JYU DISSERTATIONS 270

Jouni Pöyhönen

# Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa

## Systeemiajattelu

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 270

Jouni Pöyhönen

# Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa

## Systeemiajattelu

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen Alfa-salissa
elokuun 28 päivänä 2020 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, Alfa hall, on August 28, 2020 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2020

Editors
Timo Männikkö
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä



Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-8258-4

ISBN 978-951-39-8258-4 (PDF)
URN:ISBN:978-951-39-8258-4
ISSN 2489-9003

# ABSTRACT

Pöyhönen, Jouni
Cyber security management and development as part of a critical infrastructure organization – System Thinking
Jyväskylä: University of Jyväskylä, 2020, 236 p. (+included articles)
(JYU Dissertations
ISSN 2489-9003; 270)
ISBN 978-951-39-8258-4 (PDF)

The structure of the modern society is based on the cooperation of different parts of the critical infrastructure. Their mutual functional ability depends primarily on operationally reliable organizations that form systems, i.e. parts of the infrastructural whole.

This doctoral dissertation focuses on developing cybersecurity leadership in enterprises and other organizations in the network of national critical infrastructure. The research emphasizes controlling the continuity of their functional processes in all operational environments. The dissertation presents different models of cybersecurity leadership and development for organizations. The focus is on proactiveness as well as creating trust, preserving reputation and managing the continuity of functional processes. The research method used was Soft Systems Methodology, SSM.

While the people, processes and technologies of an organization present its capabilities, they also contain vulnerabilities. The most central research question of the dissertation concentrates on cybersecurity leadership procedures and a comprehensive system review of cybersecurity management in a national critical infrastructure organization. It means cybersecurity management on all levels of decision-making (strategic, operative and technical/tactical). Three practical measures for development are presented: first, embedding new technological solutions into the organization's piers cyber security structure, second, drafting comprehensive cyber security risk assessments and third, preparing contingency plans in order to improve an organization's resilience.

In implementing the organizational cybersecurity development measures presented in the dissertation, the PDCA-method of process improvement can be applied. These organization-specific measures advance the protection of national critical infrastructure and thus also cyber self-sufficiency, comprehensive security, security of supply and both national and organization-specific competitive advantage.

Keywords: cyber security, national critical infrastructure, system, organization, process, system, device

# TIIVISTELMÄ

Pöyhönen, Jouni
Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu
Jyväskylä: University of Jyväskylä, 2020, 236 p. (+ artikkelit)
(JYU Dissertations
ISSN 2489-9003; 270)
ISBN 978-951-39-8258-4 (PDF)

Modernin yhteiskunnan toiminta perustuu useiden kriittisen infrastruktuurin eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu lähtökohtaisesti toiminnaltaan luotettavista organisaatioista, joista muodostavat infrastruktuurin osakokonaisuudet, systeemit.

Tämä väitöstutkimus keskittyy kansalliseen kriittiseen infrastruktuuriin lukeutuvien yritysten ja muiden organisaatioiden kyberturvallisuuden kehittämiseen johtamisen näkökulmasta. Tutkimuksessa painottuu niiden toimintaprosessien jatkuvuuden hallinta kaikissa toimintaympäristöissä. Väitöskirjassa esitetään organisaation kyberturvallisuuden johtamisen ja kehittämisen malleja, jotka liittyvät proaktiiviseen toimintaan, toimintaprosessien jatkuvuuden hallintaan, luottamuksen edistämiseen ja maineen ylläpitämiseen. Tutkimusmenetelmänä on käytetty pehmeää systeemimetodologiaa.

Organisaation ihmiset, prosessit ja käytettävät teknologiat muodostavat kyberturvallisuuden kyvykkyydet, mutta ne sisältävät myös haavoittuvuuksia. Väitöstyön keskeisimpään tutkimuskysymykseen menettelyistä kriittisen infrastruktuurin organisaation kyberturvallisuuden johtamisessa ja kehittämisessä esitetään vastauksena kokonaisvaltaista systeemitarkastelua kyberturvallisuuden hallintaan. Se tarkoittaa kyberturvallisuuden johtamis- ja kehittämistoimenpiteitä kaikilla organisaation päätöksentekotasoilla (strateginen, operatiivinen, teknillinen/taktinen). Käytännön kehittämistoimenpiteiksi esitetään yhtäältä organisaation ICT-infrastruktuurin vyöhykesuojaukseen integroituja uuden teknologian ratkaisuja, ja toisaalta kattavasti laadittavia kyberturvallisuuden riskitarkasteluja sekä niiden jatkuvaa ylläpitämistä, ja kolmantena menettelynä varautumissuunnitelmien laadintaa siten, että organisaation toiminnan resilienssiä voidaan parantaa.

