osittain avoin systeemi. Siinä systeemissä oleva materia pysyy systeemin omistuksessa, mutta systeemi voi vaihtaa energiaa ympäristönsä kanssa. Kolmas (3) systeemi kuvaa termodynamiikan mukaista suljettua systeemimallia. Siinä systeemissä on energiaa ja materiaa, joka säilyy vain systeemin omassa käytössä. Systeemi ei ota, eikä luovuta mitään ympäristöönsä.



KUVIO 1: Systeemin eri avoimuuden tasot

Avoimella systeemillä on jatkuva pyrkimys systeemin sisäiseen tasapainoon, koheesioon. Systeemin sisäinen tasapaino on tila, jossa systeemi toimii sille oletetulla tavalla. Avoin systeemi koostuu osista (ainakin kaksi elementtiä muodostaa systeemin siten, että sille syntyy identiteetti), mutta se ei ole koskaan kokonaisuuksiensa summa. Sen osat voivat yksinään olla heikkoja tai vahvoja, mutta yhdessä ne muodostavat uniikin kokonaisuuden, jonka vahvuus voi olla suurempi yhdessä, kuin yhteenlaskettuna erillisinä osina. Sosiaalisia systeemejä, niiden sosiaalisten (vuorovaikutuksellisten) ulottuvuuksien vuoksi voidaan pitää lähtökohtaisesti avoimina. (Kast & Rosenzweig, 1972, s. 450-454.)

Kuviossa 2 on kuvattu miten avoin systeemi toimii. Se ottaa vastaan syötteitä (*input*) ympäristöstään, käsittelee saamansa syötteen niiden toimintamallien tai käytänteiden mukaisesti, joita systeemissä on ja tuottaa ympäristöönsä uusia tuotoksia (*output*). Avoimessa systeemissä sen alemmilla kerroksilla systeemin avoimuuden tai sulkeutuneisuuden aste voi vaihdella, riippuen siitä mikä tehtävä alasysteemillä on suhteessa systeemiin, missä se sijaitsee, sekä siihen ympäristöön, jossa se sijaitsee. Systeemi on kuitenkin kokonaisuudessaan edelleen avoin systeemi, vaikka sillä olisikin eriasteisesti avoimia alasysteemejä. Systeemi kokonaisuutena vaihtaa energiaa ja materiaa ympäristönsä kanssa, vaikka systeemin alasysteemit eivät näin välttämättä toimisikaan koko systeemin kesken. (Kast & Rosenzweig, 1972, s. 450-454.)



KUVIO 2: Avoimen systeemin toimintamalli

Systeemiteorian mukaan avoimella systeemillä on pyrkimys kohti erilaistamista ja kompleksisuutta. Systeemissä tapahtuva energian ja materian liike on omiaan muuttamaan systeemin koostumusta, mikä lisää kompleksisuutta systeemin sisällä. Avoin systeemi pyrkii siis kehittymään vuorovaikutuksessa ympäristön kanssa, kohti mutkikkaampaa muotoa. Samalla kun avoin systeemi kehittyy, lisääntyy systeemissä sen kompleksisuus. (Kast & Rosenzweig, 1972, s. 450; Schneider & Somers, 2006, s. 352.)

2.3 Kompleksisuus sosiaalisessa systeemissä

Systeemiteorian mukaan systeemi voi sisältää kompleksisuutta (*complexity*) tai systeemi voi olla monimutkainen (*complicated system*). Glouberman ja Zimmerman (2016) ovat esittäneet näiden käsitteiden välisiä eroja. Kompleksinen systeemi elää vuorovaikutuksessa muuttuvan ympäristönsä kanssa ja adaptoituu ympäristön vaatimusten ja systeemin oman päätöksenteon mukaan. Kompleksinen systeemi pitää sisällään jatkuvaa epävarmuutta, ennustamattomuutta, sekä ei-lineaarisuutta. Monimutkainen systeemi on taas järjestäytynyt, lineaarinen systeemi, jossa voi olla monimutkaisia rakenteita, mutta sen päätöksenteko ja toiminta on johdonmukaista. Monimutkainen systeemi ei ole adaptoituva, jolloin sen tulee sijaita staattisessa ympäristössä. (Glouberman & Zimmerman, 2016, s. 9-10.)

Kuten aiemmin on havaittu Luhmannin systeemiteoria pitää sisällään myös kompleksisuuden käsitteen. Luhmannin (2004) mukaan systeemin kompleksisuus lisääntyy sen suhteista systeemin osien kesken ja mahdollisuudesta muodostaa näitä suhteita. Luhmannin mukaan kompleksisuus syntyy suhteiden luonnin valinnanvapaudesta osien kesken. Systeemin osilla voi olla valittavana useampia vaihtoehtoisia suhteita, kuin se jonka ne lopulta päättävät valita. Osat eivät kuitenkaan muodosta suhteita sattumanvaraisesti, vaan tekevät valintoja perustuen systeemin sisäisiin malleihin. Valintojen ulkopuolelle jääviä suhteita Luhmann kuvaa toteutumattomina mahdollisuuksina. (Luhmann, 2004, s. 241.)

2.4 Kompleksinen sopeutuva systeemi

Kompleksinen adaptiivinen systeemi (*Complex Adaptive System*) on kokoelma erilaisia osia (toimijoita), jotka hierarkisella tavalla ovat (kommunikoimalla) yhteydessä toisiinsa. Systeemin osat vaihtavat informaatiota keskenään, mutta ovat myös yhteydessä ympäristöönsä, josta keräävät jatkuvalla prosessilla tietoa. Keräämänsä tiedon perusteella systeemi mukautuu siihen tilaan, jota kerätty tieto sille tuottaa. Eidelson (1997) kutsuu tällaista kompleksista systeemiä oppivaksi järjestelmäksi. Oppivan järjestelmän edellytyksenä on, että järjestelmä osaa jalostaa keräämänsä tiedon järjestelmän käyttöön, muuntautuakseen tiedon edellyttämään tilaan. (Eidelson, 1997, s. 43.)

Holland (2006) on määritellyt kompleksiselle adaptiiviselle systeemille neljä perustavanlaatuista ominaisuutta 1) rinnakkaisuus, 2) ehdollinen toiminta, 3) modulaarisuus ja 4) sopeutuminen ja evoluutio. Rinnakkaisuudella Holland kuvaa systeemin sisällä olevia useita yhtäaikaisia toimijoita, jotka viestivät yhtäaikaisesti lähettämällä ja vastaanottamalla signaaleja ympärilleen. Ehdollisuus perustuu sisäisten toimijoiden mahdollisuuteen toimia haluamallaan tavalla, vaikka ne olisivatkin riippuvaisia saamistaan signaaleista. Holland kuvaa systeemin ehdollisuus-ominaisuutta *IF/THEN* -toiminnolla. Siinä toimija ottaa vastaan sille lähetetyn signaalin. Se ei pakota toimijaa mihinkään toimintoon, vaan toimija tekee itse valinnan, millaisen toiminnon suorittaa tai jättää suorittamatta saamansa signaalin perusteella. Toiminnan ehdollisuus on yhteydessä toiminnan rinnakkaisuuteen siten, että *IF/THEN*-mallisia toimintoja voidaan tehdä yhtäaikaisesti. Modulaarisuudella tarkoitetaan systeemin toimijoiden sisäisiä sääntöjä ja toimintamalleja. Toimijoilla saattaa systeemin sisällä olla sisäisiä sääntöjä, jonka mukaan ne toimivat. Näitä sääntöjä yhdistelemällä toimijat rakentavat itselleen toimintamalleja, joiden mukaan toimia tietynlaisen signaalin saatuaan. Toimijoiden ei tällöin tarvitse joka kerta käsitellä jokaista saamaansa signaalia yksitellen, vaan ne voivat toimia ennalta opitulla tavalla. Neljäs ominaisuus

Hollandin mukaan on sopeutuminen ja evoluutio. Systeemin sisällä toimijat aika ajoin muuttuvat ja vaihtelevat. Yleensä toimijan muuttuminen johtuu systeemin kehittymisestä. Systeemin kehittyminen on sopeutumista uusiin tiloihin, joita sisäiset toimijat toimin-nallaan tuottavat. Systeemin toimijoiden muutokset eivät perustu satun-naisuuteen, vaan toimijoiden muutoksella systeemi pyrkii kehittämään ja tehos-tamaan toimintaansa. (Holland, 2006, s. 1-2.)

Systeemin sisäistä itseorganisoitumista pidetään myös kompleksisen systeemin ominaisuutena. Itseorganisoitumisella tarkoitetaan, että systeemi löytää itse järjestyksen, joka on systeemin itsensä kannalta tarkoituksenmukaisin. Systeemi on vuorovaikutuksessa ympäristönsä kanssa ja tämän vuorovaikutuksen seurauksena, ilman systeemin ohjausta, se löytää tarkoituksenmukaisimman järjestyksen tai muodon. (Smirnov, Kashevnik & Shilov, 2015, s. 168.)

2.5 Toimijaverkkoteoria

Tämän tutkimuksen yhteydessä on myös hyvä lyhyesti mainita toimijaverkkoteoria (*Actor Network Theory*) mahdollisena systeemimallina tutkimuksen systeemille. Vaikka tässä tutkimuksessa toimijaverkkoteoriaa ei ole valittu tutkittavan systeemin teoreettiseksi viitekehykseksi, on toimijaverkkoteorialla useita sellaisia ominaisuuksia, jotka vastaavat sellaista. Tämän luvun lopussa on myös perusteltu, miksi toimijaverkkoteoria on jätetty valitsematta tutkimuksen teorian pohjaksi.

Toimijaverkkoteoria on Latourin, Callonin ja Lawin 1980-luvun alussa kehittämä teoria, jossa kuvataan sosiaalisen ja luonnollisen maailman vuorovaikutusta keskenään. Latourin (2005) mukaan Latourin, Callonin ja Lawin teoria kuvaa verkoston osien (toimijoiden) yhdistelmiä ja vuorovaikutuksia ja niiden suhdetta verkoston toimintaan. Nimensä mukaisesti toimijaverkkoteoriassa tutkitaan verkostossa olevien toimijoiden vuorovaikutusta. (Latour, 2005, s. 22-24.)

Toimijaverkkoteoria on systemaattinen tapa tutkia systeemin infrastruktuuria. Toimijaverkkoteoria esitellään tässä tutkimuksessa sen vuoksi, että myös sillä voidaan myös tutkia turvallisuussysteemiä, systeemin toimijoiden näkökulmasta. Toimijaverkkoteorian ajatus lähtee siitä olettamuksesta, että maailma on rakennettu yhteen kietoutuneista verkoista, jotka ovat kompleksisella tavalla yhteydessä (vuorovaikutuksessa) toisiinsa. Teorian mukaan yhteydet eivät ole pysyviä, vaan ne muuttuvat koko ajan itsestään. Toimijaverkkoteoriassa yhteyksillä tarkoitetaan niin ihmisten ja laitteiden, kuin laitteiden ja laitteiden välisiä verkkoja. Toimijaverkkoteorialla voidaan myös

osuvasti kuvata kyber-maailman ja fyysisen maailman toimijoiden yhteyttä toisiinsa. (Carroll, Richardson & Whelan, 2012, s. 55.)

Toimijaverkkoteoriaa kuvataan teoriaksi, vaikka se ei sitä ole edes sen kehittäjänsä Latourin (2005) mielestä. Toimijaverkkoteoria ei vastaa tutkimuksessa kysymykseen *miksi*, vaan se kuvaa toimijoiden välisiä suhteita. Lisäksi sen avulla voidaan kuvata asioita, joita on olemassa vain abstraktilla tasolla, eikä niitä muutoin voitaisi kuvata, niin kauan kuin kuvattava kohde muodostuu verkoista. (Latour, 2005, s. 142-143.)

Belliger (2014) lähestyy toimijaverkkoteoriaa organisaation näkökulmasta ja siitä, miten toimijaverkkoteoria voi selittää organisaatiotasolla sen sisäistä toimintaa. Belliger kuvaa sitä menetelmälliseksi symmetriaksi ihmisten ja ei-inhimillisten välillä. Siinä organisaation koko ei ole osiensa summia, vaan kokonaissumma on aina pienempi kuin sen osien yhteenlaskettu summa. Tässä teoria mallissa toimija on aina verkko. Verkolla ei kuitenkaan tarkoiteta organisaatiota, vaan sitä kokonaisuutta, jossa organisaatio on olemassa. (Belliger 2014, 12-13.)

Kuvattaessa turvallisuusjärjestelmää kokonaisuutena, niin systeemiteoria, kuin toimijaverkkoteoria pystynevät esittämään kuvauksen järjestelmän mallista ja sen sisäisestä vuorovaikutuksesta. Tutkittaessa kokonaisuuden (eli järjestelmän) resilienssiä, tutkimus keskittyy tällöin kokonaisuuden tutkimiseen. Toimijaverkkoteorian avulla tutkimus kohdistuu nimenomaan järjestelmän sisäisiin toimijoihin ja verkostoon, kun taas systeemiteoria tarkastelee systeemin toimintaan kokonaisuutena. Systeemiteorian näkökulmasta yksittäisellä toimijalla on pienempi merkitys tutkimuksen kannalta, tutkittaessa tällaisen kokonaisuuden resilienssiä. Tämän vuoksi tässä tutkimuksessa teoreettiseksi viitekehykseksi on nimenomaisesti valittu systeemiteoria toimijaverkkoteorian sijaan.

3 TURVALLISUUSJÄRJESTELMÄ KYBER-FYYSISENÄ SOSIAALISENA SYSTEEMINÄ

3.1 Kyber ja fyysinen - rinnakkaiset maailmat

Informaation ja kommunikoinnin lisääntyminen teknologisen kehityksen myötä ovat synnyttäneet uuden ulottuvuuden, jota kutsutaan Kuusiston ja Kuusiston (2015) mukaan kybermaailmaksi. Kybermaailma ja fyysinen maailma voidaan ymmärtää osittain toisiinsa limittyvinä systeemin elementteinä. Fyysinen maailma on kaikki fyysisesti oleva, sisältäen siihen liittyvät ihmiset (sosiaalinen) ja fyysisen materian (fyysinen). Kybermaailma on ulottuvuus, joka pitää sisällään tietoverkot ja niihin liittyvät laitteet. Kybermaailma sisältää myös ihmisen läsnäolon ja osallistumisen tietoverkoissa. Osallistumisella tarkoitetaan sosiaalista kanssakäymistä ihmisten ja laitteiden kesken verkkoteknologian avustamana. Kybermaailma pitää sisällään tietokoneisiin, tietojärjestelmiin, tietoverkkoihin ja niiden väliseen kommunikaatioon liittyvät elementit. Kybermaailma on osa kyber-fyysisen sosiaalisen systeemin kokonaisuutta. (Kuusisto, T. & Kuusisto, R. 2015, s. 31-34.)

Kybermaailma (*Cyber World*) ja kyberympäristö (*Cyber Environment*) ovat termejä, jotka usein sekottuvat keskenään. Ne eivät ole synonyymejä toisilleen, vaikka niillä onkin hyvin toisiaan lähellä oleva määritelmä. ITU-T (*International Standardization Sector of International Telecommunication Union ITU*) määrittelee kyberympäristön seuraavalla tavalla: *se on ympäristö, joka sisältää käyttäjät, tietoverkot, laitteet, ohjelmistot, prosessit, informaation siirron tai varastoinnin, sovellukset, palvelut ja järjestelmät, jotka voidaan kytkeä suoraan tai epäsuorasti tietoverkkoihin*. Kyberympäristö on sen mukaan tila, jossa kybermaailma voi olla olemassa. (ITU-T 2008, s. 2.)

Kuviossa 3 on kuvattu Kuusiston ja Kuusiston (2015) mukaan tapahtumien ja niiden ilmentymien suhdetta kyber- ja fyysisen maailman välillä. Kybermaailman ja fyysisen maailman rajapinnat voidaan erotella alla olevan kuvion mukaisesti, fyysinen-fyysinen, fyysinen-kyber, kyber-kyber, kyber-fyysinen. Tällä tarkoitetaan sitä, että maailmojen välillä voi olla tapahtumia, joiden tapahtumapaikka on esimerkiksi fyysisessä maailmassa ja ilmentyminen

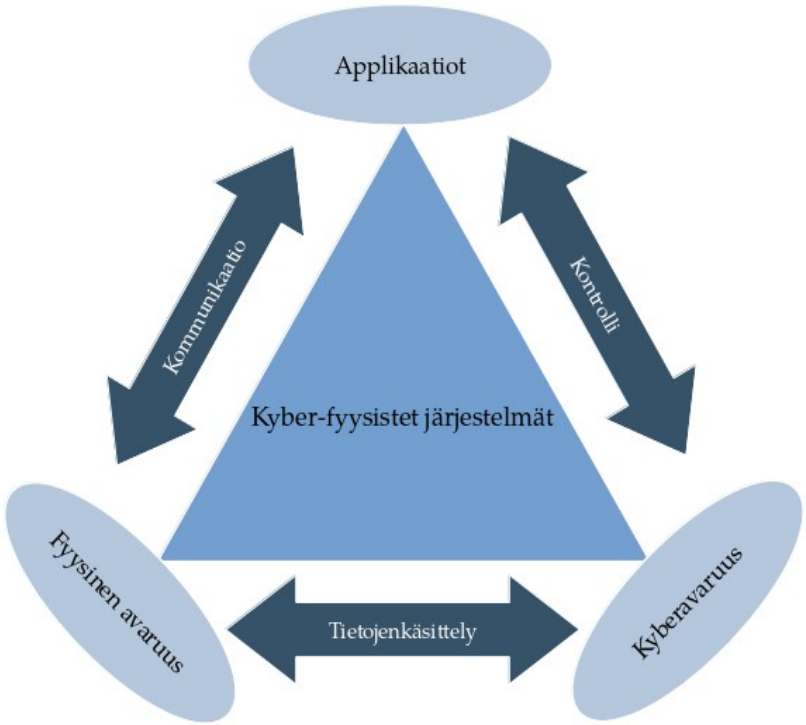
jommassa kummassa fyysisessä- ja/tai kybermaailmassa. Tällä tavoin havainnollistettuna voidaan huomata näiden kahden elementin suhde ja riippuvuus keskenään. Riippuvuutta Kuusisto ja Kuusisto (2015) kuvaavat kuviossa 3 olevin esimerkein. Fyysisessä maailmassa tapahtuva ja siellä ilmentyvä, voi olla esimerkiksi fyysinen taistelu miekoilla ja kilvin. Kun taas fyysisessä maailmassa katkaistaan tietoliikennekaapeli, ilmenee sen vaikutukset kybermaailmassa verkon toimimattomuutena. Haittaohjelman levitys tapahtuu kybermaailmassa, jossa myös sen seuraukset (ensisijaiset) ilmenevät. Tilannekuvan lähettäminen taistelukentältä tapahtuu kybermaailmassa, mutta se ilmenee fyysisessä maailmassa. Kompleksisuus, joka on sosiaalisen systeemiteorian keskeisimpiä käsitteitä on siten läsnä myös kybermaailmassa. Kuusisto ja Kuusisto (2015) kuvaavat kybermaailmaa kompleksisena adaptiivisena systeeminä.

KUVIO 3: Kyber- ja fyysisen maailman suhde

Kybermaailman kompleksisuus esiintyy sen sisällä tapahtuvassa toiminnassa, sen osien ja elementtien välillä. Toiminnat, joita kybermaailmassa suoritetaan, eivät ole ennustettavissa, eivätkä ole aina kenenkään hallinnassa. Järjestelmän toiminta tai sen toiminnan seurauksena syntyvät tuotokset eivät välttämättä ole ennustettavissa. Kyber-fyysisen systeemin perusajatuksena on ollut kuvata kybermaailman ja fyysisen maailman yhdistyminen ja keskinäinen

vuorovaikutus. Sillä tarkoitetaan vuorovaikutusta ja toimintoja, jotka tapahtuvat siinä systeemissä, jonka kumpikin näistä tekijöistä muodostaa. (Kuusisto T. & Kuusisto R., 2015, s. 34.)

Tällainen systeemi rakentuu kyber- ja fyysisestä tilasta (avaruudesta), sekä applikaatioista, jotka toimivat systeemin sisällä. Näillä kolmella ulottuvuudella on keskinäinen kontrolli, kommunikaatio ja tietojärjestelmiin liittyvä toiminta (tietojenkäsittely). Wang (2010) on kuvannut kyber-fyysisen järjestelmän sisäistä toimintaa ja vuorovaikutusta kuviossa 4.



KUVIO 4: Kyber-fyysisen järjestelmän havainnollistaminen ja toiminta National Science Foundationin mukaan

Kyber-fyysinen sosiaalinen systeemi lähtee ajatuksesta, että tällainen järjestelmä omaa myös vahvasti sen sosiaalisen ulottuvuuden. Tällöin kyber-fyysinen systeemi on tiiviissä integraatiossa ja yhteenliittymässä sosiaalisen ja inhimillisen ulottuvuuden kanssa, joka koordinoi systeemin toimintaa. Wang perustaa näkemyksensä Karl Popperin vuonna 1978 esittämään todellisuuden teoriaan, jossa todellisuutta tarkastellaan kolmen maailman (fyysinen, henkinen ja keinotekoinen) kautta. Wang (2010) on ottanut tähän teoriaan lisäksi kybermaailman, jota Popperin teoriaa kehitettäessä ei ollut vielä käytettävissä. Kybermaailma (kyberavaruus tai -ympäristö) käsitteenä kehittyi vasta internetin kehityksen jälkeen. Wangin mukaan nämä eri elementit ovat osa kompleksista

avaruutta ja muodostavat yhdessä kompleksisen systeemin. (Wang, 2010, s. 85-86.)