Väitöstyössä esitettävien organisaation kyberturvallisuuden kehittämistoimenpiteiden implementointiin voidaan soveltaa toiminnan kehittämisen PDCA-menetelmää. Organisaatiokohtaisilla toimenpiteillä edistetään kansallisen kriittisen infrastruktuurin suojaamista ja siten osaltaan myös kyberomavaraisuutta, kokonaisturvallisuutta, huoltovarmuutta ja sekä kansallista että organisaatiokohtaista kilpailuetua.

Avainsanat: kyberturvallisuus, kansallinen kriittinen infrastruktuuri, systeemi, organisaatio, prosessi, järjestelmä, laite

**Author's address**

Jouni Pöyhönen
Faculty of Information Technology
University of Jyväskylä
Finland

**Supervisors**

Professor of Practice Martti Lehto
Faculty of Information Technology
University of Jyväskylä
Finland

Professor Rauno Kuusisto
Finnish Defence Research Agency
University of Jyväskylä
Finland

Professor Pekka Neittaanmäki
Faculty of Information Technology
University of Jyväskylä
Finland

**Reviewers**

Professor Kirsi Helkala
Norwegian Defence Cyber Academy
Norway

Adjunct Professor Rauno Pirinen
National Defence University and
Laurea University of Applied Sciences
Finland

**Opponent**

Adjunct Professor Henry Sivusuo
National Defence University
Finland

# ESIPUHE

Tämä väitöskirja on tehty Jyväskylän yliopistossa Informaatioteknologian tiedekunnassa osana kyberturvallisuuden koulutus- ja tutkimusohjelmaa, joka oli myös yliopiston erityisenä profiloitumisalueena vuosina 2016 - 2019. Tutkimustyö on toteutettu kriittisen infrastruktuurin suojaamiseen tähtäävässä tutkimuskokonaisuudessa, joka on toinen kyberturvallisuuden päätutkimusalueista. Lisäksi kyberturvallisuuden puolustuksellinen näkökulma muodostaa oman tutkimuksellisen kokonaisuutensa. Kriittisen infrastruktuurin suojaamiseen kuuluvat osa-alueina muun muassa informaationinfrastruktuuri, mukaan lukien laitteiden internet (IoT), sekä energia-, terveydenhuolto-, ajonauvo-, siviili-ilmailujärjestelmät ja tilannetietoisuus. Väitöstyön otsikon ”Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa - Systeemiajattelu” mukainen aihealue on yhdistelmä organisaation johtamista ja kehittämistä, joka tähtää sen toimintaprosessien kyvykkyyden parantamiseen digitalisaation mukanaan tuomassa kybertoimintaympäristössä. Väitöstyössä on käsitelty yhteiskunnan kriittisestä infrastruktuurista muita toimialueita tarkemmin ja erityisesti esimerkin omaisesti yksityisen sektorin energiantuotantoon ja julkisen sektorin terveydenhuoltoon lukeutuvia organisaatioita. Näiden lisäksi yhteiskunnan välttämättömiä palveluja tuottavat laaja joukko erilaisia muita organisaatiota eri toimialoilta, joiden toiminnan kehittämiseen toivoisin väitöstyön tuloksia voitavan soveltaa samalla laajuudella.

Väitöstyön aihealue herätti kiinnostukseni asiaan julkisen keskustelun käynnistyttyä digitaalisen kehityksen edellyttämästä turvallisuudesta. Lähtökohtana on ollut myös vuonna 2013 julkaistu ensimmäinen kansallinen kyberturvallisuuden strategiamme. Pitkäaikainen palvelukseni Puolustusvoimissa ja erityisesti Ilmavoimien johtamis-, valvonta- ja tiedustelujärjestelmien parissa sekä organisaation eritasoisissa johtamistehtävissä selittänee parhaiten kiinnostustani aihealueeseen.