3.2 Kyber-fyysisen sosiaalisen systeemin tekninen rakenne

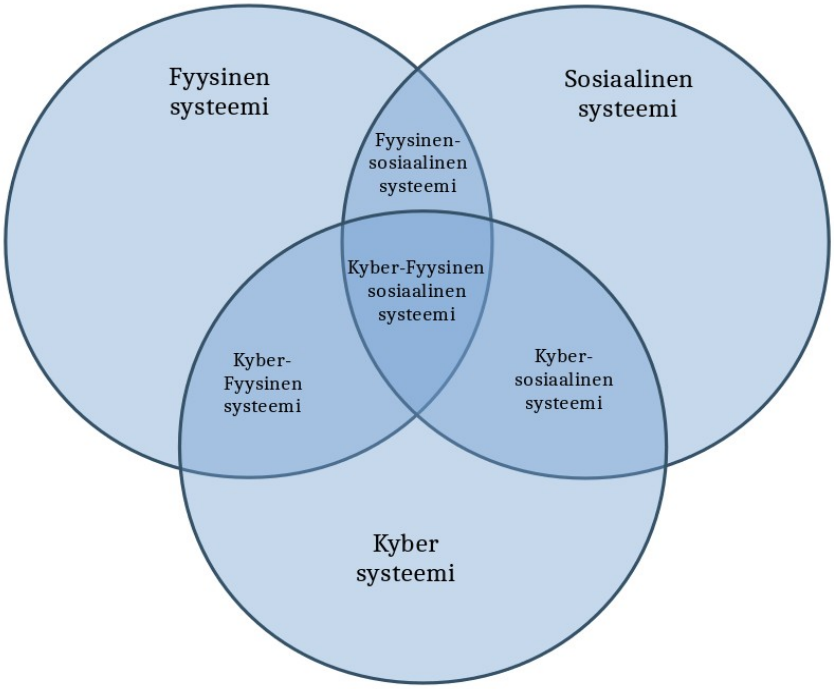
Systeemin kompleksisuutta voidaan hahmottaa myös systeemin teknisen toiminnan kautta. Kyber-fyysisellä systeemillä on tyypillisiä sitä kuvaavia ominaispiirteitä, joita yleisellä tasolla voidaan erottaa jokaisesta systeemistä (Xiong ym., 2015, s.321).

1. Systeemin fyysiset ja kyber -elementit toimivat läheisesti yhdessä tietojärjestelmien kautta. Tietojärjestelmät ovat sulautuneet osaksi kumpaakin elementtiä. Tietojärjestelmien kautta sulautuneilla elementeillä on yleensä rajoitettu kaistanleveys ja laskentateho.
2. Systeemillä on useita epäluotettavia yhteyksiä, kuten langalliset ja langattomat yhteydet. Yhteyksien epäluotettavuus tekee systeemin vuorovaikutuksesta arvaamatonta.
3. Korkea heterogeenisyyden taso. Toimijat systeemin sisällä ovat erilaisia.
4. Mobiililaitteet lisäävät kompleksisuutta. Yhteydet toisiin laitteisiin perustuvat yhteyksien ennalta arvaamattomuuteen. Yhteys toisiinsa niillä on vain silloin, kun tarvittavat mobiililaitteet ovat kantaman sisällä.
5. Ihmisen ja laitteen välinen yhteys. Näissä yhteyksissä esiintyvien epävarmuustekijöiden vuoksi systeemissä esiintyy epäluotettavuutta.
6. Johtuen epäluotettavista yhteyksistä systeemillä tulee olla yhteyksien ja verkkojen uudelleen konfigurointi mahdollisuus, jolla voidaan paikata niitä epäluotettavuustekijöitä, joita kompleksiset yhteydet systeemissä aiheuttavat. (Xiong ym., 2015, s. 321.)

Tekniseen tasoon lisättävä sosiaalinen ulottuvuus tekee systeemistä myös sosiaalisen systeemin. Laitteiden käyttö, konfigurointi ja implementointi vaativat systeemissä ihmisen läsnäoloa, ja se tekee systeemin toiminnasta riippuvaisen ihmisen läsnäolosta. Systeemin sosiaalista aspektia voidaan mahdollisesti tulevaisuudessa osittain korvata keinoälyllä, jolla koneiden välinen (M2M) kommunikointi lisääntyy. Keinoäly voi kaventaa inhimillisen osan määrää systeemissä, mutta se ei kuitenkaan kokonaan poista sitä. (Xiong ym., 2015, s. 321.)

Kuviossa 5 on kuvattu eri maailmojen limittyminen ja kyber-fyysisen systeemin perusta. Kuten aiemmin on todettu systeemin olemassaolo, sisältö ja laajuus määrittyvät siinä hetkessä ja paikassa, jossa systeemi on, myös näiden eri elementtien koko vaihtelee kyber-fyysisen systeemin sisällä. Xiongin mukaan elementtien rajapinnat kytkeytyvät toisiinsa eri metodein. Fyysinen- ja kybermaailma kytkeytyvät toisiinsa verkkojen ja sensoreiden välillä. Sosiaaliset

verkot yhdistävät kybermaailman ja sosiaalisen maailman toisiinsa. Fyysinen maailma on siis ympäristö, jossa sosiaalinen toiminta ja inhimillisen läsnäolo tapahtuvat. Näiden ekementtien sijaitseminen fyysisessä maailmassa yhdistää silloin nämä kaksi elementtiä. (Xiong ym., 2015, s. 323-324.)



KUVIO 5: Kyber-fyysisen sosiaalisen systeemin kuvaus

Liun, Yangin, Wenin ja Zhangin (2011) mukaan erityisesti hiearkiseen käskyvaltasuhteeseen perustuvissa kyber-fyysisissä sosiaalisissa systeemeissä, kuten sotilasorganisaatioissa on eroteltavissa neljä systeemin peruspilaria: fyysinen-, informaatio-, kognitiivinen- ja sosiaalinen ulottuvuus. Näillä peruspilareilla on merkitystä koko systeemin toiminnan kannalta, sekä sen johtamisen ja hallinnan näkökulmasta. Tässä tutkimuksessa juuri näiden peruspilarien varaan rakennetun systeemin toimintaa tullaan tarkastelemaan. Kyber-fyysinen sosiaalinen systeemi koostuu kyber- ja fyysisestä ulottuvuudesta (maailmasta), ihmisen tuottamasta tiedosta, henkisistä kyvyistä ja kulttuurisista elementeistä. Systeemissä esiintyy eri tasoja, joilla systeemi tuottaa toimintoja. Olennaista systeemille on, että systeemin osat toimivat vuorovaikutuksessa toistensa kanssa. (Liu, Yang, Wen & Zhang, 2011, s. 92-96.)

3.3 Päätöksenteko kyber-fyysisessä sosiaalisessa systeemissä

Tarkasteltaessa turvallisuusjärjestelmää, voidaan havaita sen pitävän sisällään paljon kompleksisuutta, sen sisältäessä useita edellä kuvattuha elementtejä, sekä niiden välisen kommunikaation. Järjestelmässä on useita toimijoita, joita ohjaa eri säännökset, ja useita irrallisia järjestelmiä sekä komentoketjuja, joilla ei ole suoraa yhteyttä toisiinsa. Silti järjestelmällä on yksi yhteinen tarkoitus, kokonaisturvallisuuden ylläpito ja sen kehittäminen. Se on toiminnaltaan avoin ja ottaa vastaan yhteiskunnan syötteitä ja palauttaa yhteiskuntaan oman tuotoksensa (turvallisuus). Systeemin avoimuus ja sen tahtotila kehittyä kohti kehittyneempää muotoa, ovat tekijöitä jotka lisäävät systeemin kompleksisuutta. Kompleksiivinen adaptiivinen systeemi toimii siten hyvänä viitekehyksenä turvallisuussysteemitutkimuksessa.

Turvallisuusorganisaatiota voidaan hyvin kuvata Schneiderin ja Somersin (2006) mukaan systeemiteorian ja avoimen systeemin kautta. Yleisesti organisaation rakenne sisältää näiden mallien ominaisuuksia. Turvallisuusorganisaatio on hierarkisesti johdettu ja sillä on useita eri toiminnan tasoja. Organisaatiolla on sisäiset ja ulkoiset rajat, jotka muodostavat sen fyysisen rakenteen. Turvalliuussorganisaatiolla on sille asetettu yhteiskunnallinen tehtävä, joka on lainsäädännöllä säädelty. Systeeminä organisaatio koostuu sen sisällä olevasta ihmisistä ja laitteista, joilla on riippuvuussuhde toisiinsa. Nämä ihmiset ovat vaikutuksessa toisiinsa omassa ympäristössään, jota säätelee sisäisen tasapainon periaate. Systeemi pyrkii tällöin sisäiseen koherenssiin. (Schneider & Somers, 2006, s. 352-353.)

Liu ym. (2011) ovat tutkineet militaristista järjestelmää, joka perustuu käskyvalta (*command and control*) suhteeseen, kyber-fyysisenä sosiaalisena systeeminä. Artikkelissaan he esittävät tällaiselle systeemille neljä peruspilaria, joista se koostuu ja joita voidaan pitää avaintekijöinä systeemin kannalta. Ensimmäisenä elementtinä on se tila tai avaruus, jossa systeemi on olemassa. Liun ym. mukaan sitä voidaan kuvata fyysisenä ja kyber-tilana. Toisena elementtinä on systeemin informaatio, inhimillinen tieto ja ymmärrys, jonka systeemiin liittyvät ihmiset siihen ovat keränneet. Kolmantena peruspilarina on kuvattu systeemin kognitiivista aspektia, eli systeemin henkisiä kykyjä. Neljäs peruspilari on systeemin sosiaalinen aspekti, eli systeemin sosiokulttuuriset ulottuvuudet ja elementit. (Liu ym., 2011, s. 92.)

Liun ym. (2011) mukaan teknologian kehityksellä ja sen soveltamisella käytäntöön on ollut suurta merkitystä käskyvalta organisaatioiden kehityksessä. Teknologisella kehityksellä organisaatioiden rakenteet ovat muuttuneet matalammiksi. Toisin sanoen johtaminen on tullut lähemmäksi toimintaa. Teknologinen kehitys on samalla mahdollistanut dynaamisemman informaation välittämisen ja monimutkaisemman vuorovaikutuksen organisaatiossa. Liu ym.

(2011) kuvaakin organisaatioiden muuttumista kohti orgaanisia kokonaisuuksia, jotka pitävät sisällään sensoreita, mahdollistajia, kommunikaatiota ja ihmisten välisiä sosiaalisia verkostoja. Edellä mainitut komponentit muodostavat kyber-fyysisen sosiaalisen systeemin, jossa nämä komponentit ovat läheisessä vuoro-vaikutuksessa keskenään, mahdollistavat informaation keräämisen systeemissä, tilannetietoisuuden, suunnittelun ja päätöksenteon ja toiminnan jatkuvana toimintana. Tekoälyä apuna käyttäen organisaatiolla on mahdollista muun-tautua haluamaansa tarkoitukseen sopivaksi. (Liu ym., 2011, s. 92-94.)

3.4 Kyber-fyysinen sosiaalinen turvallisuusjärjestelmä

Turvallisuussysteemin toiminta päätasolla perustuu sille annettuun tehtävään ja sitä säätelevään lainsäädäntöön. Kompleksisuusteorian avulla turvallisuussysteemin toimintaa voidaan tarkastella uudella tavalla, tutkimalla siinä esiintyviä ilmiöitä. Systeemiteorian avulla voidaan kuvata myös tutkit-tavan systeemin rakennetta. Tässä tutkimuksessa rakenteella ei tarkoiteta sen reaalimaailman mallia, vaan sen elementtien ja osien yhteenliittymää ja niiden vuorovaikutusta.

Tutkimuksen sisäisen turvallisuuden systeemiä ei tarkoituksellisesti ole nimetty, eikä sen yksilöiminen yksiselitteisesti edes onnistuisi. Kokonaisturvallisuutta tarkasteltaessa, jokaisella viranomaisella ja toimijalla on omat tehtävänsä. Tehtäväkentät ovat lainsäädännöllä jaettu eri virastojen tai laitosten vastuulle. Ideaalitilanteessa viranomaiset kuitenkin toimivat kohti yhteistä hyvää tai päämäärää, jolloin niiden vastuualueet voivat limittyä toistensa kanssa. Tämän vuoksi tässä tutkimuksessa kuvattu sisäisen turvallisuuden turvallisuussysteemi voi pitää sisällään useampia eri viranomaisia, virastoja ja toimijoita. Systeemiteorian mukaan systeemin koko, elementit ja sen ominaisuudet määrittyvät aina siinä hetkessä, jossa sitä tarkastellaan, jolloin sen sisältökin voi vaihdella.

4 KYBER-FYYSISEN SOSIAALISEN SYSTEEMIN RESILIENSSI

4.1 Resilienssin määritelmä

Verkkosanakirja Merriam-Webster Online Dictionary määrittelee termin resilienssi: *"kyvyksi palautua tai sopeutua helposti vastoinkäymiseen tai muuttua"*. Resilienssi on siis varautumista tulevaan, sekä toimia joita tapahtuu jonkin toisen tapahtuman jälkeen. Eri tieteenaloilla resilienssillä on useampia toisistaan hieman poik-keavia merkityksiä. Esimerkiksi insinööritieteissä resilienssillä voidaan kuvata esimerkiksi materiaalin joustavuutta tai sen elastisuutta. Humanistisissa tieteissä resilienssillä voidaan kuvata ihmisen henkistä sietokykyä ja kykyä selviytyä stressin alla. Yhteistä näille määritelmille kuitenkin on, että sillä mitataan jotakin sietokykyä. (Tierney, 2014, s. 163.)

Systeemiajattelussa resilienssillä kuvataan systeemin muodon muutosta edellisestä muodosta uuteen ja toimintoja systeemin sisällä. Muodonmuutos voi olla sisä- tai ulkosyntyistä, mutta se ei tapahdu systeemin omasta vapaasta tahdosta, vaan siitä syystä, että joku tekijä pakottaa systeemin muuttumaan. Hyvönen ja Juntunen (2016) ovat kuvanneet julkaisussaan resilienssin merkitystä turvallisuustutkimukselle. Heidän mukaansa resilienssillä systeemiajattelussa voidaan kuvata systeemin sisäisten muutosten prosessia. Sen avulla voidaan tarkastella systeemin itseorganisoitumisen astetta, sekä sitä millainen valmius systeemillä on muuttua ja oppia. Systeemin resilienssitutkimus eroaa oleellisesti insinööritieteiden tutkimuksessa. Siinä missä insinööritieteissä keskitytään lujuuden ja sitkeyden tutkimukseen, systeemitutkimuksessa tutkimuskohdetta lähestytään sen kimmoisuuden ja sopeutuvuuden kautta. Kyse on siis sopeutumisen tutkimisesta. (Hyvönen & Juntunen, 2016, s. 208.)

Longstaffin, Armstrongin, Perrinin, Parkerin ja Hidekin (2010) mukaan systeemin sopeutumisella ei tarkoiteta, että systeemi palaisi aina tarkalleen saman näköisenä toimintaan. Heidän mukaansa systeemin palautuminen tarkoittaa yksilöllisten toimintojen (sisäisten) palautumista takaisin systeemin käyttöön, mutta resilienssin kehittymisen (sopeutuminen uuteen tilaan) vuoksi

systeemi saattaa näyttää kriisin jälkeen muodollisesti erilaiselta. Tällöin systeemissä tapahtuu kehitystä, jonka tavoitteena on viedä systeemiä yhä resilientimpään suuntaan. (Longstaff, Armstrong, Perrin, Parker & Hidek, 2010, s. 4.)

4.2 Resilienssin yhteiskunnallinen ulottuvuus

Hyvösen ja Juvosen (2016) mukaan yhteiskuntaan kohdistuvat uhat pitävät sisällään tietynlaisen paradoksaalisuuden. Samalla kun kriisit uhkaavat yhteiskunnan toimivuutta, voivat ne olla mahdollisuus uudistaa yhteiskuntaa resilientimpään suuntaan. Yhtäältä yhteiskunnalla on siten systeeminä mahdollisuus kehittää toimintojaan kestämään paremmin kriisejä, sietämään niitä ja palautumaan niistä. Toisaalta sosiaalisella tasolla se kehittää varautumista luomalla ihmisille kuvaa turvallisuusympäristöön liittyvästä pysyvästä epävarmuuden tilasta. Turvallisuus syntyy ja kehittyy turvattomuuden tilan kehittämisen kautta. (Hyvönen ym., 2016, s. 216-217.)

Systeemin resilienssin kehittäminen on sen jatkuvuuden ja toimivuuden kannalta erittäin merkityksellistä yhteiskunnallisesta näkökulmasta. Longstaffin ym. (2010) mukaan esimerkiksi nykyaikaiset elintarvikkeiden- ja vedenjakelujärjestelmät ovat hyviä esimerkkejä kompleksisista systeemeistä. Ne ovat pitkälle automatisoituja, laajuudeltaan suuria ja koostuvat useista hajautetuista yksiköistä. Longstaffin ym. mukaan yhteiskunta rakentuu yhä kasvavassa määrin kompleksisista systeemeistä, joihin ihmisellä on yhä vähenevässä määrin kontrollin mahdollisuutta. Yleensä nämä kompleksiset systeemit huolehtivat yhteiskunnan toimivuudesta, ja samalla yhteiskunta muuttuu yhä riippuvaisemmaksi näistä systeemeistä. Longstaffin ym. mukaan kompleksisuus voi olla myös resilienssiä, sillä kompleksisiin systeemeihin on suunniteltu sisäisesti resilienssiä, koska ne sisältävät eri asteista diversiteettiä. Diversiteetti toimii samalla järjestelmän suojakeinona. Toisaalta tämä diversiteetti ei kuitenkaan itsessään tee systeemistä resilienttiä. (Longstaff ym., 2010, s. 1-2.)

4.3 Resilienssin piirteet

Tierney (2014) määrittelee resilienssille neljä merkittävää piirrettä (lujatekoisuus, päällekkäisyys, älykkyys ja nopeus), joilla systeemin resilienssiä operatiivisella tasolla voidaan mitata. Näistä kahta ensimmäistä Tierney (2014) pitää systeemin sisäsyntyistä resilienssiä kuvaavina piirteinä. Niillä voidaan kuvata systeemin kyvykkyyttä, eli sen selviytymiskykyä ja sietokykyä. Näiden piirteiden avulla voidaan arvioida systeemin sisäisiä mekanismeja; varautumiskykyä, kestävyyttä ja vahvuutta. Hyvösen ja Juvosen (2016) mukaan

kaksi ensimmäistä piirrettä edustavat systeemin luontaista ja sisäsyntyistä resilienssiä. Heidän mukaansa nämä piirteet valmistavat systeemiä vastustamaan kriisejä. Kaksi jälkimmäistä piirrettä kuvaavat Tierneyn (2014) mukaan systeemin resilienssiä kriisissä, eli systeemin kykyä toimia ja aktivoida toimintojaan systeemin sisällä uuteen tilaan sopeutuakseen. (Tierney, 2014, s. 168; Hyvönen ja Juvonen, 2016, s. 213.)

Lujatekoisuus. Ensimmäisenä piirteenä Tierneyn (2014) mukaan on lujatekoisuus (*robustness*), jota on kuvattu kykynä sietää negatiivisia seurauksia. Tierneyn mukaan kestävyys (kyky voimallisesti vastustaa) on resilienssin avaintekijä. Simmons ja Yoder (2013) lähestyvät samaa ominaisuutta psykologisesta näkökulmasta, tutkimuksessaan resilienssistä sotilailla, sen kovuuden (*hardiness*) kautta. Heidän mukaansa kovuudella tarkoitetaan kykyä sietää negatiivisia kokemuksia, henkisten kykyjen avulla. Näitä ovat sitoutuminen, kontrolli ja haastaminen. Vaikka Simmons ja Yoder (2013) kuvaavat ominaisuuksia yksilön ominaisuuksina, voidaan niitä perustellusti pitää myös sosiaalisen systeemin ominaisuutena eli henkisenä pääomana. Hyvösen ja Juvosen (2016) mukaan kestävyys on systeemin luontainen ja sisäsyntyinen ominaisuus, joka syntyy systeemin omista lähtökohdista. Kestävyys on Hyvösen ja Juvosen (2016) mukaan osa systeemin varautumisajattelua, jolla tavoitellaan systeemin identiteetin säilyttämistä. (Tierney, 2014, s. Xx; Simmons & Yoder, 2013, s. 20; Hyvönen & Juvonen, 2016, s. 213.)

Päällekkäisyys. Toisena tärkeänä resilienssin piirteenä Tierney (2014) pitää päällekkäisyyttä (*redundancy*). Päällekkäisyydellä Tierneyn mukaan tarkoitetaan niitä päällekkäisiä toimintoja, joita systeemi kykenee pitämään yllä säilyttääkseen toiminnallisuutensa. Tierneyn mukaan päällekkäisyydellä voidaan kuvata sitä systeemin toiminta-astetta, joka sillä on systeemiin kohdistuneesta iskusta huolimatta. Päällekkäisyyttä systeemissä on mahdollista kehittää lisäämällä systeemin diversiteettiä. Diversiteetin avulla systeemin toimintoja voidaan hajauttaa, joka samalla lisää päällekkäisyyttä ja useamman toiminnan mahdollisuutta. Hyvösen ja Juvosen (2016) mukaan systeemin menestyksen ehtona on sen kyky tehdä vaihtoehtoisia päätöksiä ja toimia vaihtoehtoisin tavoin toimintakyvyn ylläpitämiseksi. Ollakseen resilientti, systeemillä tulee olla suunniteltuja varajärjestelmiä käytettäväksi, ensisijaisten järjestelmien kaatuessa tai vaurioituessa. (Tierney, 2014, s. Xx; Hyvönen & Juvonen, 2016, s. 213.)

Giezen, Salet ja Bertolini (2015) lähestyvät tutkimuksessaan redundanssia päätöksentekoprosessin näkökulmasta. Redundanssi, Giezenin ym. (2015) mukaan, mahdollistaa tietoon perustuvan päätöksentekoprosessin (ts. tietojohtaminen), joka hyödyttää systeemiä ja lisää sen resilienssiä. Giezenin ym. (2015) mukaan redundanssin kehittämisellä systeemin tietämys lisääntyy ja se mahdollistaa entistä tehokkaamman ja moniulotteisemman päätöksen-

tekoprosessin. Redundanssilla siis luodaan vaihtoehtoisia toimintoja niiden tilalle, jotka kaatuvat tai eivät ole tehokkaita. (Giezen, Salet, & Bertolini, 2015, s. 171.)

Älykkyys. Systeemin resilienssin kannalta kolmantena merkittävänä piirteenä Tierney (2014) pitää systeemin älykkyyttä (Hyvösen ja Juvosen (2016) käännös termistä *resourcefulness*). Tierney (2014) kuvaa älykkyyttä systeemin kekseliäisyydeksi (*resourcefulness*). Sillä Tierney (2014) kuvaa systeemin kykyä tunnistaa ongelmia ja käyttää hyväksi systeemin omia resursseja niiden ratkaisemiseksi. Termillä Tierney (2014) tarkoittaa systeemin kykyä hyödyntää sisäisiä prosesseja ja kapasiteettia vahingon torjumiseen. Älykkyydellä tarkoitetaan myös kykyä palauttaa käyttöön niitä resursseja, jotka ovat kriisissä vahingoittuneet tai osoittautuneet tehottomiksi. Älykkyys on siten systeemin kykyä soveltaa ja oppia hyödyntämään käytössään olevia resursseja muuttuvilla tavoilla. (Tierney, 2014, s. 168; 170; Hyvönen & Juvonen, 2016, s. 213.)

Hyvönen ja Juvonen (2016) pitävät älykkyyttä systeemin kykynä luoda kulttuurisia tietovarantoja. Kulttuuriset tietovarannot mahdollistavat Hyvösen ja Juvosen mukaan kriisiaikana systeemin nokkeluuden, kyvyn kehittää uusia toimintamalleja ketterästi. Kulttuuriset tietovarannot ovat kaikkia niitä kerättyjä toimintamalleja, kulttuurisia ja henkisiä ominaisuuksia, joita systeemi on toimiessaan hankkinut itselleen. (Hyvönen ja Juvonen, 2016, s. 213.)

Nopeus. Neljäntenä piirteenä Tierney (2014) kuvailee systeemin kyvykkyyttä nopeisiin ratkaisuihin. Nopeudella, eli ajalla, on merkitystä palautumisen kannalla. Tierneyn (2014) mukaan ajassa mitataan kaikki ne inhimilliset ja aineelliset tappiot, joita systeemi kärsii iskussa. Mitä lyhyemmäksi iskusta palautumiseen käytettävä aika jää, sitä pienemmät ovat systeemin kokemat tappiot. Mitä lujatekoisempi, redundantimpi ja älykkäämpi systeemi on, sitä suurempi on myös systeemin kriisistä toipumisen nopeus, mikäli systeemi osaa hyödyntää näitä ominaisuuksiaan. (Tierney, 2014, s. 171.)

Hyvönen ja Juvonen kuvaavat systeemin nopeutta ominaisuutena kyvyksi nopeaan itseorganisoitumiseen. Heidän mukaansa itseorganisoituminen on systeemin (tai yhteisön) kyky reflektoida omaa toimintaansa kriisitilanteessa ja organisoitua ilman keskusjohtoista toimintaa, käyttäen hyväksi kollektiivista tietämystä, jota systeemissä on. Hyvösen ja Juvosen (2016) näkemys itseorganisoitumiseen perustuu Tierneyn malliin systeemin nopeuteen vaikuttavista ominaisuuksista (lujatekoisuus, redundanssi ja älykkyys), joiden perusteella itseorganisoitumisen taso jatkuvasti kehittyy. Se on kyky korjata tai jälleenrakentaa nopeasti. Tierneyn (2014) mukaan tähän nopeaan jälleenrakentamiseen liittyy myös problematiikkaa. Mahdollisimman nopean palautumisen aikaan saamiseksi systeemin punnittavaksi tulee, jälleenrakennetaanko vauriot mahdollisimman nopeasti, vai tulisiko rakenteita uudistaa entistä paremmiksi. Entistä paremmin rakentaminen ei luonnollisesti ole yhtä nopeaa,

kuin jälleenrakentaminen. Nopeaa palautumista tällöin tukisi mahdollisimman nopea jälleenrakentaminen. Toisaalta silloin saatettaisiin menettää niitä asioita, joiden avulla systeemistä voitaisiin rakentaa entistä parempi. (Ståhle & Kuosa, 2009, s. 14-15; Tierney, 2014, s. 170; Hyvönen & Juvonen, 2016, s. 213.)

4.4 Diversiteetti resilienssin ominaisuutena

Longstaffin ym. (2010) mukaan systeemin kompleksisuus sisältää aina diversiteettiä. Diversiteetillä kuvataan Longstaffin ym. (2010) mukaan sitä lukumäärää erilaisia mahdollisia resursseja ja toimintoja, joita systeemillä on varattuna kriittisiä toimintoa varten. Eli mitä enemmän systeemillä on erilaisia resursseja tietyn kriittisen toiminnon suorittamiseen, sitä suuremmaksi systeemin diversiteetti kasvaa. Diversiteettiä voi kuvastaa esimerkiksi samaan toimintoon tarkoitetut laitteet, tai ihmiset, joilla on eri taustoistaan johtuvaa erilaista tietämystä tai kykyä toiminnon suorittamiseksi. Walkerin ja Saltin (2010) mukaan diversiteetti lisää systeemin joustavuutta ja kykyä käyttää sen omistamia ominaisuuksia älykkäällä tavalla. Diversiteetillä voidaan kuvata systeemin erilaisia varajärjestelmien toimivuutta. Esimerkiksi toimintojen kahdentaminen kahdella eri tavalla lisää diversiteettiä enemmän, kuin kahdentaminen toiminnot samalla tavoin. (Longstaff ym., 2010, s. 6; Walker & Salt, 2010, 121.)

4.5 Sosiaalinen resilienssi systeemissä

Systeemin häiriöttömän toiminnan ja jatkuvuuden kannalta on tärkeää, että sillä on useita erilaisia ominaisuuksia ja se pystyy käyttämään näitä ominaisuuksia yhtäaikaa joustavasti ja älykkäästi. Kyber-fyysisen sosiaalisen systeemin resilienssi syntyy sen elementtien ominaisuuksista ja niiden kyvystä toimia yhteistyössä. Sosiaalisen systeemin merkityksellisenä tekijänä pidetään sen inhimillistä ominaisuutta. Tämän vuoksi on perusteltua lyhyesti esitellä inhimilliseen resilienssiin liittyviä piirteitä.

Inhimillinen resilienssi on henkistä ja fyysistä kykyä sietää kriisiä ja kykyä selviytyä sellaisesta. Simmons ja Yodler (2013) ovat julkaisussaan määritelleet inhimillisen resilienssin tekijöitä. Simmonsin ym. (2013) julkaisu keskittyy sotilaalliseen inhimilliseen resilienssiin, mutta on varsin vertailukelpoinen tekijöiden suhteen yleisesti inhimillisestä resilienssistä puhuttaessa. Sotilaan inhimillisellä resilienssillä pyrkimyksenä on torjua posttraumaattisia stressioireita ja luoda kykyä jatkaa toimintaansa. Sotilaillakin esiintyy oireita, joita kenellä tahansa ihmisellä esiintyy kriisin aikana ja sen jälkeen. Sotilaiden resilienssin sietokykyä tutkitaan taisteluolosuhteissa, sillä niissä olosuhteissa sotilaiden tulee mahdollisimman pitkään kyetä toimimaan. Simmonsin ym.

määritelmän (2013) mukaan inhimillinen resilienssi koostuu sopeutuvasta elämänhallinnasta, henkilökohtaisesta kontrollista, henkilön lujuudesta, sekä sosiaalisesta tuesta. (Simmons & Yodler, 2013, s. 18, 20.)

Sopeutuva elämänhallinta. Simmonsin ym. (2013) mukaan sopeutuvalla elämänhallinnalla tarkoitetaan kykyä vastustaa ja sopeutua muutoksiin. Sillä ei välttämättä tarkoiteta kykyä sietää negatiivisia kokemuksia, vaan enemmän kyseessä on kyky sopeutua muutokseen, hyväksyä muutos, oppia siitä ja jatkaa toimintaa entistä vahvempana. Siihen kuuluu kyky mukautua ja mukauttaa (säätää) omaa toimintaansa siten, että se sopii muutokseen. (Simmons & Yodler, 2013, s. 20.)

Henkilökohtainen kontrolli. Simmonsin ym. (2013) mukaan henkilökohtaisella kontrollilla tarkoitetaan henkilön kykyä hallita itseään ja kykyä johtaa itseään, sekä vaikuttaa omaan elämäänsä. Usko omaan elämään tutkimusten mukaan vähentää henkilön epävarmuutta tulevaisuuttaan kohtaan. (Simmons & Yodler, 2013, s. 20.)

Lujuus. Simmonsin ym. (2013) mukaan lujuudella tarkoitaan inhimillistä kykyä kestää ja sietää stressiä ja kriisiolosuhteita. Lujuus koostuu henkilön yksilöllisistä ominaisuuksista, kuten sitoutumisesta, kontrollista ja kyvystä vastata haasteisiin ja ylittää niitä. Mitä suurempi henkilön lujuus on, sitä suurempia haasteita henkilö kykenee selvittämään. (Simmons & Yodler, 2013, s. 20.)

Sosiaalinen tuki. Sosiaalinen tuki Simmonsin ym. (2013) mukaan, on kyky tukea avun tarvitsijaa. Sosiaalinen tuki koostuu ihmisten verkostosta, joka tukee toinen toistaan ja auttaa joukon heikointa pysymään mukana. Tästä voidaan heidän mukaansa käyttää myös termiä empatia. Sosiaalinen tuki on ihmisten välistä aktiivista toimintaa, joka perustuu jo olemassa oleviin verkostoihin tai uusien verkostojen syntymiseen. (Simmons & Yodler, 2013, s. 20.)

5 YHTEENVETO

5.1 Systeemiajattelu turvallisuusjärjestelmän kuvaajana

Systeemiajattelu on mallintamista siitä, miten systeemiä voidaan kuvata. Sen avulla voidaan hahmottaa systeemin sisäisiä tapahtumia, sekä niiden vaikutusta koko systeemiin ja sen toimintaan. Kuten on jo aiemmin todettu, sosiaalinen systeemi syntyy siinä hetkessä, kun sille syntyy luontainen tarve olla olemassa ja pitää sisällään siinä hetkessä mukana olevat elementit. Tämän vuoksi onkin mahdotonta sanoa, että systeemi koostuisi koko ajan tietyistä tai samoista elementeistä. Voidaankin sanoa, että systeemi omistaa eri elementtejä eri hetkinä, sen sisäisen tarpeen mukaan. Systeemi määrittää itsenäisesti sisäisen tarpeen mukaan sen, mitkä elementit kulloinkin se omistaa. Systeemiajattelun tarkoitus on siis mallintaa olemassa olevia rakenteita, ei rakentaa niitä.

5.2 Resilienssi kyber-fyysisessä sosiaalisessa systeemissä

Tarkastellessa avoimen, kompleksisen ja adaptiivisen systeemin ominaisuuksia voidaan huomata, että tärkeimmät ominaisuudet systeemin resilienssin kannalta ovat sen lujuus, sopeutuvuus ja kyky muuttua. Ollakseen mahdollisimman resilientti systeemi, tulisi sen olla adaptiivinen, kyvykäs muuntautumaan (varajärjestelmät, vaihtoehtoiset tavat toimia), sosiaalisesti älykäs (tietovarannot), sekä omistaa kulttuurista pääomaa. Resilienssin kannalta merkityksellistä on, että systeemi kykenee käyttämään näitä ominaisuuksia oikein, tekemällä oikeita havaintoja ja päätöksiä, sekä oppimalla niistä virheistä, joita se tekee.

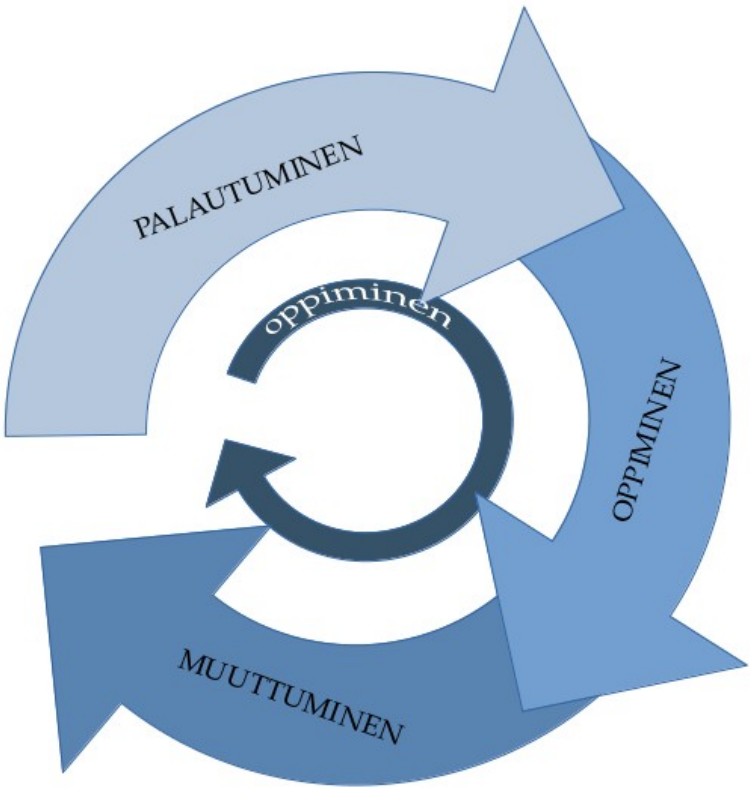
Tässä systeemin resilienssitutkimuksessa fokus on vaikutusten ja toiminnan jatkumisen tutkimisessa. Tutkimuksessa keskitytään kokonaisuuden tutkimiseen, vaikka systeemi useammasta elementistä koostuukin. Se, että systeemiin kohdistuvassa iskussa tms. sen sisällä olevat elementit (alasysteemit yms.) saattavat kokea hyvinkin merkittäviä muutoksia, eivät ne välttämättä koko systeemin mittakaavassa aiheuta merkittävää haittaa, eivätkä systeemitasolla näin ollen ole relevantteja tutkia. Tutkimuksen kannalta merkit-

tävää onkin, miten systeemi osaa kokonaisuutena sopeutua, muuttua ja oppia siitä, mitä se kohtaa. Toiminnan kannalta tärkeintä on kuitenkin päätöksenteko ja priorisointi. Se miten nopea päätöksentekokyky ja -ketju systeemillä on, ratkaisee sen miten paljon systeemin tarvitsee muuttua ja kuinka nopeasti se kykenee muutoksen vaatimaan päätöksentekoon. Kyber- fyysisessä sosiaalisessa systeemissä se tarkoittaa myös kykyä sovittaa yhteen eri maailmoiden vaatimukset ja niiden asettamat rajoitteet.

Kuviossa 6 on kuvattu systeemin resilienssiä esimerkki systeemin kautta. Kuviossa systeemi on kuvattu jossain satunnaisessa tilassa ja koostumuksessa. Kuviossa on havainnollistettu systeemiin kohdistuva ulkopuolinen vaikutus (kriisi tai häiriö), joka pakottaa systeemin muutokseen. Huomion arvoista on, että systeemi elää koko ajan jatkuvassa muutoksessa, mutta ulkopuolinen vaikutin saa aikaan systeemissä sellaisen muutoksen, joka ei ole sille luonnollinen.

Jo kriisin aikana ja sen jälkeen alkaa systeemin palautumisprosessi (1), jossa se pyrkii suojaamaan vielä toimivia järjestelmiä, sekä korjaamaan niitä vioittuneita resursseja ja prosesseja, jotka ylläpitävät sen ydintoimintoja. Se edellyttää systeemiltä älykkyyttä käyttää edelleen toimivia ja olemassa olevia resursseja oikealla tavalla, sekä nopeutta toimintojen mahdollisimman nopeaan palautumiseen. Koska systeemi ei välttämättä palaudu saman muotoiseen tilaan, jossa se ennen kriisiä oli, tulee systeemin sopeutua (2) tähän uuteen tilaansa ja muotoonsa. Systeemille on tärkeintä säilyttää sen toiminnan kannalta elintärkeät resurssit ja prosessit, ei muotoa. Systeemin sopeuduttua uuteen tilaansa ja palautettua elintärkeät toimintonsa, jatkuu systeemissä kehitystyö muuttamalla (3) systeemiä yhä resilientimpään suuntaan, oppimalla siitä mitä se on kokenut ja kehittämällä suojaustaan vastaisuuden varalle ja luomalla näiden pohjalta jotain uutta. Muuttuminen on osa oppimista ja varautumista.

Resilienssin on siis vastustuskykyä, sopeutumista, oppimista ja toiminnan jatkuvuutta. Kuvion sisemmällä kehällä kuvataan sitä jatkuvaa oppimisprosessia, joka systeemin sisällä alkaa muutoksen aikana ja jatkuu koko ajan sen jälkeen. Tässä vaiheessa oikein toimiva systeemi muuttaa toimintaansa siten, että jatkossa se olisi varautunut sellaiseen pakottavaan muutokseen, josta se nyt yrittää toipua. Oppimisesta ja sen soveltamisesta käytäntöön syntyy entistä resilientimpi systeemi. Resilienssi ei ole siis paluuta ”vanhaan toimivaan” vaan se on muutos uuteen toimivaan, entistä vahvempaan muotoon.



KUVIO 6: Systeemin resilienssin kehitysprosessi.

Resilientti systeemi sisältää preventiivisiä sekä defensiivisiä ominaisuuksia. Lujatekoisuuden ja redundanssin avulla voidaan kehittää systeemin preventiivistä kykyä torjua kriisejä. Preventiiviset toimet eivät estä systeemiin kohdistuvaa kriisiä, mutta yhdessä ne ja systeemin defensiiviset ominaisuudet, älykkyys ja nopeus, mahdollistavat systeemille mahdollisimman pienet vauriot ja toisaalta kyvyn toiminnan jatkuvuudelle mahdollisimman nopeasti. Näiden ominaisuuksien lisäksi systeemin tulee sisältää diversiteettiä, jonka avulla voidaan varmistaa edellä mainittujen ominaisuuksien monipuolinen toimintamahdollisuus. Resilienssi koostuu systeemin luontaisista ominaisuuksista, sekä ominaisuuksista, joita systeemillä on kyky kehittää. Tämä syntyy yhteistyössä systeemin elementtien kesken. Jokainen systeemin osa tuottaa sille oman kontribuutionsa, josta syntyy systeemin resilienssi.

6 METODOLOGIA

6.1 Tutkimusmenetelmä

Tutkimuksen teoreettisen viitekehyksen tarkoituksena oli muodostaa kuva kyber-fyysisestä sosiaalisesta systeemistä, sekä siitä mitä resilienssillä tällaisessa systeemissä tarkoitetaan. Systeemiä tarkasteltiin tässä kokonaisuutena ja todellisuutta vastaavana rakenteena. Teoreettisessa viitekehyksessä etsittiin vastausta siihen millainen on kyber-fyysinen systeemi eli laadullista kuvausta systeemistä. Tutkimukseni empiirisessä osuudessa käytetään hyväksi jo aiemmin luotua teoreettista sosiaalisen systeemin mallia. Tutkimusmenetelmänä käytetään skenaarioanalyysiä, jonka avulla tutkitaan tällaiseen systeemiin kohdistuvan ulkopuolisen monivaikutteisen iskun vaikutusta systeemin resilienssiin. Skenaarioanalyysiä käyttämällä luodaan systeemille vaihtoehtoisia tulevaisuuden kuvauksia. Empiirisen tutkmuksen toisena menetelmänä on asiantuntijahaastattelu. Sen tarkoituksena on koetella skenaarioanalyysin tuloksia.

Tutkimus on laadullinen, koska tutkimuksessani etsitään vastausta kysymykseen millainen. Tähän kysymykseen etsitään laadullista, ei määrällistä vastausta. Tutkimukseni tarkoituksena on tutkia kyber-fyysistä systeemiä kokonaisuutena, johon laadullinen tutkimusmenetelmä on sopiva, sillä laadullisessa tutkimuksessa aineistoa tarkastellaan Alasuutarin (2012) mukaan kokonaisuutena ja sillä voidaan kuvata jonkin loogisen kokonaisuuden rakennetta. Myös Hirsjärven, Remeksen ja Sajavaaran (2011) mukaan laadullisen tutkimuksen tarkoituksena on tutkia kohdetta kokonaisvaltaisesti ja kuvata todellista elämää. Laadullisessa tutkimuksessa on myös tavanomaista, että siinä sovelletaan muuttuja-ajattelua, kuten tässä tutkimuksessa on tehty. (Hirsjärvi, Remes & Sajavaara, 2011, s. 161; Alasuutari, 2012, s. 27, 31-32.)

Yinin (2015) mukaan laadullinen tutkimus sopii erinomaisesti jonkin instituution toiminnan ja reaktioiden, sekä sosiaalisten suhteiden tutkimiseen. Tässä tutkimuksessa on pyritty havainnollistamaan kokonaisuuden toimintaa ja kokonaisuuden resilienssiä sen eri elementtien (kyber, fyysinen ja sosiaalinen)

kautta. Tutkimuksessa on keskitytty nimenomaan systeemin reaktioiden ja vaikutusten tutkimiseen. (Yin, 2015, s. 4.)