Jäätyäni pois Puolustusvoimien erikoisupseerin virasta vakituisen palvelusajan täytyttyä hakeuduin jatko-opiskelijaksi Jyväskylän yliopistoon Informaatioteknologian tiedekuntaa vuonna 2015 professori Martti Lehdon ja silloisen dekaanin professori Pekka Neittaanmäen innoittaman. Jatko-opinnot ja osa-aikainen projektitutkijan työ alkoivat vielä saman vuoden aikana. Jatko-opintojen ohella olen siten saanut olla yliopiston kyberturvallisuuden eri tutkimushankkeissa osa-aikaisena projektitutkijana koko väitöstyöprosessin ajan. Lehdon ja Neittaanmäen lisäksii tämän ovat mahdollistaneet nykyinen tiedekunnan dekaani Pasi Tyrväinen sekä esimieheni professori Timo Hämäläinen. Kiitän heitä kaikkia tästä mahdollisuudesta ja haluan erityisesti korostaa tutkimushanketyötä ja niistä muodostettujen tietojen merkitystä väitöstyön onnistumiseen ja sisältöön.

Professori Martti Lehto, professori Rauno Kuusisto ja professori Pekka Neittaanmäki ovat toimineet väitöstyön ohjaajina. Olen erittäin kiitollinen heidän avustaan väitöstyöprosessin eri vaiheissa. Lisäksi haluan esittää kiitokset

väitöstyöhön liittyvien tutkimushankkeiden tutkijakollegoille, artikkelien kirjoituskumppaneille sekä tiedekunnan tuelle, niin koko tutkimustyön ajalta kuin erityisesti kirjoitustyön loppuvaiheessa ja väitöskirjan julkaisemisessa.

Lopuksi haluan kiittää erityisesti lähimmäisiäni – puolisoani Maaritia ja tytärtäni Ainoa kaikesta siitä tuesta ja kannustuksesta, jonka olen heiltä saanut tutkimustyön eri vaiheissa. Kiitokset kuuluvat myös muille sukulaisille ja ystäville, joiden mielenkiito väitöstyötäni kohtaa on korostanut aiheen merkitystä päivittäisessä toiminnassamme.