6.2 Tutkimusongelma

Tässä tutkimuksessa tutkitaan siis kyber-fyysisen turvallisuussysteemin resilienssiä. Turvallisuusjärjestelmää tutkitaan systeemiteorian näkökulmasta, jossa järjestelmää itsessään kuvataan kyber-fyysisenä sosiaalisena systeeminä. Tutkimuksessa keskitytään edellä mainitun systeemin resilienssin tutkimiseen, kun systeemiin kohdistetaan monivaikutteinen ulkopuolinen isku. Tutkimus on laadullinen tutkimus, jonka tarkoituksena on tuottaa tietoa kyber-fyysisen sosiaalisen systeemin toiminnasta ja sen resilienssistä. Tutkimuksen kantavana tutkimuskysymyksenä on: *Millainen on resilienssi kyber-fyysisessä turvallisuussysteemissä?*

6.3 Tutkimusongelman rajaus

Tutkimuksessa turvallisuussysteemiä tutkitaan kyber-fyysisenä sosiaalisena systeeminä, joka koostuu saman tasoisista tai eritasoisista eri systeemin elementeistä. Systeemin sisällä elementit voivat olla yhteydessä toisiinsa, niiden toiminta voi olla riippuvaista toisistaan tai niillä voi olla rajapintoja toistensa kanssa, mutta yhteistä kaikille systeemin elementeille on, että ne toimivat systeemin sisällä itsenäisesti.

Tässä tutkimuksessa ei tutkita minkään yksittäisen viranomaisen tai toimijan toimintaa erityisesti tai sen toimintamalleja yksittäisenä toimijana. Välttääkseen tämän, tässä tutkimuksessa systeemin sisältämiä toimijoita ei tulla ollenkaan nimeämään, vaan siitä käytetään nimitystä turvallisuussysteemi.

Tämän tutkimuksen tarkoituksena on luoda neljä reaalisesti mahdollista skenaariota ja arvioida systeemin resilienssiä kussakin skenaariossa. Tutkimuksen tavoitteena on löytää sellaisia skenaarioita yhdistäviä tekijöitä, joilla on merkitystä resilienssin kasvattamiseen, sekä sellaisia tekijöitä systeemissä, jotka laskevat resilienssiä tai muodostavat uhan sellaiseen. Tässä tutkimuksessa ei lasketa todennäköisyyksiä näiden eri skenaarioiden toteutumiseksi.

6.4 Skenaarioanalyysi

Skenaariotyöskentely (skenaarioanalyysi) on tulevaisuudentutkimukseen kehitetty tutkimusmenetelmä. Se on alunperin kehitetty toisen maailmansodan jälkeen Herman Kahnin toimesta sotilaallisen päätöksenteon tueksi ja varautumiseksi, sekä Kahnin ansiosta myöhemmin 1950-luvulla myös yhteiskunnalliseen ja taloudelliseen toimintaan ja päätöksentekoon. Skenaario-analyysi

kehitettiin analyysimenetelmäksi etsimään tulevien tapahtumien indikaattoreita, sekä oikeita päätöksenteko hetkiä. (Amer, Daim & Jetter, 2015, s. 23-24.)

Rubinin (2015) mukaan skenaariolla on tulevaisuuden tutkimuksessa kaksi erilaista merkitystä. Ensiksi sillä pyritään kuvaamaan tulevaisuudentila useiden erilaisten vaihtoehtoisten tilojen ja vaiheiden kautta, eikä pelkästään valmiiksi määriteltynä oletettuna tulevaisuutena. Toisen merkityksen antaa sen menetelmällinen ulottuvuus. Rubinin mukaan skenaarioanalyysiä käytetään menetelmänä tehdä yhteenveto tulevaisuuden tutkimuksen tuotoksista. Sen avulla voidaan tehdä havaintoja tulevaisuuden tiloissa havaituista yhteneväisyyksistä ja eroavaisuuksista. (Rubin, 2015.)

Hsian ym. (1994) mukaan skenaarioanalyysi on erityisesti prosessi, jolla pyritään ymmärtämään, analysoimaan ja kuvaamaan sitä kuinka tutkittavana olevan objektin (tässä tutkimuksessa systeemin) tulisi toimia. Prosessin avulla pyritään kuvaamaan tutkittavan objektin oletettuja syötteitä tai tapoja, ja niihin saatuja vastauksia. Analyysiprosessin lopputuloksena syntyy skenaario (tai useita skenaarioita), jota voidaan pitää oikeanlaisena ja mahdollisimman luotettavana tulevaisuuden kuvauksena. (Hsia ym., 1994, s. 34.)

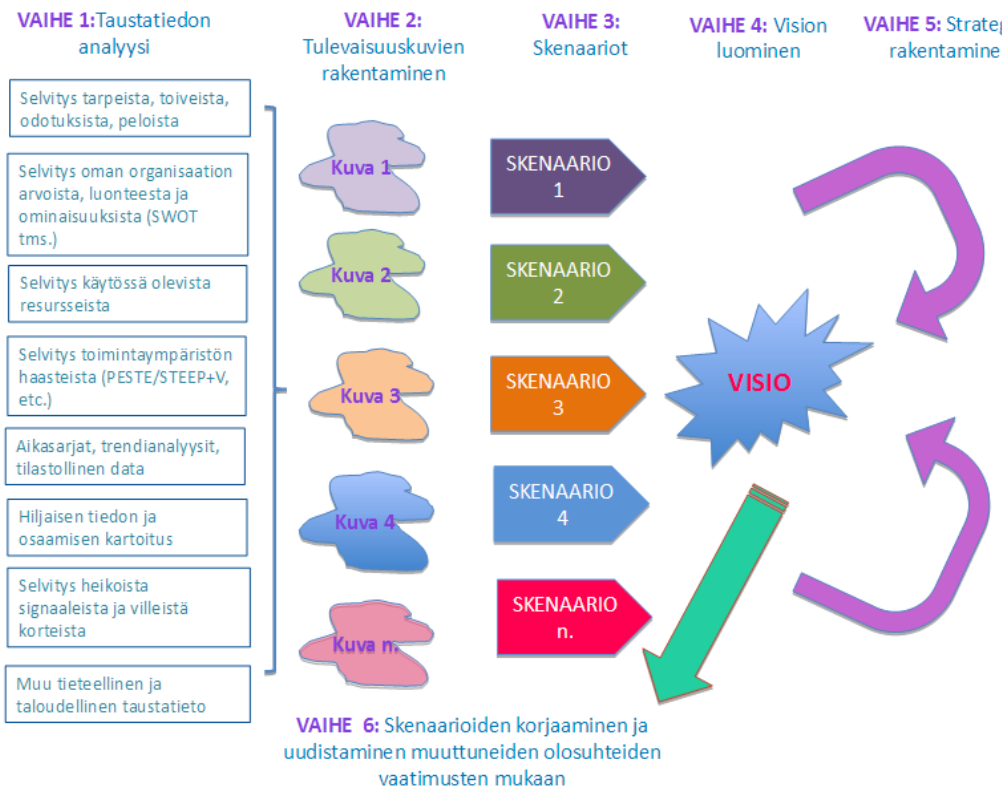
Skenaarioanalyysi tarjoaa Amerin ym. (2015) mukaan oivallisen työkalun organisaatioille päätöksenteon tueksi. Malaskan, Malmivirran, Meristön ja Hansénin (1984) mukaan skenaarioanalyysi on nimenomaisesti strategisen johtamisen ja päätöksenteon työkalu. Se mahdollistaa valmistautumisen ja varautumisen tuleviin mahdollisiin tapahtumiin. Tulevaisuuden kuvien avulla voidaan tehdä ennusteita, kehittää varautumisajattelua, sekä ohjata päätöksentekoa. (Malaska, Malmivirta, Meristö & Hansén, 1984, s. 48; Amer ym., 2015, s. 23-24.)

Skenaario voidaan sekoittaa helposti ennusteen kanssa. Rubinin (2015) mukaan skenaarioilla kuvataan rakenteellisesti erilaisia tulevaisuudentiloja, joilla on looginen juoni. Ennusteen tarkoitus on kuvata perusmallista johdettua erikseen määriteltyä tulevaisuuden kehitystä. Skenaariossa tutkitaan perusmallissa eri tasoilla olevia ilmiöitä ja niissä tapahtuvia muutoksia. Amerin ym. (2015) mukaan ennusteen tarkoituksena on tuottaa todennäköisin mahdollinen johtopäätös, kun taas skenaarioanalyysillä tutkitaan epävarmuustekijöistä johtuvia tuloksia saadaan vaihtoehtoisia ja silti mahdollisia tulevaisuuden kuvauksia. Tosin skenaarioanalyysissä laaditaan myös eräänlainen ennuste (ennalta toivottu) yhtenä osana prosessia. (Amer ym., 2015, s. 25; Rubin, 2015.)

Skenaariotyöskentelyn tavoitteena on tuottaa useampia toisistaan poikkeavia malleja päätöksenteon avuksi. Rubinin (2015) mukaan tavallisesti pyritään luomaan neljä tai viisi erillaista tulevaisuudentilaa. Tällä pyritään välttämään sitä, että ilmiöitä ja muutoksia arvioimalla luotaisiin ennalta toivottu tulevaisuuden kuvaus. Tämän välttääkseen luodaan myös vastakkainen skenaario, *negaatio*, jossa tarkastellaan tulevaisuuden tilaa, mikäli edellisessä

skenaariossa annettuihin muutoksiin, eikä skenaarion kulkuun puututtaisi. Tutkimuksessa tuleekin tarkastella kriittisesti siinä luotuja skenaarioita, jotta vältettäisiin ennalta arvattavia tai toivottuja skenaarioita tai annettaisi skenaarion oletettavan lopputuloksen ohjata skenaarion kehittämistä. Skenaarion ei tule ohjata lopputulosta vaan sen tulee keskittyä lopputulokseen johtavaan kehitykseen. (Rubin, 2015.)

Tulevaisuudenkuvat muodostuvat useasta eri tekijöistä ja niiden lopputuloksiin vaikuttavat erilaiset kehityspolut. Tulevaisuuden tutkimuksessa on aina mahdollista myös odottamattomat tapahtumat tai sattumat. Skenaariomenetelmällä tällaisia seikkoja voidaan ottaa myös huomioon. Skenaariomenetelmä on valittu tutkimusmenetelmäksi juuri sen vuoksi, että sen avulla voidaan analysoida useita erilaisia kehityspolkuja ja havainnollistaa systeemin muutosta eri tekijöiden vaikutuksesta. Erilaisten skenaarioiden avulla voidaan tutkia systeemin muutos- ja oppimiskykyä. Menetelmän etuna tässä tutkimuksessa on useamman mahdollisen vaihtoehdon toteuttaminen. Tämä tutkimus tullaan toteuttamaan sovelletusti Rubinin (2015) alla esittämän mallin mukaisesti. Rubinin (2015) mukaan skenaariotyöskentelyssä voidaan erottaa kuusi eri työvaihetta (kuvio 7).



KUVIO 7: Skenaariotyöskentelyn vaiheet Rubinin mallin mukaan

1. Nykytilan määrittely. Kartoitetaan systeemin nykytila (SWOT ja PEST+V -analyysit) ja analysoidaan mahdolliset kehityskulkuun vaikuttavat ulkoiset tekijät.
2. Tulevaisuuskuvien rakentaminen. Rakennetaan aihiot, joihin skenaariot tulevat pohjautumaan.
3. Skenaarioiden määrittely. Rakennetaan useampi toisistaan poikkeava tulevaisuuden skenaario.
4. Vision luominen. Skenaarion pohjalta rakennetaan visio siitä, millainen systeemi voisi olla.
5. Rakentamisvaihe. Tässä tutkimuksessa rakentamisvaiheessa käytetään asiantuntijahaastattelua, jossa skenaarioanalyysillä luotuja skenaarioita koetellaan asiantuntija-paneelia käyttämällä.
6. Skenaarioiden korjaaminen. Rubinin mukaan skenaariotyöskentely on prosessi, jota toistamalla tutkittavana oleva systeemi pysyy ajan tasalla. Tässä tutkimuksessa skenaarioanalyysin ja asiantuntijahaastattelun tulosten perusteella syntyy korjausehdotuksia jo luotuihin skenaarioihin.

6.4.1 Tulevaisuuskuvien rakentaminen

Tulevaisuuspolku on Kamppisen, Malaskan ja Kuusen (2002) mukaan sellainen mahdollinen reitti, joka kulkee nykyisyydestä tulevaisuuteen ja on ajallisesti järjestynyt. Siinä tapahtumat tapahtuvat aikajärjestyksessä, eikä seuraavaa tapahtumaa voi olla ilman ajallisesti edellistä sellaista. Ajallisuuden järjestäytymisellä on merkitystä, kun tulevaisuuspolku haarautuu. Tulevaisuuspolulla tarkoitetaan niitä toimenpiteitä, jotka mahdollistavat siirtymisen nykytilasta tulevaisuuteen, sekä niitä reuna ehtoja, jotka tätä kehityspolkua rajaavat. Se on palautumaton, joka tarkoittaa, että sitä voidaan kulkea vain yhteen suuntaan, eteenpäin. Polkua pitkin ei voida kulkea takaisin päin, sillä sen mahdollistavat ja rajaavat tekijät eivät toimi tulevaisuudesta nykyisyyttä arvioitaessa. (Kamppinen, Malaska & Kuusi, 2002, s. 27-28.)

Skenaario on Kamppisen ym. (2002) mukaan tulevaisuuspolun toteutettavissa oleva oleva maailma, joka on erityisen merkittävä. Skenaariot ovat yleensä tulevaisuuden maailmoina, joko erittäin haluttuja tai vältettyjä. Tieteellisessä tutkimuksessa tulee välttää haluttuja tulevaisuuden kuvia ainoina tulevaisuuden maailmoina, jonka vuoksi tulee tutkimuksessa huomioida myös katastrofi tulevaisuuden maailma. Tällöin huomioitavia tulevaisuuspolkuja ovat uhkakuvat ja -tekijät, jotka voivat aiheuttaa ei-toivottavien tulevaisuuskuvien tai tapahtumien toteutumisen. Tulevaisuuspolkua voidaan kuvata myös aikajanalla, jossa on alku ja loppu. Aikajanalla esiintyy mahdollisesti tapahtumia, jotka voivat vaikuttaa aikajanan suuntaan tai sen haarautumiseen. (Kamppinen ym., 2002, s. 31-33.)

6.4.2 Useamman skenaarion rakentaminen

Useamma skenaarion rakentamisen (*Multiple Scenario Analysis*) ajatuksena on Schoemakerin (1993) mukaan tuottaa päätöksenteon tueksi vaihtoehtoisia tulevaisuuden kuvia. Sen avulla voidaan pyrkiä ennustamaan muuttujien epävarmuutta ja niiden kompleksisuutta, sekä näiden yhteisvaikutusta tutkittavan ongelman ratkaisuun. Useamman skenaarion avulla voidaan luoda ennusteita, sekä laskea niille todennäköisyyksiä, ennusteiden toteutumiseksi. Mitä suuremmaksi epävarmuuden ja kompleksisuuden suhde kasvaa, sitä suuremmaksi ennusteen epävarmuus nousee. Useamman skenaario analyysi on työkalu ennusteiden laatimiseksi, eikä se itsessään ennusta tulevaisuutta. (Schoemaker, 1993, s. 195, 197.)

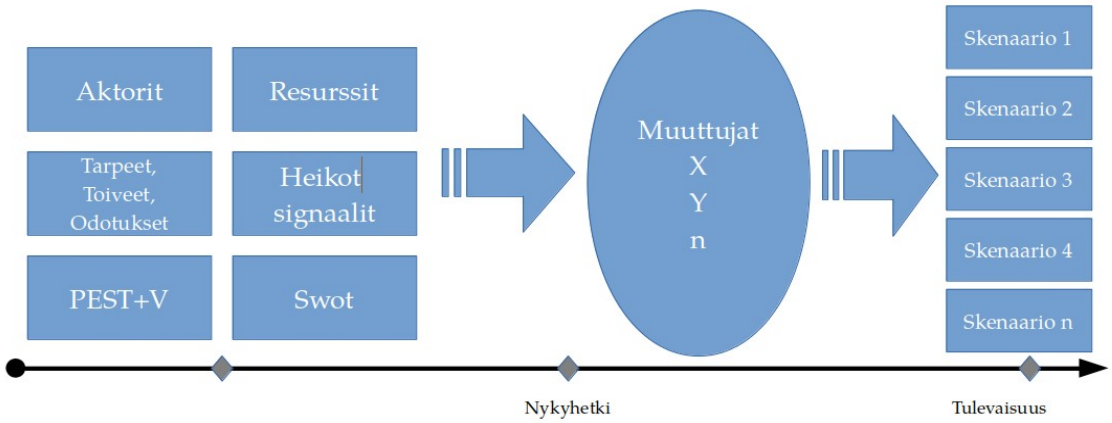
Boodin (1997) mukaan useamman skenaarion rakentaminen auttaa havaitsemaan päätöksentekijän tietämättömyyttä, sekä mahdollisia pullonkauloja, jotka saattavat olla esteenä haluttuun lopputulokseen pyrittäessä. Useamman skenaarion rakentaminen on päätöksentekotyökalu, jolla Boodin mukaan voi harjoitella erilaisia seurauksia tulevaisuudessa ja se antaa myös palautetta tehdyistä toimenpiteistä, sekä niiden vaikutuksista. Lisäksi sillä voidaan lisätä yhteisymmärrystä systeemin sisällä päätöksenteon merkityksestä ja vaikutuksista systeemin tulevaisuuteen. Skenaarioiden rakentamisessa avaintekijänä on se, että sen tekee systeemi itse, eikä sitä tuota esimerkiksi ulkopuolinen konsultti tilaustyönä, jolloin skenaarioanalyysistä katoaa mahdollisuus havaita mahdollisia vaarantavia virheitä kesken päätöksentekoprosessin, sekä kyky oppia niistä. (Bood, 1997, 644-645.)

6.4.3 Skenaarioanalyysi prosessina

Skenaarioanalyysi on prosessi, jossa mahdollisten tulevaisuuskuvien perusteeksi kerätään riittävä määrä tietoa, jotta sen perusteella voidaan kartoittaa systeemin nykytila ja laatia sen tiedon pohjalta skenaariomallit. Alla olevassa kuviossa 8 on kuvattu tämän tutkimuksen skenaarioanalyysi prosessina. Prosessin ensimmäisenä vaiheena on taustatiedon analyysi. Taustatiedon analyysissä määritellään tutkimuksen skenaarioanalyysin laajuus, aikajana tai ajalliset rajat (luku 7.1.1), jossa tutkimus toteutetaan. Tämän lisäksi kartoitetaan sen keskeiset toimijat (luku 7.1.2), systeemin olemassa olon tarkoitus (luku 7.1.3), tehdään SWOT-analyysi systeemin nykytilasta (luku 7.1.4), tehdään systeemin toimintaympäristön analyysi PEST+V (luku 7.1.5), sekä havainnoidaan systeemin tulevaisuuteen vaikuttavista mahdollisista heikoista signaaleista (luku 7.1.6).

KUVIO 8: Deduktiivisen tutkimuksen skenaarioanalyysin prosessikaavio

Tutkimus on toteutettu deduktiivisena skenaarioanalyysinä. Deduktiivisessa skenaarioanalyysissä tarkastellaan tutkittavaa kohdetta sen nykytilassa ja luodaan kuvia, jotka suuntautuvat nykyhetkestä tulevaisuuteen, käyttäen hyväksi tiedettyjä muuttujia. Kuviossa 9 on kuvattu deduktiivinen skenaarioprosessi. Siinä systeemin nykyhetki riippuu ennen nykyhetkeä olevista tapahtumista, sekä niiden vaikutuksesta systeemiin. Deduktiivinen päättely on Johnson-Lairdin (1999) mukaan menetelmäprosessi, jossa olemassa olevien muuttujien avulla tehdään loogisia päätelmiä. Se on siis päättelyketju, jossa joko/tai -arvojen perusteella edetään loogisesti kohti lopullista päätelmää käyttäen ainoastaan tiedossa olevia muuttujia. Tulevaisuuteen suuntaavassa skenaarioanalyysissä systeemin tulevaisuuskuviin vaikuttavat nämä muuttujat, jotka ohjaavat systeemin tulevaisuuden kehitystä. Muuttujien yhdistelmät ja muutokset (joko/tai -mahdollisuus) toimintaympäristössä vaikuttavat jokaiseen mahdolliseen tulevaisuuskuvaan. (Rubin, 2015 & Johnson-Laird, 1999, s. 114.)



KUVIO 9: Deduktiivinen skenaarioanalyysi prosessina.

6.5 Asiantuntijahaastattelumenetelmä resilienssin analysoinnissa

Skenaarioanalyysin tuloksena muodostetaan neljä erilaista skenaariota kolmen eri muuttujan kautta. Näiden muuttujien perusteella rakennetaan analyysi siitä, millainen systeemin resilienssi on valitussa skenaariossa. Asiantuntijahaastattelun tarkoituksena on koetella tutkimuksella saatuja tuloksia, sekä laajentaa resilienssin näkemystä useammasta perspektiivistä. Asiantuntijat muodostavat SWOT-analyysin avulla kuvan systeemin sisäisistä ja ulkoisista ominaisuuksista.

Ruusuvuoren ja Tiittulan mukaan (2017) tutkimushaastettelu on menetelmällinen tapa kerätä tutkimuksen avuksi. Siinä haastattelulla on tietty tarkoitus ja siihen osallistujilla on jokaisella määritellyt roolit. Haastattelu lähtee tutkijan aloitteesta ja tutkijan tarpeesta haastattelulle. Tutkimushaastattelussa tieto on tutkijalla, johon haastattelija vastauksillaan tuottaa omaa kontribuutiotaan, jota tutkimuksessa jalostetaan edelleen uudeksi tiedoksi. (Ruusuvuori & Tiittula, 2017, s. 39, 46.)

Tutkimus on toteutettu kyselyhaastatteluna, jossa kerätään laadullista tietoa skenaarioanalyysin tueksi. Vastaajia on pyydetty vastaamaan kyselylomakkeeseen, joka etsii vastausta kysymykseen *millainen.* Leinosen, Otonkorpi-Lehtorannan ja Heiskasen (2017) mukaan laadullisen haatattelun tavoitteena on haaastateltavien yksilölliset näkemykset ja tutkijan tavoitteena on tulkita niitä. Haastattelun struktuuri voi voi vaihdella tarpeen mukaan. Tässä tutkimuksessa haastattelulla on yhteinen struktuuri, joka on SWOT-kyselylomake. Haastateltavat tuottavat tähän lomakkeeseen oman näkemyksen SWOT-analyysin avulla. (Leinonen, Otonkorpi-Lehtoranta & Heiskanen, 2017, s. 68.)

Leinosen ym. (2017) tutkijan tulee itse arvioida sitä, onko valittu aineistokeruumenetelmä sopivin ko. tutkimusta varten. Tässä tutkimuksessa asiantuntijahaastetteluita käytetään tutkijan omien tulosten koetteluun ja tällöin niiden arvioiminen SWOT-analyysillä tuottaa tietoa tutkimuksessa saadun tiedon laadusta, vahvistaa niitä tai korjaa niitä. Tutkimuksessa käytettävä kyselylomake on jokaiselle haastateltavalle samanlainen ja asiantuntijat vastaavat niihin oman alansa asiantuntijuuden näkökulmasta. (Leinonen ym., 2017, s. 68-69.)

6.5.1 Asiantuntijoiden valinta

Tutkimuksen asiantuntijoiksi on valittu kolme asiantuntijaa, joiden ydinosaamisalue on kyberturvallisuudessa, hybridivaikuttamisessa, sekä kokonaisturvallisuudessa. Tutkimuksen kannalta asiantuntijuus on määritelty henkilön ammatillisen tehtävien kautta. Alastalon, Åkermanin ja Vaittisen

(2017) mukaan asiantuntijuus määrittyy henkilön toiminnan tai institutionaalisen aseman kautta, mutta se ei ole kuitenkaan pysyvä olotila. Asiantuntijuus tutkimuskohteelle määrittyy aina tapauskohtaisesti. Asiantuntijoiden valinnassa tulee Alastalon ym. (2017) mukaan kiinnittää huomiota siihen, että he pystyvät tarjoamaan riittävän laajan näkemyksen tutkittavaan asiaan ja tarvittaessa tarjoamaan myös kriittisiä näkemyksiä. Tässä tutkimuksessa asiantuntijoiden tehtävänä on nimenomaisesti arvioida skenaarioanalyysin tuloksia ja koetella tutkijan itsensä saamia tuloksia. (Alastalo, Åkerman & Vaittinen, 2017, s. 181-184.)

6.5.2 Haastattelun anonymiteetti

Asiantuntijat osallistuvat tutkimukseen anonyymeina, koska pätevien asiantuntijoiden saaminen haastatteluun vaikeutui oleellisesti, jos haastatteluun olisi tullut osallistua omalla nimellä. Vastaajilla on ammatti- tai työsidonnaisuuksia, jotka saattoivat vaikuttaa haluun vastata omalla nimellä. Anonymisoinnilla pyritään eliminoimaan juuri näiden ammatti- tai työsidonnaisuuksien vaikutusta haluun ja mahdollisuuteen vastata tutkimuksen kyselyyn. Lisäksi se mahdollistaa vastaajille olla edustamatta työnantajansa näkemyksiä ja pohtimaan omia näkemyksiään laajemmin. Asiantuntijoille on annettu tunnisteet A, B ja C, joiden avulla heidän vastauksensa voidaan erotella tutkimusdatasta.

6.6 Tutkimuskohde

Tutkimuksessa käytetään kuvitteellista alkutilannetta, jolla simuloidaan systeemiin kohdistuvaa vaikutusta. Alkutilanteessa on kuvattu tila, johon tutkittavana oleva kyber-fyysinen systeemi on joutunut ja siihen on kohdistunut siitä riippumattomia vaikuttimia, jotka pakottavat sen johonkin toimintaan ja muutokseen.

Alkutilanne, josta skenaarioiden rakentaminen alkaa: Useita viranomaisia vastaan on tehty laajamittaisia palvelunestohyökkäyksiä, jossa julkisen hallinnon tietojärjestelmät ovat kaatuneet tai toimivat rajatusti. Lisäksi viranomaisverkko on lähes koko ajan paikallisesti ylikuormittunut, eikä toimi käytännössä ollenkaan. Tapahtuma-alueella on ollut myös ongelmia matkapuhelinverkossa sen ylikuormittumisen vuoksi, eikä esimerkiksi hätäkeskukseen ole aina voinut soittaa.

Samaan aikaan internetissä on liikkunut jo useita päiviä lähinnä poliisiin ja sosiaaliviranomaisiin kohdistuvaa uutisointia, liittyen kolme päivää aiemmin tapahtuneeseen ulkomaalaisen perheen lasten huostaanottoon, jossa poliisi on joutunut käyttämään voimakeinoja avustaessaan lastensuojeluviranomaisia.

Verkossa leviää materiaalia useilla erilaisilla media-alustoilla, joissa poliisia syytetään vanhempien pahoinpitelystä ja sosiaaliviranomaisia kansalaisuuteen perustuvasta tarkoitushakuisesta toistuvasta syrjinnästä.

Sosiaalinen media pursuaa viestejä, joissa viranomaisia syytetään salailusta, väkivallasta, sekä kansallisuuteen perustuvasta syrjinnästä. Viestien määrä sosiaalisessa mediassa lisääntyy koko ajan ja muuttuu koko ajan aggressiivisemmaksi. Useat viranomaiset ovat saaneet häirintäviestejä jopa henkilökohtaisille sosiaalisen median tileille. Sosiaaliseen mediaan on lyhyessä ajassa liittynyt paljon uusia käyttäjiä, jotka ottavat osaa keskusteluun ja viranomaisten painostamiseen voimakkaaseen ja jopa aggressiiviseen sävyyn.

Samaan aikaan viranomaisten toimenpiteiden kohteeksi joutuneen perheen oman maan ulkoministeri on julkisesti moittinut Suomen viranomaisia heidän kansalaisiin kohdistuneesta kasvavasta väkivallasta ja laittomista toimista, sekä uhannut, että tulisivat puolustamaan kansalaisiaan myös Suomessa, mikäli suomalaiset viranomaiset eivät tähän kykenisi.

Samana päivä YLE uutisoi välikohtauksesta Suomen valtion raja-asemalla, jossa kaksi autoa, sisällä kasvot peittäviin asuihin pukeutuneita henkilöitä, ovat ajaneet rajanylityspaikan lävitse pysähtymättä, aina Suomen puolelle asti ja jatkaneet pakoa sisämaahan päin. Tämän jälkeen heistä ei ole havaintoa.

7 TULOKSET

Tässä luvussa esitellään tämän skenaarioanalyysin tulokset. Analyysin jälkeen tutkimuksessa saatuja tuloksia koetellaan asiantuntijoiden tekemillä arvioilla tulevaisuuskuvien resilienssistä (SWOT-analyysi), jonka avulla arvioidaan tulosten oikeellisuutta. Kyber-fyysisen turvallisuussysteemin resilienssiä tässä tutkimuksessa tarkastellaan kolmen systeemiin kohdistuvan vaikuttimen näkökulmasta. Vaikuttimet kohdistuvat systeemin keskeisiin toiminnallisiin ulottuvuuksiin kyber-fyysisessä maailmassa. Vaikuttimien toiminnallisuuksia tarkastelemalla muodostuu systeemille erilaisia tulevaisuuden tiloja. Tarkasteltavina vaikuttimina tutkimuksessa ovat:

- *Systeemiin kohdistuvat kyberhyökkäykset*
- *Informaatiovaikuttaminen systeemissä*
- *Fyysinen isku systeemiä vastaan*

7.1 Nykytilan kartoitus

7.1.1 Skenaarion laajuuden määrittely

Tässä tutkimuksessa laadittavilla skenaarioilla on ajallisesti kahden ajanjakson välillä oleva tapahtumasarja. Aikajanan pituudet määrittyvät sen perusteella, jolloin halutun muuttujan tai muuttujien vaikutus on todennettavissa kyseisessä skenaariossa. Skenaarion ajallinen ulottuvuus on siis sidottu haluttujen muuttujien vaikutuksiin ja esiin nousemiseen.

Kuitenkaan aikajana ei ole niin pitkä, että skenaarioita laadittaisiin perustuen sellaisiin odotuksiin ja tekniikoihin, joita ei ole vielä ehditty keksiä. Kyseessä on yksittäiseen tapaukseen liittyvät tulevaisuuden kuvat, jonka aikana ei ehdi syntyä uutta teknologiaa, eikä muuta sellaista muuttujaa, jota tämän hetkisen tietämyksen valossa ei tunnettaisi. Toimintaympäristössä voi tapahtua lyhyessäkin ajassa yllättäviä muutoksia, jotka skenaarioanalyysissä olisi merkityksellistä huomioida mahdollisimman hyvin.

7.1.2 Keskeiset toimijat

Koska tarkastelu tapahtuu systeemitasolla, tutkimuksessa keskeiset toimijat ovat systeemi ja sen ympäristössä olevat toiset systeemit, sisäiset toimijat, sekä ympäristö itse, joka myös määritelmän (kts. s. 12) mukaan on oma systeeminsä.

Pilkottaessa tutkittavaa systeemiä osiin, sen sisältä löytyvät tutkimuksen elementit, ihmiset (sosiaalinen ulottuvuus) ja laitteet (kyberulottuvuus), sekä fyysinen maailma. Koska tutkimuksen toimijaa katsotaan abstraktista näkökulmasta, keskeisenä toimijana pidetään tässä tutkimuksessa koko tutkittavaa systeemiä. Vaikka systeemi pitää sisällään useita eri sisäisiä systeemejä, keskitytään tutkimuksessa vain turvallisuussysteemin havainnointiin.

7.1.3 Systeemin tarpeet, toiveet ja odotukset

Turvallisuussysteemin olemassa olon tarkoituksena on olla kokonaisturvallisuuden, yhteiskuntarauhan ylläpitäjänä ja aktiivinen toimija sen kehittäjänä. Yhteiskunta (ympäristö systeemin ulkopuolella) sekä systeemi itsessään asettavat sen toiminnalle ja kyvykkyydelle resursseja sekä vaatimuksia, joihin systeemin odotetaan vastaavan. Systeemiltä vaaditaan, että se kykenisi suoriutumaan sille määritellyistä tehtävistään myös kriisien aikana. (Turvallisuuskomitea, 2017, s. 7-8.)

Systeemin toiminnan varmistaminen lähtee sen kyvystä varautua tuleviin tapahtumiin, havaita poikkeamia tapahtumavirrassa, sekä kyetä ennakoimaan niitä, sekä vastaamaan näihin poikkeamiin ja tällä tavoin varmistaa sen häiriötön toiminta myös kriisiaikana. Vastatakseen näihin odotuksiin, systeemillä täytyy olla sen ympäristön tuki ja hyväksyntä sen toimille. Tämä edellyttää luottamusta systeemin ja ympäristön kesken. Luottamus syntyy siitä, että systeemin yhteiskunnalliset toimijat (viranomaiset) käyttävät toimivaltaansa ja sille annettuja oikeuksia lainsäätäjän edellyttämällä tavalla. Lisäksi luottamusta edistää toiminnan läpinäkyvyys ja toiminnan tehokas laillisuusvalvonta. Perustuslaissa (1999) on määritelty viranomaisen toimivaltuuksien edellytykset. Niiden mukaan kenenkään perustuslaillisiin oikeuksiin, ei saa puuttua ilman laissa säädettyä perustetta (Perustuslaki 2 luku, 7 §, 3. momentti). Viranomaisten toimivaltuuksista on säädetty tarkemmin kutakin viranomaista koskevassa lainsäädännössä, jossa on määritelty viranomaisten toimivaltuudet erikseen.

7.1.4 SWOT-analyysi systeemin nykytilasta

SWOT-analyysin avulla pyritään selvittämään tutkittavan systeemin vahvuudet, heikkoudet, mahdollisuudet ja uhat sen nykytilassa. SWOT-analyysi on Pickton

ja Wrightin (1998) mukaan katsaus järjestelmän sisäisiin ja ulkoisiin tekijöihin. Picktonin ja Wrightin mukaan SWOT-analyysin tarkoitus on analysoida järjestelmän sisäisiä tekijöitä suhteessa sen kykyyn ja resursseihin, sekä analysoida järjestelmän ulkoisia tekijöitä, jotka liittyvät sen ympäristöstä tunnistettaviin muuttujiin. (Pickton ja Wright, 1998, s. 103.)

Taulukossa 1 on kuvattu SWOT-analyysin sisäisten tekijöiden (vahvuudet ja heikkoudet) ominaisuuksia ja taulukossa 2 ulkoisten tekijöiden (mahdollisuudet ja uhat) ominaisuuksia. SWOT-analyysin tarkasteltaviksi ominaisuuksiksi on tutkimuksessa määritelty systeemin johtaminen, tilannekuva, osaaminen, ja teknologia. SWOT-analyysin ominaisuudet on valittu siten, että ne mahdollisimman monipuolisesti kuvaavat kyber-fyysistä kompleksista turvallisuussysteemiä, ja ne kuvastavat kyber-fyysisen turvallisuussysteemin kriittisiä toiminnallisuuksia ja vaatimuksia koko systeemin tasolla.

	VAHVUUDET	**HEIKKOUDET**
Johtaminen	Monialaosaaminen johtamisen tukena Johtosuhteiden määrittely ennalta	Toiminnan luonteen tunnistaminen Johtovastuun tunnistaminen
Tilannekuva	Kokonaisturvallisuus huomioitu strategiassa Tärkeimmät uhat tunnistettu strategiassa	Onko kaikki uhkatekijät tunnistettu? Onko tunnistamatta keskeisiä uhkia? Ei tiedetä, mitä ei tiedetä
Osaaminen	Koulutettu henkilöstö Operatiivinen koulutus Yhteistoiminta -harjoitukset	Sisäisten osien välinen osaaminen ja ymmärrys Resurssien riittävyys
Teknologia	Nykyaikainen teknologia Ylläpito ostopalveluna	Järjestelmiin kohdistuvat häiriöt Varajärjestelmien käyttö operatiivisessa toiminnassa

TAULUKKO 1: SWOT-analyysin sisäiset attribuutit

	MAHDOLLISUUDET	UHAT
Johtaminen	Toimijoiden ja vastuualueiden tunnistaminen Tilannekuva johtamisen työkaluna	Johtamistyhjiö Päätöksentekokyvyttömyys
Tilannekuva	Mahdollisuus useamman toimijan yhteiseen tilannekuvaan	Tiedonvaihto Tilannekuvan päivittyminen
Osaaminen	Koulutuksen muuttaminen läpileikkaavaksi	Resurssien riittäminen koulutukseen
Teknologia	Teknologian käyttö operatiivisessa toiminnassa ja johtamisessa	Kyberhäiriöt lamauttavat toiminnan Teknologian kestävyys

TAULUKKO 2: SWOT-analyysin ulkoiset attribuutit

Johtaminen. Systeemin johtamisen vahvuuksia ovat turvallisuusuhkien tunnistaminen ja kokonaisturvallisuuden huomioinen viranomaistoiminnassa. Yhteiskunnan turvallisuusstrategiassa 2017 on kuvattu kokonaisturvallisuuden yhteistoimintamalli, jossa määritellään yhteiskunnan varautumisen vastuunjako, sekä lainsäädäntöön perustuvat tehtävät. Johtamisesta on siis olemassa suunnitelma- ja vastuunjakomallit. Systeemin vahvuutena on, että sen sisäiset prosessit on tunnistettu ja toiminnat vastuutettu. Yhteiskunnan turvallisuusstrategian mukaan vastuun jaossa on myös tunnistettu vastuut johtamisessa. Johtamisen heikkoutena on johtovastuun tunnistaminen kriisitilanteessa. Systeemin sisällä on useita eri toimijoita, joilla on oma toimivaltaan perustuva tehtäväkenttänsä. (Turvallisuuskomitea, 2017, s. 7, 11.)

Johtamisen mahdollisuuksia systeemissä ovat toimijoiden ja vastuualueiden tunnistaminen, sekä kattavan tilannekuvan ylläpito, mikä mahdollistaa tehokkaan operatiivisen toiminnan. Mikäli näitä ominaisuuksia pystytään hyödyntämään oikein, tehostaa se systeemin resurssien käyttöä, sekä lisää sen kykyä reagoida mahdollisimman varhaisessa vaiheessa. Johtovastuun tunnistamisesta johtuvat vaikeudet voivat johtaa johtamistyhjiöön, joka tarkoittaa, ettei tiedetä kuka kulloinkin johtaa tai olisi lainsäädännön perusteella siihen velvoitettu. Tämä aiheuttaa systeemissä päätöksenteon hitautta ja vaikeutta. Samanlainen ongelma johtamisen suhteen syntyy, kun käynnissä olevaa tilannetta ei tunnisteta tai siitä tehdään virheellisiä päätelmiä. Tämä on selkeä uhka systeemin toiminnalle. Taulukossa 3 on esitetty kuvainnollisesti uhkien tunnistamiseen liittyvä ajatusmalli, jonka on alun perin esittänyt Yhdysvaltain puolustusministeri Donald Rumsfeld (2002) tässä muodossa.

	KNOWN	UNKNOWN
KNOWN	Known- known	Known - unknown
UNKNOWN	Unknown-known	Unknown-unknown

TAULUKKO 3: Uhkien tunnistamiseen tarkoitettu ajatusmalli

Taulukon tarkoitus on strategisesti kartoittaa ymmärrystä tiedostetuista ja tiedostamattomista uhista. Taulukon avulla voidaan kartoittaa niitä seikkoja, jotka tällä hetkellä jo tiedetään tai seikkoja joita ei tiedetä, mutta niiden olemassaolo on huomioitu. Sen avulla voidaan myös kartoittaa, onko olemassa sellaisia seikkoja, joita ei edes osata ottaa huomioon (unknown-unknown). Ei tiedetä, mitä ei tiedetä (vrt. tiedetään mitä ei tiedetä). Taulukon perusteella voidaan lisäksi analysoida omaa tietämystä uhkien suhteen. (Rumsfeld, 2002.)

Tilannekuva. Sisäisen turvallisuuden strategian (Sisäministeriö, 2017) mukaan turvallisuussuunnittelussa on huomioitu kokonaisturvallisuuden kannalta merkittäviä uhkia. Strategiassa on kiinnitetty huomiota erityisesti sellaisiin arjen turvallisuuteen liittyviin ilmiöihin, jotka ovat merkittävästi kohonneet. Systeemin vahvuutena voidaan pitää sitä, että sillä on määritelty järjestelmä, joka tietoisesti pyrkii kartoittamaan sisäiseen turvallisuuteen liittyviä uhkia ja varautuu niihin etupainotteisesti. (Sisäministeriö, 2017, s. 11.)

Systeemin heikkouksina ovat tunnistamattomat uhkatekijät, asiat joita ei tiedetä, että niitä ei tiedetä, kuten taulukossa 3 on esitetty. Samalla se on myös ulkoinen uhka systeemin toiminnalle ja resilienssille.

Tilannekuvan osalta systeemin mahdollisuus on useamman toimijan muodostama yhteinen tilannekuva. Tämän avulla voidaan kartoittaa suuria kokonaisuuksia, sekä ohjata systeemin resursseja oikeaan paikkaan, tarkoituksen mukaisella tavalla. Uhaksi se muodustoo silloin, kun yhteiseen tilannekuvaan ei saada kaikilta toimijoilta oikeata tietoa, tai tieto ollenkaan. Tällöin systeemin sisäinen tiedonvaihto ei toimi ja vaillinainen tilannekuva saattaa johtaa vääriin johtopäätöksiin tai toimiin.

Osaaminen. Systeemin osaaminen perustuu koulutukseen. Koulutuksella tarkoitetaan systeemin elementtien saamaa peruskoulutusta, sekä operatiivista koulutusta, jolla ylläpidetään ja kehitetään systeemin toimintaa. Systeemin koulutus on samalla sen vahvuus, kuin sen heikkous. Systeemin osaset on

koulutettu oman alueensa osaamiseen, mutta laaja-alaista elementtien ylittävää koulutusta on vähäisemmässä määrin. Toiminnan kannalta on heikkous, mikäli eri elementit eivät riittävästi tunne toisten toimijoiden tehtäväkenttää ja ymmärrä niiden tarkoitusta koko systeemille.

Osaamisen kehittäminen on systeemille mahdollisuus, mikäli koulutusta tarjotaan riittävässä määrin systeemin läpileikkaavana, eikä osaaminen ja ymmärrys systeemissä siiloudu. Uhkatekijänä tälle on resurssien (aika ja henkilöstö) riittäminen tällaiselle koulutukselle.

Teknologia. Systeemin teknologisen toiminnan kehittämisestä ja ylläpidosta vastaavat ulkopuoliset toimijat, joiden vastuulla on huolehtia järjestelmien toimivuudesta toimialariippumattomasti. Tämä on systeemille vahvuus, koska se pystyy keskittämään toimintansa sen omiin ydintoiminntoihinsa. Toisaalta järjestelmien kestävyys on selkeä heikkous systeemin toiminnalle. Systeemin toiminta on paljolti riippuvaista teknologiasta ja sen toimimattomuus luo selkeän uhan tilannekuvan ja johtamisen toimivuudelle. Toisaalta systeemin mahdollisuutena on tehdä myös aktiivisti kehitystyötä teknologian resilienssin parantamiseksi, sekä sen kehittämiseksi systeemille parhaiten sopivaksi.