Jyväskylässä 6. päivänä elokuuta 2020

Jouni Pöyhönen

## LYHENTEET

**APT**, Advanced Persistent Threat

**BIOS**, Basic Input-Output System

**BYOD**, Bring Your Own Device

**CAN**, Controller Area Network

**CATWO**E, Customer, Actors, Transformation process, World view, Owners, Environmental constraints

**CERT**, Computer Emergency Response Team

**CIIP**, Critical Information Infrastructure Protection,

**CIIRP**, Critical Information Infrastructure Resiliency Protection

**CIO,** Chief Information Officer

**CIRP**, Critical Infrastructure Resiliency Protection

**CISA**, Cybersecurity and Infrastructure Security Agency

**CMS**, Central Monitoring System

**COTS**, Commercial off-the-shelf

**CPS**, Cyber-physical system

**DCS**, Distributed Control Systems

**DMZ,** Demilitarized Zone

**ECHO**, European network of Cybersecurity centres and competence Hub for innovation and Operations

**EECSP**, Energy Expert Cyber Security Platform

**EHR**, Electronic Health Record

**EMR**, Electronic Medical Record

**ENISA**, European Union Agency for Network and Information Security

**EPCIP**, European Programme for Critical Infrastructure Protection

**ERP**, Enterprise Resource Planning

**FIPS,** Federal Information Processing Standards

**FSC**, Facility Security Clearance

**GDBR**, General Data Projection Regulation

**HAVARO,** Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä

**HCIC**, Health Care Industry Cybersecurity

**HVK**, Huoltovarmuuskeskus

**ICS**, Industrial Control System

**ICT**, Information and Communication Technology

**IDS**, Intrusion Detection System

**IEC**, International Electrotechnical Commission

**IoT**, Internet of Things

**IPS**, Intrusion Prevention System

**IP,** Internet Protocol

**IR-manager**, Incident Response manager

**ISO**, International Organization for Standardization

**ITIL**, Information Technology Infrastructure Library

**ITS**, Intelligent Transport Systems

**ITU**, International Telecommunication Union

**KATAKRI**, kansallinen turvallisuusauditointikriteeristö

**KTK**, Kyberturvallisuuskeskus

**LAN**, Local Area Network

**LSTM**, Long short-term memory –verkko

**MBA**, Master of Business Administration

**MES**, Manufacturing Execution System

**MTI**, Massachusetts Institute of Technology

**M2M**, Machine to Machine

**NCSA,** National Communications Security Authority

**NCSI**, National Cyber Security Index

**NERC,** North American Electric Reliability Corporation

**NIAC**, National Infrastructure Assurance Council

**NIS**, Network and Information Security

**NIST**, National Institute of Standards and Technology

**NRA**, National Regulatory Authority

**OCSVM**, One-class Support Vector Machine

**OODA**, Observe-Orient-Decide-Act

**OSI**, Open Systems Interconnection

**OSINT**, Open Source Intelligence

**OSI-RM**, Open Systems Interconnection Reference Model

**PACS**, Picture Archiving Communications Systems

**PDCA**, Plan, Do, Check, Act

**PLC**, Programmable Logic Control

**PPP**, Public Private Partnership

**PTJ**, Potilastietojärjestelmä

**QM**, Quality Management

**RFID,** Radio Frequency Identification

**RIS**, Radiology Information System

**RTU**, Remote Terminal Unit

**SCADA**, Supervisory Control and Data Acquisition Systems

**SFS**, Suomen standardisoimisliitto ry.

**SIEM**, Security Information and Even Management

**SOC**, Security Operation Center

**SOS,** System-of-Systems

**SSH,** Secure Shell

**SSM**, Soft Systems Methodology

**SWOT**, Strengths, Weaknesses, Opportunities, Threats

**UBS**, Universal Serial Bus

**VAHTI-ohjeet**, Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän ohjeisto

**VMM,** Virtual Machine Monitor

**VPN**, Virtual Private Network

**WAN**, Wide Area Network

**YTS**, Yhteiskunnan turvallisuusstrategiassa

## KUVIOT

# TAULUKOT

# SISÄLLYSLUETTELO

## LISTA TUTKIMUSARTIKKELEISTA JA -RAPORTEISTA

Työ pohjautuu oheisiin seitsemään julkaisuun (P1-P7) ja yhdeksään tutkimusraporttiin (RR1-RR9). Julkaisut P1-P7 ovat liitteinä.

Tutkimusartikkelit (P1-P7):

P1. Pöyhönen, J., Lehto, M., 2017. Cyber security creation as part of the management of an energy company. ECCWS 2017: Proceedings of the 16th European Conference on Cyber Warfare and Security (pp. 332-340). Published by Academic Conferences and Publishing International Limited. Reading. UK

P2. Pöyhönen, J., Nuojua, V., Lehto, M., Rajamäki, J., 2018. Application of Cyber Resilience Review to an Electricity Company. ECCWS 2018: Proceedings of the 17th European Conference on Cyber Warfare and Security (pp. 380-389). Published by Academic Conferences and Publishing International Limited. Reading. UK.

P3. Pöyhönen, J., Kotilainen, P., Kalmari J., Poikolainen, J., Neittaanmäki, P,. 2019. Cyber security of vehicle CAN bus. ECCWS 2019: Proceedings of the 18th European Conference on Cyber Warfare and Security (pp. 354-363). Published by Academic Conferences and Publishing International Limited. Reading. UK

P4. Pöyhönen, J., Nuojua, V., Lehto, M., Rajamäki, J., 2019. Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations. Digital Transformation, Cyber Security and Resilience. DIGILIENCE 2019. Volume 43, no. 2 (2019): 236-256.

P5. Pöyhönen, J., Nuojua, V., Lehto, M., Rajamäki, J., 2019. Cyber Situational Awareness in Critical Infrastructure Organizations. Springer artikkeli on painoprosessissa.

P6. Pöyhönen, J., Lehto, M., 2020. Cyber security: Trust based architecture in the management of an organization security. Originally published in the proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS2020, 25-26 June 2020, University of Chester, UK, pages 304-313

P7. Pöyhönen, J., Rajamäki, J., Ruoslahti, H., Lehto, M., 2020. Cyber Situational Awareness in Critical Infrastructure Protection. Cyber Security of Critical Infrastructure 2020 (CYSEC2020) conference, October 27th, 2020 - October 28th, 2020. Dubrovnik. Croatia. Artikkeli hyväksytty 2.3.2020.