7.1.5 PEST+V -analyysi

PEST+V-analyysin tarkoituksena on tarkastella systeemin ulkoista toimintaympäristöä. Toimintaympäristöä tarkastellaan poliittisten, taloudellisen, sosiaalisten, teknologisten ja arvojen näkökulmasta. Taulukossa 4 on esitetty PEST+V analyysin tulokset. PESTLE (tunnetaan myös STEEPLE) analyysin avulla yritykset ja organisaatiot voivat tarkastella tulevaisuuden trendejä omassa makroympäristössään ja omista toiminallisista lähtökohdistaan. Analyysissä voidaan ottaa hyvin huomioon tarkasteltavan organisaation tai yrityksen tarpeet sen omista lähtökohdista, sekä paikalliset muuttujat. (Walden, 2011, s. 3.)

POLIITTINEN (P)	TALOUDELLINEN (E)	SOSIAALINEN (S)	TEKNOLOGINEN (T)	ARVOT (V)
Lainsäädäntö mahdollistaa kriisiajan toiminnan	Taloudellisista resursseista päätökset tekee eduskunta	Länsimainen yhteiskunta ja -kulttuuri	Nykyaikaiset teknologiset välineet	Korkea moraali ja etiikka
Vakaa hallinto	Mahdollisuus päättää annettujen resurssien käytöstä itsenäisesti.		Teknologinen kyvykkyys ja korkea osaamisen taso	Vahva normien kulttuuri, lainkuuliaisuus
				auktoriteettien kunnioitus

TAULUKKO 4: PEST+V -Analyysi

Poliittisesta näkökulmasta systeemin vahvuuksiin kuuluu lainsäädännön tuomat toimivaltuudet, jotka mahdollistavat sellaisetkin toiminnat, joita voidaan toimeenpanna ilman toiminnan kohteen suostumusta. Systeemillä on siis oikeus käyttää lain suomia pakkokeinoja. Toinen verrattain tärkeä merkitys on valtion vakaa hallinto, jota systeemi on tehty myös puolustamaan. Vakaan hallinnon tehtävänä on mahdollistaa systeemin itsenäinen ja puolueeton toiminta. Tähän sisältyy myös uhka, mikäli vakaa hallinto joutuu koetukselle ja systeemiä pyritään käyttämään hyödyksi hallinnon ylläpitämiseksi väärin perustein. Tämä saattaisi aiheuttaa systeemissä ristiriitoja sen yhteiskunnallisen tehtävän ja siltä vaaditun toiminnan kesken. Ristiriidat voisivat tehdä systeemi kyvyttömän sen yhteiskunnallisessa merkityksessä.

Taloudellisesta näkökulmasta systeemin toiminta on turvattu hallinnon toimesta. Sille on annettu määritelty taloudellinen resurssi, jonka tehokkaasta ja tuloksellisesta käytöstä se saa päättää melko itsenäisesti.

Systeemin sosiaalisia tukipilareita ovat demokraattisen yhteiskuntamallin normit, jotka perustuvat demokratialle ja yksilön vapaudelle. Lisäksi ihmiset ovat korkeasti koulutettuja ja osaamisen taso korkea.

Teknologian taso korkea ja kehitystyötä sen saralla tapahtuu paljon. Tutkimuksen ja kehityksen taso on korkea. Systeemi on vahvasti teknologia riippuvainen.

Systeemillä on korkea moraali ja etiikka ja noudattaa toiminnassaan lainsäädäntöä. Normien noudattamista pitävät yllä korkeatasoinen koulutus, sekä ulkopuolinen valvonta. Lisäksi systeemi noudattaa sen sisäistä hierarkiaa, eikä pyri kaatamaan tai vahingoittamaan sen johtosuhteita.

7.1.6 Heikot signaalit

Mannermaan (2004) mukaan heikoilla signaaleilla tarkoitetaan ilmiöitä, jotka ovat orastavasti havaittavissa. Ennen havaitsemistaan heikot signaalit eivät välttämättä ole olleet vielä olemassa, taikka ne eivät ole olleet merkityksellisiä. Näin ollen heikoilla signaaleilla ei ole tunnistettavaa menneisyyttä, vaan ne nousevat esiin omassa kontekstissaan usein useamman heikon signaalin yhteydessä. Heikko signaali ei yksin ole trendi, mutta sillä on mahdollisuus tulla sellaiseksi. Heikko signaali voi vahvistaa itseään, joka aiheuttaa heikon signaalin muuttumisen trendiksi. (Mannermaa, 2004, s. 113-115.)

Heikko signaali syntyy kontekstissa, esimerkiksi yhteiskunnallisessa ympäristössä. Sen havaitseminen on usein vaikeaa, mutta sen havaitseminen antaa mahdollisuuden varautua tuleviin ilmiöihin muita aiemmin. Heikkojen signaalien havaitseminen on hankalampaa, mitä lähempänä tarkasteltavana olevaa tapahtumaa tai ilmiötä ollaan. Tutkimuksen kohteena olevan systeemin havaintokyky tapahtumaan liittyvistä heikoista signaaleista saattaa olla hyvinkin rajoittunut, kun taas tapahtumaa kauempaa seuraavat yhteiskunnalliset päättäjät saattavat nähdä sellaisia signaaleja, jotka vaikuttavat systeemin toimintaan tai sen toimintaympäristöön tulevaisuudessa. Mannermaan mukaan heikon signaalin havaitseminen edellyttääkin usein näkökulman muuttamista. Mannermaa vertaa näkökulman muuttamista esimerkiksi katsomiseksi lapsen tai vaikkapa avaruuden näkökulmasta. Heikon signaalin havaitseminen on helpointa jälkikäteen. (Mannermaa, 2014, s. 115-116, 122.)

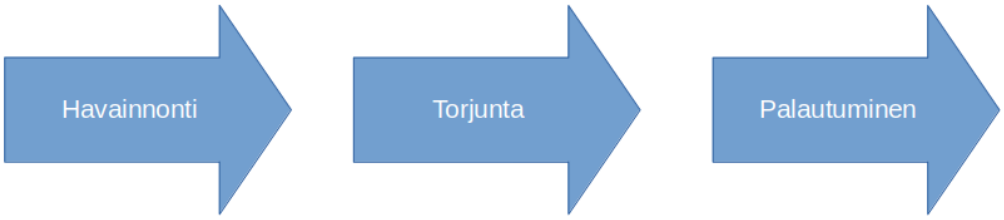
Heikoille signaalille ominaista on, että ne usein aluksi saattavat näyttää kovinkin naurettavilta tai epäuskottavilta. Lisäksi ne yleensä tulevat tarkasteltavan ilmiön ulkopuolelta. Heikkojen signaalien elinkaari on usein lyhyt. Kun heikko signaali vahvistuu trendiksi, lakkaa se olemasta enää heikko signaali, eikä sitä voida enää sellaisena käyttää tulevaisuuden ennustamisessa. (Mannermaa, 2014, s. 120-121.)

Heikkojen signaalien tarkasteleminen ilmiönä on merkityksellistä sen vuoksi, että usein jälkeen päin arvioitaessa voidaan havaita, että merkkejä tietyn tapahtuman esiin nousemisesta on ollut havaittavissa. Tässä tutkimuksessa alkutilanteen ja lopputilanteen (skenaarioiden) välinen aikajakso on suhteellisen lyhyt, mutta jo tällä aikavälillä voidaan havaita tiettyjen vaikutusten osalta aiempia signaaleja, joiden perusteella olisi voinut mahdollisesti ennustaa tulevaa kehitystä.

7.2 Skenaariot

Taustatiedon analyysin perusteella laaditaan 4 erilaista tulevaisuudenkuvaa, jotka ovat reaalisesti mahdollisia, ottaen huomioon kyber-fyysisen maailman

rajallisuudet. Skenaarioissa tutkitaan neljän vaikuttimen suhdetta SWOT-analyysillä tutkittaviin ominaisuuksiin, sekä toimintaympäristön muutoksiin. Skenaarioanalyysissä systeemin vaikuttimia arvioidaan kolmivaiheisesti (kuvio 10), kuinka systeemi havaitsee ilmiön, kuinka se kykenee torjumaan sen ja miten systeemi palautuu sen aiheuttamasta vaikutuksesta.



KUVIO 10: Vaikuttimien analysointi prosessina

Resilienssiä määritellessä jokaisen vaikuttimen osalta, sen toiminta analysoidaan näiden kolmen vaiheen kautta. Vaiheistamisen tarkoituksena on löytää se kohta vaikuttimen toimintaprosessissa, joka saa aikaan ei-toivottavan vaikutuksen systeemissä. Seuraavissa kappaleissa on kuvattu kunkin vaikuttimen osalta, miten se tutkimuksessa määritellään.

Kyberhyökkäykset: Andress ja Winterfeld (2014) määrittelevät kyberhyökkäykset *(Cyber Operations)* verkkoympäristössä tapahtuviksi tietojenkäsittelylaitteisiin kohdistuviksi aktiiviksi toimiksi. Kyberhyökkäyksillä tässä tutkimuksessa tarkoitetaan edellä mainitun määritelmän mukaisesti tietoverkkoja hyväksi käyttäviä tapoja, joilla pyritään aiheuttamaan tietojärjestelmissä suoraan tai epäsuorasti haittavaikutuksia taikka niiden toimimattomuutta. (Andress & Winterfeld, 2014, s. 4.)

Palvelunestohyökkäysten torjunnassa havainnoimisen oikea-aikaisuudella on erittäin suuri merkitys toiminnan tuloksellisuuden kannalta. Riittävän aikaisella havainnoinnilla (järjestelmissä olevat herätteet ja niiden oikeanlainen tulkinta) voidaan aloittaa toimenpiteet palvelunestohyökkäysten aiheuttamien vahinkojen rajoittamiseksi ja jopa ehkäistä palvelunestohyökkäysten näkyminen kohde systeemissä. Mohayn ym. (2011) mukaan palvelunestohyökkäysten torjunnassa kriittisintä on anomalioiden riittävän aikainen havainnointi, sekä toimivat strategiset suunnitelman tällaisten ilmiöiden torjumiseen. Kun havainnointi- torjuntatoimet ovat hallittuja, palautuminen operatiiviseen toimintaan onnistuu tehokkaammin. Hyökkäystekniikoiden muuttuessa ja kehittyessä erittäin tärkeää on myös tehdä jatkuvaa tutkimustyötä systeemin vastatoimistrategian päivittämiseksi. (Mohay ym., 2011, s. 131.)

Informaatiovaikuttaminen. Informaatiovaikuttaminen *(Information Warfare)* on Ventren (2016) mukaan informaatioympäristössä tapahtuvaa

ihmisiin ja laitteisiin vaikuttamista, jossa vaikuttamisen kohteena olevat ihmiset yritetään saada muuttaamaan mielipidettään vaikuttajan määrittelemään tavoitteeseen. Se voi tapahtua manipuloimalla tietojenkäsittelylaitteita tai yleisön nähtäville tarkoitettuja viestejä. Poiselin (2013) mukaan informaatiovaikuttamisella *(Information Operations)* tarkoitetaan toimija, joilla vaikutetaan vastapuolen informaatioon ja pyritään puolustamaan omaa informaatiota. Tässä tutkimuksessa informaatiovaikuttamisella kuvataan nimenomaan ihmisten manipulointia viestijärjestelmien kautta tai niitä hyväksikäyttämällä. (Ventre, 2016, s. 204-211.)

Informaatiovaikuttamisen torjumisessa avaintekijä on kyky havaita systeemiin kohdistuvaa informaatiovaikuttamista ja kyky aloittaa tehokkaasti torjumaan sen vaikutusten minimoiminen. Se edellyttää systeemiltä suunniteltuja ja koordinoituja toimintamalleja, joiden vaikutusta ja tehokkuutta arvioidaan jatkuvasti.

Eu-Komission HLEG (*High Level Group*) (2018) on laatinut suosituksen monitasoisesta lähestymistavasta disinformaation ehkäisemiseen, havainnoimiseen ja torjumiseen. Suosituksen mukaan disinformaation torjumisessa on viisi keskeistä pilaria, joilla disinformaatioon ja sen levittämiseen voidaan vaikuttaa.

1. Verkossa olevien uutisten läpinäkyvyyden vahvistaminen
2. Medialukutaidon lisääminen käyttäjissä
3. Työkalujen kehittäminen vahvistamaan käyttäjiä ja toimittajia estämään disinformaation levitys
4. Median diversiteetin ja kestävyyden turvaaminen
5. Tutkimus ja kehitystyö disinformaation mahdollisista vaikutuksista ja vastatoimista

Vaikka komission suositus on laadittu koko EU-alueelle, toimivat suosituksessa olevat pilarit myös turvallisuussysteemin tasolla. Pilareiden käyttäminen edellyttää turvallisuussysteemiltä kykyä sisäiseen toimintaan, sekä yhteistyötä ulkoisten sidosryhmien kanssa.

Fyysinen isku. Fyysisellä iskulla tässä tutkimuksessa tarkoitetaan väkivaltaista toimintaa tai sillä uhkaamista jolla pakotetaan uhri luopumaan toimenpiteestä tai tekemään jotakin vastentahtoisesti.

7.2.1 Skenaario 1: Toivottu skenaario

Toivottu skenaario kuvaa systeemin tilaa, jossa systeemi tekee (ja on jo aiemmin tehnyt) oikea-aikaisia havaintoja, oikeita torjuntatoimenpiteitä ja oikeita päätöksiä, sekä kykenee ylläpitämään systeemin toiminnassa, että kykenee operatiiviseen toimintaan. Taulukossa 5 on kuvattu tiivistetysti toivotun skenaarion muuttujat ja niiden vaikutusten arviointi. Skenaario on kuvattu, jotta

resilienssiä voidaan arvioida suhteessa muihin skenaariomalleihin, sekä poissulkea itsestään selvä vastaus.

VAIKUTIN	TOIMINTA	VAIKUTUSTEN ARVIOINTI
Kyberhyökkäykset	Havainto hyökkäyksestä Torjuntatoimet oikea-aikaiset Viranomaisverkko saadaan palautettua operatiiviseen toimintaan tai varajärjestelmät otettua käyttöön GSM-yhteyksien viat saadaan korjattua	Operatiivinen toimintavalmius järjestelmien suhteen saadaan pidettyä yllä (CIA) Tilannekuva säilyy Johtaminen teknisin menetelmin mahdollista Sisäinen viestintä teknisin menetelmin mahdollista
Informaatiovaikuttaminen	Kontrolloidut toimet yhdessä median kanssa valeuutisten korjaamiseksi Resurssien keskittäminen disinformaation torjutaan Havaittuihin ilmiöihin puututaan suunnitelmallisesti	Ei merkittävää vaikutusta systeemin toimintaa sisäisesti Vahvistaa systeemin luottamusta yhteiskunnassa ja kansalaisten keskuudessa
Fyysinen isku	Yhteistoiminnalla tunkeutujat paikallistetaan ja otetaan hallitusti kiinni	Yhteiskuntarauhan ja luottamuksen vahvistaminen Kyky torjua fyysinen uhka ulkoapäin vahvistuu kokemuksen ja oppimisen myötä.

TAULUKKO 5: Skenaario 1. Toivottu skenaario

Tässä skenaariossa systeemin vahvuutena on kyky tehdä oikeanlaisia havaintoja ja toimia ei-toivottujen tapahtumien ehkäisemiksi tai niiden rajoittamiseksi. Sen sisäiset prosessit ja toimiva viranomaisyhteistyö mahdollistavat jatkuvan tilannekuvan ylläpidon ja sitä osataan operatiivisesti hyödyntää oikein. Tilannekuvan rakentamiseksi systeemi on osannut hyödyntää tekemiään havaintoja, sekä havaitsemiaan heikkoja signaaleja tilannekuvan rakentamiseksi, sekä uhka-arvion tekemiseksi. Systeemillä on lisäksi riittävän hyvää

osaamista, toimivat prosessit ja tieto-taitoa meneillään olevan operaation suorittamiseksi.

Systeemin heikkoutena on, ettei mikään pakota sitä analysoimaan toimintojaan kriittisesti, eikä tekemään vaihtoehtoisia ratkaisumalleja. Asiantuntija A:n mukaan systeemin heikkoutena ja tulevaisuuden uhkana voidaankin pitää sen menestystä: ”*Tilanne menee lopulta hyvin, mutta kukaan ei nosta onnistumisen edellytyksiä kriittiseen tarkasteluun*” (Asiantuntija A). Koska kaikki toiminnot systeemin sisällä menevät, kuten systeemissä on suunniteltu, saattaa siltä unohtua tärkeä toimenpide sen suhteen, jos kaikki ei olisikaan mennyt hyvin. Tämä saattaa tulevaisuudessa johtaa systeemin oppimisprosessin heikent-ymiseen, jos systeemi ei havaitse oppimis- ja kehittämistarpeita myös niillä sektoreilla jossa se operatiivisesti menestyi. Asiantuntija A:n mukaan systeemi saattoi kyetä torjumaan ulkoisen uhan, vain sen vuoksi, että nykyinen osaaminen/kyky riittivät juuri siihen. Mikäli systeemi ei kykene kriittisesti havaitsemaan sitä, että se on mahdollisesti ollut suorituskykynsä ylärajalla, seuraava vakavampi tai toisenlaista hyökkäysmetodia käyttävä isku saattaa olla systeemille kohtalokas.

Systeemin suurin uhka on, myös kaikkien haastateltujen asiantuntijoiden mukaan, systeemin menestyksen tuoma sokeus toimintojen kriittiselle tarkastelulle. Tällöin riskinä on, ettei tapahtuneesta opita riittävästi, vaan tuudittaudutaan tyytyväisyyteen hyvin tehdystä työstä. Vaikka systeemin resilienssi on tässä tapauksessa korkealla tasolla, resilienssin suurin uhka on sisäinen, kehittämisprosessin heikentyminen sekä kriittisen tarkastelun puute. ”*Oppimiskyvyn puute itsessään on systeemissä piilevä latentti haavoittuvuus, jonka vaikutukset paljastuvat kenties jo seuraavalla kerralla ongelmien triggeröidyttyä. Voi myös olla, että tällä kertaa koettu tilanne oli luonteeltaan sellainen, jonka hoitaminen ei lopulta vaatinut erityistä viranomaisyhteistyötä – tilanne saattoi olla palasteltavissa kyberhyökkäyksen, informaatiovaikuttamisen ja fyysisen iskun elementeiksi. Ensi kerralla kohdattava ongelma saattaa olla huomattavasti systeemisempi, erilaisia rajoja ylittävä sotku, jonka palasteleminen sektorikohtaisten toimivalta-alueiden viipaleiksi vain pahentaa tilanteen hoitamisen edellytyksiä*.” (Asiantuntija A)

7.2.2 Skenaario 2: Negaatio

Skenaario 2 on käänteinen eli negaatio skenaariolle 1 (Toivottu skenaario). Tässä skenaariossa tarkastellaan skenaarion muuttujia silloin, kun ulkoiset muuttujat saavat aikaan systeemissä ei-haluttuja vaikutuksia aikaiseksi. Negaatiota voidaan kutsua myös termillä *worst-case-scenario*. Skenaarion 2 muuttujat ja vaikutukset on kuvattu taulukossa 6.

VAIKUTIN	TOIMINTA	VAIKUTUSTEN ARVIOINTI
Kyberhyökkäykset	Hyökkäystä ei havaita ollenkaan tai se havaitaan liian myöhään. Torjuntatoimet ovat riittämättömiä ja/tai vääriä. Viranomaisverkko ei toimi GSM-verkkovikoja Systeemi ei paikallista sen lamauttavaa vikaa/vikoja	Järjestelmät ei-käytettävissä. Ongelmia kommunikaatio-yhteyksissä. systeemin sisäinen viestintä vaikeutuu. Tilannekuvan muodostaminen vaikeutuu. Operatiivinen johtaminen vaikeutuu.
informaatiovaikuttaminen	Valeuutisten leviäminen medioissa Systeemin maalittaminen Systeemin painostaminen luopumaan toimenpiteistä Systeemin itsenäinen päätöksenteko kärsii	Systeemin uskottavuus ja luotettavuus kärsii Kansalaisten tuen puute yhteiskuntaa kohtaan lisääntyy
Fyysinen isku	Tunkeutujia ei kyetä pysäyttämään, eikä niiden toimintaa keskeyttämään	Yhteiskuntarauhan muutokset Yhteiskunnan turvallisuuden uskottavuus kärsii Sisäisen turvallisuuden uhka kasvaa merkittävästi.

TAULUKKO 6: Skenaario 2, negaatio

Tässä skenaariossa systeemin havainnointi- ja torjuntakyky ulkopuoliselle toiminnalle on puutteellista. Systeemi ei ole kyennyt jo varhaisessa vaiheessa havaitsemaan sellaisia varoittavia signaaleja, jotka saattaisivat enteillä tulevaa toimintaa. Tämän lisäksi havainnoinnissa jo alkaneessa tilanteessa on ollut puutteita, eikä tarvittavia torjuntatoimenpiteitä ole kyetty aloittaman riittävän ajoissa. Systeemi ei kykene muodostamaan riittävää tilannekuvaa tapahtumista, ja sen sisäinen viestintä on ollut rajoittunutta, sekä se on lopulta lamaantunut ulkopuolisista syistä.

Systeemi on lähellä hetkeä tulla toimintakyvyttömäksi kokonaan ja osia sen toiminnoista on jo toimintakyvyttöminä. Sen uskottavuus yhteiskunnan silmissä kärsii, joka saattaa johtaa kansalaisten tuen puutteeseen ja yleisen mielipiteen kääntymiseksi sitä vastaan. Tätä voidaan osaltaan myös pitää

yhtenä informaatiovaikuttamisen tavoitteena. Informaatiovaikuttamisen tavoitteena on myös luoda hajaannusta systeemin sisälle jakamalla virheellistä informaatiota, joka voi vaikuttaa systeemin tilannekuvaan vääristävästi. Tämä voi johtaa virheelliseen analyysiin ja päätöksentekoon. Asiantuntija C:n mukaan systeemin vahvuus on kuitenkin sen perusosaaminen, peruskonsepti kokonaisturvallisuudesta, joka antaa pohjan johtamiselle. *"Kokonaisturvallisuuden konsepti olemassa – antaa perusteita johtamiselle "* (Asiantuntija C).

Asiantuntija A:n ja asiantuntija B:n mukaan systeemillä on heikosta tilanteesta riippumatta potentiaalisia mahdollisuuksia suorituskykynsä parantamiseen. *"Mahdollisuus oppia tapahtuneesta ja kehittää tilannekuvan kokoamista"* (Asiantuntija B). Molempien mukaan systeemin mahdollisuus on oppimisessa ja uusien ajattelu- ja toimintamallien kehittämisessä. Toisaalta oppimiseen sisältyy myös uhka, mikäli systeemiä kohdanneesta vastoinkäymisestä ei oteta oppia tai ne analysoidaan väärin.

Hetkellisesti systeemin resilienssi on tällä hetkellä heikko, mutta vastoinkäymiset ovat mahdollisuuksia kehittää resilienssiä, mikäli niitä pystytään kriittisesti tarkastelemaan riittävän rehellisesti. Tässä tapauksessa systeemillä on mahdollisuus kehittää resilienssiä jopa paremmin, kuin skenaariossa 1, jossa uhkana oli kritiikitön analyysi tapahtumien kulkuun. Asiantuntija A:n mukaan systeemillä on mahdollisuus ajatella myös laatikon ulkopuolelta, joka voi tuoda sillä uusia toiminnallisia mahdollisuuksia. *"Ylipäätään osaamista ja erilaisia kyvykkyyksiä saattaisi olla käytettävissä viranomaisorganisaation ulkopuolella. Tällaisten resurssien valjastaminen vaatii jonkinlaista joustamista perinteisen byrokraattisen ja hierarkkisen toimintamallin kohdalla."* (Asiantuntija A). Systeemin resilienssin heikentyessä, heikentyy myös koko yhteiskunnan resilienssi. Systeemi, joka vastaa yhteiskunnan kokonaisturvallisuudesta, halvaantuessaan voi syöstää yhteiskunnan kriisiin.

Systeemillä ei ole tässä vaiheessa tiedossa, mihin tunkeutujat pyrkivät. Toisaalta tällöin systeemin sisällä tiedostetaan se tosiasia, että tiedetään, ettei tätä seikkaa vielä tiedetä. Tieto siitä, mitä ei tiedetä on systeemille mahdollisuus.

7.2.3 Skenaario 3: Kybervaikuttaminen

Skenaariossa 3 tarkastellaan muutoksia systeemin tilassa silloin, kun siihen kohdistuva kybervaikuttaminen onnistuu haittaamaan systeemin toimintaa. Skenaariossa systeemiin kohdistuvat kyberhyökkäykset vaikuttavat sen toimintaan, haittaamalla tietojärjestelmien toimintaa, järjestelmien käyttämistä johtamisen työkaluna, sekä haittaavat viestintäyhteyksiä. Vaikka systeemi havaitsee siihen kohdistuvia kyberhyökkäyksiä, sen toimet niiden torjumiseen

eivät ole riittäviä tai oikea-aikaisia. Skenaarion muuttujat ja niiden vaikutukset on kuvattu alla taulukossa 7.

VAIKUTIN	TOIMINTA	VAIKUTUSTEN ARVIOINTI
Kyberhyökkäykset	Hyökkäystä ei havaita ollenkaan tai se havaitaan liian myöhään. Torjuntatoimet ovat riittämättömiä ja/tai vääriä. Viranomaisverkko ei toimi GSM-verkkovikoja Systeemi ei paikallista sen lamauttavaa vikaa/vikoja	Järjestelmät ei-käytettävissä. Ongelmia kommunikaatio-yhteyksissä. systeemin sisäinen viestintä vaikeutuu. Tilannekuvan muodostaminen vaikeutuu. Operatiivinen johtaminen vaikeutuu..
Informaatiovaikuttaminen	Kontrolloidut toimet yhdessä median kanssa valeuutisten korjaamiseksi Resurssien keskittäminen suunnitelmalliseen disinformaation torjutaan Havaittuihin ilmiöihin puututaan välittömästi	Ei merkittävää vaikutusta systeemin toimintaa sisäisesti Vahvistaa systeemin luottamusta yhteiskunnassa ja kansalaisten keskuudessa
Fyysinen isku	Yhteistoiminnalla tunkeutujat paikallistetaan ja otetaan hallitusti kiinni	Yhteiskuntarauhan ja luottamuksen vahvistaminen Kyky torjua fyysinen uhka ulkoapäin vahvistuu kokemuksen ja oppimisen myötä.

TAULUKKO 7: Skenaario 3, kyberhyökkäykset

Systeemin toiminnot, viestintä ja elementit ovat vahvasti riippuvaisia teknologiasta. Sen päätöksentekokyky nojaa vahvasti päivittyvään tilannekuvaan. Kattava tilannekuva kootaan pääsääntöisesti hyödyntämällä systeemin kyberulottuvuutta, tietoverkkoja. Systeemin heikkoutena on sen vahva riippuvuus tietoverkoista ja niiden toiminnasta. Samalla se muodostaa systeemille operatiivisen uhan. Tietoverkot mahdollistavat systeemissä nopean tiedonsiirron ja tilannekuvan päivittymisen. Tilannekuvaa voidaan päivittää myös ilman tietoverkkoja, käyttämällä vaihtoehtoisia tapoja. Ongelmaksi

muodostuvat elementit, jotka ovat kaukana toisistaan ja tiedon välittäminen niiden välillä edellyttää tietoverkkoja. Tällöin vaihtoehtoisin menetelmin voidaan siirtää rajatumpi määrä informaatiota, mahdollisesti hitaammin ja tilannekuva keskittyy vain kriittisiin tapahtumiin. Samalla systeemiltä katoaa rajallisen tilannekuvan ympäriltä kokonaiskuva, jossa saattaa esiintyä sellaisia syötteitä tai heikkoja signaaleja, joiden havaitseminen olisi mahdollistanut riittävän aikaisen reagoinnin.

Systeemi resilienssi on heikentynyt. Sillä on kuitenkin mahdollisuus kehittää resilienssillä analysoimalla kriittisesti niitä toimintoja, joissa systeemin toimintaan pystyttiin vaikuttamaan ulkoapäin ei-halutulla toiminnalla. Asiantuntija A:n mielestä tilanne on erityisesti johtamisen näkökulmasta erinomainen oppimistilanne. ”*Kaiken kaikkiaan tällainen koettelemus on hyvä oppitunti, jos se ymmärretään ottaa oppimiskokemuksena*” (Asiantuntija A). Asiantuntija B:n mukaan systeemin uhkana on, että se keskittyy pelkästään suojaustoimiin eikä systeemin sisällä muisteta dokumentoida uhkia ja niissä toimimista systeemin kehityksen näkökulmasta.

Systeemin toiminnan kannalta on positiivista, että se pystynyt pitämään operatiivisen toimintavalmiuden ja -kyvyn yllä, vaikka systeemin tietoverkottunut osa on ollut osin lamaantuneena. Se kertoo, että systeemillä on jo olemassa vaihtoehtoisia tapoja viestiä sisäisesti ja kyky ottaa sellaisia menetelmiä nopeasti käyttöön. Lisäksi systeemillä on ollut havainnointikyky informaatiovaikuttamisen osalta hyvällä tasolla. ”*Viranomaiset ovat terästäytyneet informaatiovaikuttamisen osalta. Se on itsessään jonkinlainen merkki siitä, että systeemin johtamisessa eletään toimintaympäristön muutosten virrass*a” (Asiantuntija A). Systeemi on selkeästi valmistautunut informaatiovaikuttamiseen ja sillä on ollut kyky vastatoimiin riittävän nopealla reagoinnilla.

7.2.4 Skenaario 4: Fyysinen isku ja informaatiovaikuttaminen

Tässä skenaariomallissa yhteiskuntaan kohdistuva fyysinen uhka konkretisoituu systeemin aktiivisista toimista huolimatta, eikä systeemi kykene torjumaan tai rajoittamaan yhteiskunnan turvallisuuteen kohdistuvaa uhkaa. Tämän lisäksi systeemiin toimintaan yritetään vaikuttaa informaatiovaikuttamisen keinoin. Systeemin vaikuttimet ja toiminnat on kuvattu taulukossa 8.

VAIKUTIN	TOIMINTA	VAIKUTUSTEN ARVIOINTI
Kyberhyökkäykset	Havainto hyökkäyksestä Torjuntatoimet oikea-aikaiset Viranomaisverkko saadaan palautettua operatiiviseen toimintaan tai varajärjestelmät otettua käyttöön GSM-yhteyksien viat saadaan korjattua	Operatiivinen toimintavalmius järjestelmien suhteen saadaan pidettyä yllä (CIA) Tilannekuva säilyy Johtaminen teknisin menetelmin mahdollista Sisäinen viestintä teknisin menetelmin mahdollista
Informaatiovaikuttaminen	Valeuutisten leviäminen medioissa Systeemin maalittaminen Systeemin painostaminen luopumaan toimenpiteistä Systeemin itsenäinen päätöksenteko kärsii	Systeemin uskottavuus ja luotettavuus kärsii Kansalaisten tuen puute yhteiskuntaa kohtaan lisääntyy
Fyysinen isku	Tunkeutujia ei kyetä pysäyttämään, eikä niiden toimintaa keskeyttämään	Yhteiskuntarauhan muutokset Yhteiskunnan turvallisuuden uskottavuus kärsii Sisäisen turvallisuuden uhka kasvaa merkittävästi.

TAULUKKO 8: Skenaario 4, luvaton tunkeutuminen ja informaatiovaikuttaminen

Tässä skenaariossa systeemi ei kykene torjumaan yhteiskuntaan ja systeemiin itseensä kohdistuvaa uhkaa. Lisäksi informaatiovaikuttaminen systeemin toimintaan kohtaan onnistuu. Onnistunut informaatiovaikuttaminen ja fyysinen uhka yhdessä aiheuttavat epävarmuutta systeemin sisällä, sekä sen ympärillä yhteiskunnassa ja kansalaisissa. Epävarmuus ja viranomaisiin kohdistuva luottamuksen lasku on omiaan lisäämään turvattomuutta koko yhteiskunnassa. Toimivan informaatiovaikuttamisen viheliäisiä puolia on, että se mahdollisesti laskee kansalaisten luottamusta systeemin. Toimiakseen tehokkaasti, systeemin menestyksen edellytyksenä on nauttia yhteiskunnan ja kansalaisten tukea.

Systeemin ehdottomia vahvuuksia on sen kyberkyvykkyyden suojaaminen ja ylläpito. ”*Kokonaisturvallisuuden konsepti olemassa – antaa perusteita johtamiselle - Vähintään tyydyttävä kyky johtaa sektoreittain (ei kokonaisuutta) kyberpuolustusta*” (Asiantuntija C). Tämä edesauttaa reaaliaikaisen

tilannekuvan ylläpitoa, sekä mahdollistaa tehokkaan päätöksenteon. Toimivat tietoverkot ja laitteet mahdollistavat systeemille nopean palautumisen fyysisestä iskusta, mikäli systeemi kykenee käyttämään vaihtoehtoisia toimintamalleja.

Tilannekuvan luotettavuus voi kärsiä tilanteessa, jossa informaatiovaikuttamisella kyetään vaikuttamaan systeemiin ulkoapäin. Näissä tilanteissa tilannekuvan päivittämisen yhteydessä kerättyyn informaatioon joudutaan suhtautumaan kriittisesti, joka hidastaa tilannekuvan muodostamista, sekä päätöksentekoa systeemin sisällä. ”*Koska valeinformaation vaikutus alkaa olla vallitsevaa, on myös tilannekuvan muodostaminen ja ylläpitäminen haasteellista. Yhtäältä siis ”tilannekuva säilyy”, kuten kuvauksessa kerrotaan, mutta se viitekehys, minkä puitteissa tilannekuvaa muodostetaan, alkaa käydä laadullisesti arvelluttavaksi*” (Asiantuntija A). Informaatiovaikuttamisella systeemistä saadaan levitettyä valheellista tietoa, joka on omiaan laskemaan sen uskottavuutta yhteiskunnan silmissä. Samalla informaatiovaikuttaminen saa aikaan epäilyksiä systeemin toiminnan kyvykkyydestä sekä toiminnan lainmukaisuudesta, sitä ulkoapäin tarkasteltaessa. Systeemin mahdollisuutena on se, että, informaatiovaikuttamiseen liittyvä pohjatyö yhteiskunnassa on vuosikymmenien kuluessa tehty hyvin. Viranomaisilla on yhteiskunnassa hyvä maine ja niitä pidetään lähtökohtaisesti luotettavina. ”*Onneksi luottamuksen lähtötaso viranomaisiin nähden on vahvalla pohjalla, joten informaatiovaikuttamisella ei kovinkaan helposti pystytä sitä olennaisesti romahduttamaan*” (Asiantuntija A). Tämä on merkittävä vahvuus informaatiovaikuttamista torjuttaessa. ”*Tilanteesta voidaan oppia ja viedä opittuja taitoja käytäntöö*n” (Asiantuntija B). ”*Johtamiselle tarjoutuu oppimismahdollisuuksia, sillä tämänkaltaista informaatiovaikuttamisen tehokkuutta ei välttämättä ole ennen nähty*” (Asiantuntija A).

7.3 Resilienssin analysointi

Resilienssi kyber-fyysisessä sosiaalisessa systeemissä koostuu useasta eri osasta. Kuten aiemmin on havaittu systeemi ei ole sen osiensa summa, eikä näin voida sanoa myöskään resilienssistä. Resilienssiin vaikuttaa systeemin jo olemassa oleva kyky torjua siihen kohdistuvia uhkia, kyky kehittää toimintaansa ja implementoida niitä käyttöön. Tutkimuksessa saatujen tulosten perusteella havaittiin että, systeemin oppimisen voidaan katsoa olevan erittäin merkittävässä roolissa resilienssiä lisäävänä tekijänä systeemissä. Tutkimuksessa nousi esiin systeemin kyky tarkastella kriittisesti sen toimintoja ja varsinkin niitä toimintoja, joissa systeemin kyvykkyys on ollut korkeammalla. Kriittisen tarkastelun puuttuminen saattaa johtaa kaikkivoipaisuuden tunteeseen, että kyseinen osa-alue systeemissä on kunnossa jatkossakin, vaikka sen kyky on riittänyt vain käynnissä olleen tapahtuman hoitamiseen. Kriittisen tarkastelun

puuttuessa systeemiltä voi jäädä havaitsematta uudenlaisia uhkia, joille se saattaa olla haavoittuvainen tai löytää heikkoja kohtia itsestään.

Useamman kerran asiantuntijoiden vastauksissa nousi esiin systeemin menestys uhkana. Menestystä lähestyttiin siitä näkökulmasta, onko systeemi menestyksestään huolimatta jo suorituskykynsä äärirajoilla. Mikäli tämä seikka kyetään systeemissä havaitsemaan kriittisessä tarkastelussa, on se tällöin systeemille mahdollisuus korottaa kykyään.

Resilienssin rakentaminen ja kehittäminen edellyttää systeemiltä kykyä havainnointikykyä ja torjumiskykyä, mutta myös havainnointia edeltävää kehitystyötä tarkastella kriittisesti kaikki systeemin toimintoja, sekä niiden kyvykkyyttä tulevaisuudessa. Työkaluina tällaisessa voi käyttää esimerkiksi skenaarioanalyysiä, jolla voidaan havaita systeemissä olevia heikkouksia tai uhkia. Tärkeää on havaita myö systeemin vahvuudet, jottei korjaavilla toimenpiteillä niitä vahingossa heikennettäisi. Lisäksi systeemin tulisi osata kriittisesti arvioida sitä, millaista tietoa ja osaamista se pitää sisällään. Koko systeemillä tulee olla käsitys siitä, millaista tietoa systeemissä on.

7.3.1 Asiantuntijahaastattelun SWOT-analyysin yhteenveto

Tutkimukseen osallistuneiden asiantuntijoiden näkemykset olivat kaikissa skenaarioissa melko samansuuntaisia. Merkittävänä tekijänä asiantuntijat korostivat oppimisprosessin tärkeyttä resilienssin kehittäjänä. Heidän näkemyksensä mukaan systeemin menestys koettiin jopa uhkana systeemin resilienssin kehittämisen näkökulmasta. Asiantuntijat arvioivat menestyksen pahimmillaan johtavan systeemin toiminnan kritiikittömään tarkasteluun, joka on selkeä uhka oppimiselle ja kehittämiselle. Toisin päin käännettynä systeemiä kohtaavat vastoinkäymiset ovat systeemin mahdollisuuksia oppia, kehittää ja menestyä.

Johtamista ja jatkuvaa tilannekuvan ylläpitoa pidettiin kaikkien asiantuntijoiden keskuudessa tärkeänä. Tilannekuvaa pidettiin nimenomaisesti tehokkaan operatiivisen johtamisen työkaluna. Tämän vuoksi tilannekuvan ylläpitäminen tulisi turvata myös poikkeusoloissa.

Resilienssin kannalta on merkityksellistä, että systeemillä on jo olemassa perusrakenteet ja -toiminnot uhkien torjumiseen. Toiminta on siis suunniteltua ja jokaisella systeemin osalla on ennalta määriteltyjä vastuita ja tehtäviä. Kun systeemin selkäranka on kunnossa, sen palautuminen on nopeampaa.

Kybertoiminnallisuuksista huolehtiminen osa kyber-fyysisen systeemin selkärangasta huolehtimista. Tilannekuvan ylläpito ja johtaminen nojaa pitkälti tietoverkkoihin. Tietoverkkoihin kohdistuu omanlaisia uhkia, joiden tunnistaminen ja niihin valmistautuminen on avainasemassa.

8 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä luvussa esitettään yhteenvetona tutkimuksen tulokset, sekä kuvataan tutkimuksen luotettavuutta ja tutkimuksen tulosten tarkkuutta. Lopuksi esitellään tutkimukselle mahdollisia jatkotutkimusaiheita.

8.1 Reliaabiliteetti ja validiteetti

Tutkimuksen reliabilius ja validiuden määrittelevät, onko tutkimuksen tuloksista johdetut päätelmät luotettavia ja toistettavissa. Eskolan (1998) mukaan kvalitatiivisessa tutkimuksessa aineiston analyysivaiheen ja luotettavuuden arviointi ei ole yhtä selkeästi erotettavissa, kuin kvantitatiivisessa tutkimuksessa. Eskolan mukaan kvalitatiivisen tutkimuksen tekijöitä onkin usein kritisoitu juuri luotettavuuskriteerien epämääräisyydestä. Kuitenkin tutkimuksen luotettavuuden arviointi on tieteen tekemisen kannalta erittäin merkityksellistä ja sen tarkoituksena on Eskolan mukaan vakuuttaa epäilevää tiedeyhteisöä. Puolimatkan (2002) mukaan kvantitatiivisen ja kvalitatiivisen tutkimuksen totuuskäsitys on sama, vaikka niissä luotettavuuden kriteerejä sovelletaan osittain eri tavoin. Puolimatkan mukaan kvalitatiivinen tutkimusmenetelmä ei itsessään ole syy luopua totuuden käsitteestä. Tällä Puolimatka tarkoittaa, että kvalitatiivisellakin tutkimuksella voidaan etsiä realistista totuutta, vaikka menetelmät sen löytämiseksi ovat erilaiset kuin kvantitatiivisessa tutkimuksessa. Kvalitatiivisessa tutkimuksessa totuuden korrespondessiteorian vastaavuutta voidaan etsiä tutkittavien kohteiden tai ilmiöiden käsityksistä, aikomuksista ja sosiaalisesta vuorovaikutuksesta. (Eskola, 1998, s. 151; Puolimatka, 2002, s. 467.)

Tutkimuksen validiuden arvioinnilla tarkoitetaan sitä, miten tutkimuksessa käytetty analyysimenetelmä (tässä tutkimuksessa skenaarioanalyysi) vastaa sitä menetelmää miten systeemin toimintaa tulisi tutkia. Tutkimuksen reliabiliteetillä tarkoitetaan sitä, että tutkimuksen tulokset ovat toisinnettavissa. (Hirsjärvi, Remes ja Sajavaara, 2009, s. 231-232.)

Tutkimuksessa on kyseessä tulevaisuudentutkimus, jossa tutkittavan systeemin toimintaa tulevaisuudessa ei voida 100 prosenttisella varmuudella

todentaa, mutta siitä voidaan analysoimalla tehdä luotettavia skenaariomalleja, joita kerätyn tiedon perusteella voidaan pitää mahdollisina. Skenaarioanalyysin avulla voidaan tehdä tarkkojakin johtopäätöksiä siitä, kuinka systeemi käyttäytyisi tai muuttuisi eri indikaattoreiden avulla. Tutkimuksen toistettavuuteen sisältyy problematiikkaa. Koska tutkimuksessa huomioidaan useiden indikaattorien muodosta tapahtumaketju, on tutkimus toistettavissa ainostaan silloin, kun nämä indikaattorit säilyvät joka kerralla muuttumattomina. Tässä tutkimuksessa luotettavuutta tarkastellaan toistettavuuden kannalta skenaarioanalyysissä luomalla 4 erilaista tulevaisuuden kuvaa. Skenaarioanalyysi itsessään on aina toistettavissa, mutta sen lopputulokseen vaikuttavat aina ulkoiset tekijät, jolloin sitä ei voida tulosten valossa toistaa samanlaisena.

Tutkimuksen toistettavuuden kannalta skenaarioanalyysissä luodaan useampia tulevaisuuden kuvia, välttääkseen ennalta määriteltyjä tuloksia. Tässä tutkimuksessa tulosten reliabilius vahvistetaan asiantuntijahaastattelulla, jossa skenaarioanalyysin tuloksia koetellaan asiantuntijoiden näkemyksillä tutkimuksen tuloksista.

8.2 Tulosten pohdinta

Tutkimuksessa kävi ilmi, että systeemin resilienssi on riippuvainen sen eri elementtien kyvykkyydestä, vaikka systeemi ei olekaan osiensa summa. Hyvin pienet muutokset systeemin osien kyvykkyydessä toimia, vaikuttavat systeemin toimintaan kokonaisuudessaan ja tekevät siitä osin haavoittuvan.

Resilienssi on kyky havainnoida ja torjua uhkia, palautua ja oppia niistä. Tutkimuksessa havaittiin, että systeemin menestys nojaa sen kykyyn oppia. Toisaalta systeemin menestys on uhka sen oppimiselle. Systeemiä kohdanneet vastoinkäymisten havaittiin olen parhaita oppimisen kannalta. Toisaalta systeemiä ei voi suunnitella epäonnistumaan vain sen vuoksi, että se oppisi. Tutkimuksessa havaittiin, että vastoinkäymiset ovat parhaita oppimistapahtumia ja menestys vaatii kriittistä tarkastelua menestykseen johtaneista seikoista. Merkittävimpänä löytönä tutkimuksessa on oppimisen ja sen implementoinnin merkitys systeemin resilienssin kehityksessä. Kaikissa asiantuntijahaastatteluissa asiantuntijat korostivat systeemin oppimiskykyä merkittävänä systeemin resilienssin kehittäjänä. Lisäksi oppimisen jalostaminen tiedoksi havaittiin kriittiseksi tekijäksi resilienssin kehittämisen kannalta.

Systeemin kyky joustaa ja muuttaa tarvittaessa muotoaan on sen vahvuuksia resilienssiä ajatellen. Tutkimuksessa havaittiin, että toimimalla avoimen systeemin tavoin, systeemi voi omistaa ja luovuttaa tarpeen mukaan niitä elementtejä, joita se toiminnassaan tarvitsee tai vastavuoroisesti ei tarvitse. Systeemin avoimuus on teoriatasolla systeemin ehtymättömän resurssitarpeen

ylläpitäjä. Reaalimaailmassa resurssien siirtäminen ja lisääminen systeemiin ei käy kuitenkaan yhtä helposti, kuin teoriassa.

8.3 Jatkotutkimusaiheet

Tutkimuksessa analysoitiin resilienssiä systeemissä tietyssä pisteessä. Jatkotutkimuksena olisi mielenkiintoista selvittää, miten oppimisprosessia voitaisiin hyödyntää resilienssin kehittämisessä systeemitasolla. Lisäksi merkityksellistä olisi tutkia voitaisiinko oppimisprosessi implementoida osaksi systeemin sisäisin prosesseja, jolloin se olisi jatkuva prosessi kaiken taustalla.

LÄHTEET

Alasuutari, P. & Alasuutari, P. (2012). *Laadullinen tutkimus 2.0*. Tampere: Vastapaino.

Alastalo, M., Åkerman, M. & Vaittinen, T. (2017). Asiantuntijahaastattelu. Teoksessa Hyvärinen, M., Nikander, P., Ruusuvuori, J. & Granfelt, R. (2017). Tutkimushaastattelun käsikirja. Tampere: Vastapaino.

Amer, M., Daim, T. U., Jetter, A. (2013). A review of scenario planning. Futures, 46, p. 23. Haettu 12.1.2018 osoitteesta: https://doi.org/10.1016/j.futures.2012.10.003

Andress, J., & Winterfeld, S. (2014). Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners (Vol. Second edition). Waltham, Massachusetts: Syngress. Haettu 13.1.2019 osoitteesta: http://search.ebscohost.com.ezproxy.jyu.fi/login.aspx?direct=true&db=nlebk&AN=558253&site=ehost-live

Belliger, A. (2016). Organizing Networks: An Actor-Network Theory of Organizations. Bielefeld, GERMANY: transcript Verlag. Haettu 13.1.2018 osoitteesta: http://search.ebscohost.com.ezproxy.jyu.fi/login.aspx?direct=true&db=nlebk&AN=1402751&site=ehost-live

Bood, R. (1997). Strategic learning with scenarios. European Management Journal, 15(6), pp. 633-647. Haettu 18.1.2019 osoitteesta: https://ac-els-cdncom.ezproxy.jyu.fi/S0263237397000479/1-s2.0-S0263237397000479-main.pdf?_tid=5a7f2692-bedd-43de-895fa7cbee1b9dcf&acdnat=1547790507_538e3149212d54b3fc4c812d7b586dcd

Carroll, N., Richardson, I., & Whelan, E. (2012). Service science: An actor-network theory approach. International Journal of Actor-Network Theory and Technological Innovation (IJANTTI), 4(3), s. 51-69. Haettu 3.1.2018 osoitteesta: https://doi.org/10.4018/jantti.2012070105

Eidelson, R. J. (1997). Complex adaptive systems in the behavioral and social sciences. *Review of General Psychology, 1*(1), s. 42-71. Haettu 18.1.2018 osoitteesta: https://doi.org/10.1037/1089-2680.1.1.42

Eskola, J. (1998). *Johdatus laadulliseen tutkimukseen*. Tampere: Vastapaino.

Giezen, M., Salet, W., & Bertolini, L. (2015). Adding value to the decision-making process of mega projects : Fostering strategic ambiguity, redundancy, and resilience. *Transport Policy, 44*, s. 169-178. Haettu 19.3.2018 osoitteesta: https://doi.org/10.1016/j.tranpol.2015.08.006

Glouberman, S., & Zimmerman, B. (2016). Complicated and complex systems: What would successful reform of medicare look like? Changing health care in canada (s. 21-53). Toronto: University of Toronto Press. Haettu 24.1.2018 osoitteesta http://www.pol.una.py/cursosverano/images/2013/files/Complicated_Systems_ZimmermanReport.pdf

Hirsjärvi, S., Remes, P., Sajavaara, P. & Sinivuori, E. (2009). *Tutki ja kirjoita* (15. uud. p.). Helsinki: Tammi.

Hsia, P., Samuel, J., Gao, J., Kung, D., Toyoshima, Y. & Chen, C. (1994). Formal approach to scenario analysis. *IEEE Software, 11*(2), s. 33-41. Haettu 28.11.2017 osoitteesta http://ieeexplore.ieee.org.ezproxy.jyu.fi/stamp/stamp.jsp?tp=&arnumber=268953

Holland, J. (2006). Studying complex adaptive systems. *Journal of Systems Science and Complexity, 19*(1), s. 1-8. Haettu 17.1.2018 osoitteesta: https://doi.org/10.1007/s11424-006-0001-z

Hyvä elämä – turvallinen arki (2017). Valtioneuvoston periaatepäätös sisäisen turvallisuuden strategiasta 5.10.2017. Sisäministeriön julkaisu 15/2017, Helsinki. 52 s.

Hyvönen, A-E. & Juntunen, T. (2016) Sopeutuva yhteiskunta ja resilienssi: turvallisuuspoliittinen analyysi. *Polisiikka-lehti, 58(3), s. 206-223.*

Johnson-Laird, P. (1999). Deductive reasoning. Annual Review of Psychology, 50, 109-35. Haettu 6.12.2018. https://search-proquest-com.ezproxy.jyu.fi/docview/205846913?accountid=11774

ITU-T (2008) X.1205: Overview of cybersecurity. ITU-T Recommendations, X Series: Data Networks, Open System Communications and Security. International Telecommunication Union (ITU) vol. 4/2008. Haettu 8.1.2018 osoitteesta: http://www.itu.int/rec/T-REC-X.1205-200804-I

Kamppinen, M., Malaska, P. & Kuusi, O. (2002). Tulevaisuuden tutkimuksen peruskäsitteet. Teoksessa Kamppinen, M., Kuusi, O. & Söderlund, S. Tulevaisuudentutkimus: Perusteet ja sovelluksia, 17-53. Helsinki: Suomalaisen Kirjallisuuden Seura.

Kast, F. & Rosenzweig, J. (1972). General systems theory: Applications for organization and management. *The Academy of Management Journal, 15*(4), s. 447-465. http://doi.org/10.2307/255141

Kihlstrom, A. (2012). Luhmann's system theory in social work: Criticism and reflections. Journal of Social Work, 12(3), s. 287-299. Haettu 27.12.2017 osoitteesta: http://doi:10.1177/1468017310386425

Kuusisto T., Kuusisto R. (2015) *Cyber World as a Social System*. Julkaisussa: Lehto M., Neittaanmäki P. (eds) *Cyber Security: Analytics, Technology and Automation. Intelligent Systems, Control and Automation: Science and*

Engineering, vol 78. Springer, Cham. Haettu 3.1.2018 osoitteesta: https://doi.org/10.1007/978-3-319-18302-2_2

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford ; New York: Oxford University Press. Haettu 19.2.2018 osoitteesta: https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=422646

Leinonen, M., Otonkorpi-Lehtoranta, K. & Heiskanen, T. (2017) Teoksessa: Hyvärinen, M., Nikander, P., Ruusuvuori, J. & Granfelt, R. (2017) Tutkimushaastattelun käsikirja. Haettu 20.1.2019 osoitteesta: https://www.ellibslibrary.com/reader/9789517686112

Liu, Z. (2011). *Cyber-Physical-Social Systems for Command and Control*. *Intelligent Systems, IEEE, 26*(4), s. 92-96. Haettu 12.12.2017 osoitteesta: https://doi.org/10.1109/MIS.2011.69

Longstaff, P., Armstrong, N. J., Perrin, K., Parker, W. M. & Hidek M. A. (2010). *Building Resilient Communities: A Preliminary Framework for Assessment.* Homeland Security Affairs, 6(3), . Haettu 16.3.2018 osoitteesta: https://search-proquest-com.ezproxy.jyu.fi/docview/1266215222?accountid=11774

Luhmann, N., Bednarz, J., Jr. & Baecker, D. (1995). *Social systems*. Stanford (CA): Stanford University Press.

Luhmann, N., Baecker, D. & Gilgen, P. (2013). *Introduction to systems theory*. Cambridge: Polity Press.

Malaska, P., Malmivirta, M., Meristö, T., Hansén, S.-O. (1984). Scenarios in Europe—Who uses them and why? Julkaisussa: Long Range Planning, 17(5), s. 45-49. Haettu 6.4.2018 osoitteesta: https://doi.org/10.1016/0024-6301(84)90036-0

Mannermaa, M. (2004). *Heikoista signaaleista vahva tulevaisuus*. Helsinki: WSOY.

Mohay, G., Ahmed, E., Bhatia, S., Nadarajan, A., Ravindran, B., Tickle, A.B., & Vijayasarathy, R. (2011). Detection and Mitigation of High-Rate Flooding Attacks. Teoksessa: *Flooding AttacksAn Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection.* India: Springer India. Haettu 19.5.2018 osoitteesta: https://link-springer-com.ezproxy.jyu.fi/book/10.1007%2F978-81-322-0277-6

Pickton, D. W., & Wright, S. (1998). What's swot in strategic analysis? Strategic Change, 7(2), 101-109.

Poisel, Richard A.. Information Warfare and Electronic Warfare Systems, Artech House, 2013. ProQuest Ebook Central, Haettu 13.1.2019 ositteesta: https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=1455537.

Puolimatka, T. (2002). *Kvalitatiivisen tutkimuksen luotettavuus ja totuusteoriat.* Kasvatus : Suomen kasvatustieteellinen aikakauskirja, *33*(5).

Rubin, A. (2015). *Skenaariotyöskentely Tulevaisuuksientutkimuksessa*. Haettu 27.11.2017 osoitteesta https://metodix.fi/2015/01/31/skenaariotyoskentely-tulevaisuuksientutkimuksessa/#Skenaarion%20kaksi%20merkityst%C3%A4

Rumsfeld, D., H. (2002). Yhdysvaltain puolustusministeri 2001–2006. Yhdysvaltaltain puolustusministeriön lehdistötilaisuudessa Pentagonissa 12.2.2002.

Ruusuvuori, J. & Tiittula, L. (2017) Tutkimushaastattelu ja vuorovaikutus. Teoksessa: Hyvärinen, M., Nikander, P., Ruusuvuori, J. & Granfelt, R. (2017) Tutkimushaastattelun käsikirja. Haettu 20.1.2019 osoitteesta: https://www.ellibslibrary.com/reader/9789517686112

Schneider, M., & Somers, M. (2006). *Organizations as complex adaptive systems: Implications of complexity theory for leadership research*. *The Leadership Quarterly, 17*(4), s. 351-365. Haettu 4.1.2018 osoitteesta: https://doi.org/10.1016/j.leaqua.2006.04.006

Schoemaker, P., H., J. (1993). Multiple scenario development: Its conceptual and behavioral foundation. Strategic Management Journal, 14(3), 193-213. Haettu 19.1.2019 https://search-proquestcom.ezproxy.jyu.fi/docview/231161993?accountid=11774

Simmons, A., & Yoder, L. (2013). *Military resilience: A concept analysis*. Nursing Forum, 48(1), 17-25. Haettu 10.1.2018 osoitteesta: https://doi-org.ezproxy.jyu.fi/10.1111/nuf.12007

Skyttner, L. (2005). General Systems Theory: Problems, Perspectives, Practice (2nd Edition). Hackensack, NJ: World Scientific.

Smirnov, A., Kashevnik, A., & Shilov, N. (2015). Cyber-physical-social system self-organization: Ontology-based multi-level approach and case study. Paper presented at the 2015 IEEE 9th International Conference on Self-Adaptive and Self-Organizing Systems, s. 168-169. Haettu 27.12.2017 osoitteesta: https:/doi.org/10.1109/SASO.2015.29

Ståhle, P. & Kuosa, T. (2009). Systeemien itseuudistuminen: Uutta ymmärrystä kollektiivien kehittymiseen. Aikuiskasvatus : aikuiskasvatustieteellinen aikakauslehti, 29(2), s. 9. Haettu 27.1.2018 osoitteesta: http://elektra.helsinki.fi.ezproxy.jyu.fi/se/a/0358-6197/29/2/systeemi.pdf

Tierney, K. J. (2014). *The Social Roots of Risk : Producing Disasters, Promoting Resilience*. Stanford, California: Stanford Business Books. Haettu 16.3.2018 osoitteesta: http://search.ebscohost.com.ezproxy.jyu.fi/login.aspx?direct=true&db=nlebk&AN=790521&site=ehost-live&ebv=EB&ppid=pp_160

Valtioneuvoston puolustusselonteko (2017). Valtioneuvoston kanslian julkaisusarja 5/2017. Vationeuvostonkanslia 34 s.

Valtion tieto- ja viestintätekniikkakeskus. Valtorin strategia. Haettu 30.4.2018 osoitteesta: http://www.valtori.fi/fi-FI/Tietoa_Valtorista/Strategia

Ventre, D. (2016). Information warfare. Haettu 13.1.2019 osoitteesta: http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=4405840

Vermeer, H. J. (2006). *Luhmann's "social systems" theory: Preliminary fragments for a theory of translation*. Berlin: Frank & Timme. Haettu 22.11.2017 osoitteesta: https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=3033544

Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., Chen, S., & Zhao, K. (2015). Cyber-physical-social system in intelligent transportation. *IEEE/CAA Journal of Automatica Sinica, 2*(3), s. 320-333. Haettu 15.1.2018 osoitteesta: https://doi:10.1109/JAS.2015.7152667

Walden, Joe (2011). Comparison of the STEEPLE Strategy Methodology and the Department of Defense's PMESII-PT Methodology. Haettu 10.2.2019 osoitteesta: http://supplychainresearch.com/images/Walden_Strategy_Paper.pdf

Walker, B. H. & Salt, D. A. (2006). *Resilience thinking: Sustaining ecosystems and people in a changing world*. Washington, DC: Island Press. Haettu 19.3.2018 osoitteesta: https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=3317645#

Wang, F. (2010). The Emergence of Intelligent Enterprises: From CPS to CPSS. *Intelligent Systems, IEEE, 25*(4), s. 85-88. Haettu 15.12.2017 osoitteesta: https://doi.org/10.1109/MIS.2010.104

Yhteiskunnan turvallisuusstrategia 2017. Valtioneuvoston periaatepäätös 2.11.2017. Turvallisuuskomitea, Puolustusministeriö 99 s.

Yin, R. K. (2015). *Qualitative research from start to finish, second edition*. Haettu 6.4.2018 osoitteesta: https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/reader.action?ppg=37&docID=2008479&tm=1522915584286

LIITTEET

LIITE 1: ASIANTUNTIJAHAASTATTELUN OHJEISTUS

Aluksi, erittäin suuret kiitokset vaivannäöstäsi jo etukäteen osallistuessasi pro gradu -tutkimukseni asiantuntijapaneeliin. Osallistumisesi asiantuntijapaneeliin mahdollistaa pro gradu -tutkimukseni, sekä lisää osaltaan sen reliabiliteettia. Asiantuntijapaneelissa paneelistit toimivat anonyymisti, jolloin teillä arvoisa asiantuntija on mahdollisuus vastata annettuihin kysymyksiin anonymiteetin tarjoaman suojan turvin. Anonymiteetin tarkoituksena on mahdollistaa vastaaminen myös niissä tapauksissa, joissa omalla nimellä vastaaminen saattaisi olla ristiriidassa työ- tai virkavelvoitteisiin. Henkilöllisyyttänne ei paljasteta edes gradun ohjaavalle opettajalle.

Asiantuntijahaastattelun tarkoituksena on analysoida kyber-fyysisen viranomaissysteemin resilienssiä skenaarioanalyysillä laadituissa systeemin tulevaisuuden tiloissa. Tutkimuksen pohjaksi olen skenaarioanalyysiä käyttäen rakentanut viisi erilaista skenaariota. Skenaarioista kaksi ensimmäistä on tutkimuksen kannalta toisensa poissulkevat skenaariot, eli toivottu skenaario ja negaatio. Nämä skenaariot on laadittu sen vuoksi, että ilmeisin vaihtoehto (kuinka kaiken toivotaan menevän) ja sen vastakohta (kun kaikki ei mene niin kuin toivotaan) saadaan näkyville.

Asiantuntijapaneelin tehtävänä on näiden skenaarioiden perusteella analysoida kussakin skenaariossa kyber-fyysisen viranomaissysteemin sen hetkistä resilienssiä. Resilienssin analysointi tapahtuu käyttämällä SWOT-analyysiä. Tehtävänäsi on tehdä SWOT-analyysi jokaiselle skenaariolle erikseen.

SWOT-analyysissä viranomaissysteemin resilienssiä arvioidaan neljän muuttujan näkökulmasta:

- Johtaminen
- Tilannekuva
- Osaaminen
- Teknologia

Tehtävänne on siis arvioida kussakin skenaariossa erikseen viranomaisssysteemin vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia peilaten niitä edellä mainittuihin muuttujiin. Skenaarioita tutkimuksessa on 4 kappaletta, joissa on kaikissa 3 samaa vaikutinta.

- Kyberhyökkäykset
- Informaatiovaikuttaminen
- Fyysinen isku

Jokaisessa skenaariomallissa nämä tekijät ovat läsnä, mutta niiden vaikutus systeemin tulevaisuudenkuvaan on erilainen. Skenaariomallit on

esitetty tämän ohjeen lopussa. Tämän ohjeen liitteenä on dokumentti, johon SWOT-analyysin vastaukset kirjataan. SWOT-analyysiin vastatessanne pyydän teitä asiantuntijuuteenne perustuen miettimään mielestänne tärkeimmät vahvuudet, heikkoudet, mahdollisuudet ja uhat (neljän muuttujan näkökulmasta).

Esimerkki: Skenaariossa X systeemiin kohdistuu palvelunestohyökkäys, jonka se havaitsee, mutta ei osaa/kykene torjumaan. Kun tapahtumaketjua tarkastellaan taaksepäin huomataan, että systeemin vahvuutena tässä asiassa on kyky havaita kyberuhkia, mutta heikkoutena on kyky torjua niitä. Teidän pohdittavaksenne jää se, onko tämä mielestänne tärkein vahvuus tai heikkous systeemin resilienssiä kokonaisuutena arvioiden kyseisessä skenaariomallissa. Koska skenaariot sisältävät myös samoja elementtejä voi eri skenaarioilla olla yhteisiä samoja vahvuuksia, heikkouksia, mahdollisuuksi tai uhkia. Systeemin resilienssi rakentuukin lopulta näiden muuttujien yhteisvaikutuksesta.

Vastausten ei tarvitse olla essee-muotoisia. Vastauksen voi muodostaa ranskalaisin viivoin ja/tai tukisanoin. Minun tehtävänäni tutkijana on lopulta tulkita vastauksiasi ja kuinka ne peilaavat lopulta omien päätelmieni kesken. Tutkimuksessa on laadittu SWOT-analyysi systeemin alkutilassa. Jätän sen kuitenkin tässä vaiheessa pimentoon, jotten johdattele näkemyksilläni ja toisaalta koetellaksi omia näkemyksiänä verratessa niitä asiantuntijatietoon.

Pro gradu -tutkimuksessa viranomaistoimintaa tarkastallaan systeemi-tasolla, eikä siinä tutkita yksittäisen viranomaisen tai toimijan resilienssiä. Systeemin resilienssi muodostuu sen kokonaisuuden perusteella ja sitä tulisi myös analysoida tästä näkökulmasta.