Tutkimusraportit (RR1-RR9):

RR1. Pöyhönen J. (2018). Standardit, ohjeet ja suositukset osana teollisuusyrityksen kyberturvallisuuden hallintaa. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 55/2018.

RR2. Pöyhönen J. (2018). Cyber security in the management of an electricity company. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 56/2018.

RR3. Pöyhönen J. (2018). Kyberturvallisuuden hallintajärjestelmän luominen energiayhtiön lämpövoimalaitokseen. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 57/2018.

RR4. Pöyhönen J. (2018). SWOT-analyysin soveltaminen yrityksen kyberturvallisuuden tilannekuvan muodostamiseen. Tutkimusmenetelmän kuvaus. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 58/2018.

RR5. Pöyhönen J., Nuojua V. (2018). Tilannekuvatieto kriittisen infrastruktuurin yrityksen tietojärjestelmien tietoturvallisuudessa, Tutkimusongelman kuvaus. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 59/2018.

RR6. Lehto M., Limnéll J., Innola E., Pöyhönen J., Rusi T., Salminen M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, helmikuu 2017.

RR7. Lehto M., Limnéll J., Kokkomäki T., Pöyhönen J., Salminen M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018, maaliskuu 2018.

RR8. Pöyhönen J., Lehto M., Lehto M. (2019). Kyberturvallisuus sairaalajärjestelmissä, toiminnan kehittäminen. University of Jyväskylä, Faculty of Information Technology, research paper, 75/2019.

RR9. Lehto M., Pöyhönen J., Lehto M. (2019). Kyberturvallisuus sosiaali- ja terveydenhuollossa. Loppuvaportti Vol 2. VFH- ja WHC-hankekokonaisuus. Jyväskylä yliopisto, IT-tiedekunta. Jyväskylä yliopisto, Informaatioteknologian tiedekunta.

Väitöstutkija on toiminut ensimmäisenä kirjoittajana tutkimusartikkeleissa P1-P7 ja tutkimusraporteissa RR1-RR5 sekä RR8. Ne perustuvat tutkimukseen ja kirjoitustyöhön kolmessa eri tutkimushakkeessa, joista yhdessä kansallisessa tutkimushankkeessa (CyberTrust-tutkimushanke) Jyväskylä yliopisto on ollut mukana osapuolena ja kaksi on ollut Jyväskylän yliopiston tutkimushankkeita (AaTi ja ja Watson Health Cloud Finland). Watson Health Cloud Finland tutkimuksen kyberturvallisuusosiossa tutkija toimi sairaalaa koskevan tutkimusosion pääasiallisena toteuttajana ja raportoijana (RR8 ja RR9). Tutkimusraportit RR5 ja RR6 käsittelevät Valtioneuvoston tutkimushankkeita, jotka Jyväskylän yliopisto toteutti yhdessä Aalto-yliopiston kanssa. Myös näitä tutkimushakkeita on hyödynnetty tutkimustyössä ja -artikkeleissa. Tutkimushankkeissa väitöstutkija toimi organisaatioiden ja kansallisen tilannetietoisuuden tutkijana ja raportoijana. Kaikissa tutkimushakkeissa tutkijanimike on ollut projektitutkija ja tutkia on ollut osa-aikaisessa työsuhteessa Jyväskylän yliopistoon.

# 1 JOHDANTO

## 1.1 Tutkimuksen kohde ja tarkoitus

Modernin yhteiskunnan toiminta perustuu useiden kriittisten infrastruktuurin eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu lähtökohtaisesti toiminnaltaan luotettavista organisaatioista, joista muodostavat kriittisen infrastruktuurin osakokonaisuudet. Kybertoimintaympäristössä yhteiskunnan kokonaisluotettavuus rakentuu organisaatioiden omasta ja keskinäisestä toiminnasta, niiden välisistä toimivista tiedonsiirtoverkostoista sekä palvelutason järjestelmien tiedon käytettävyydestä, luotettavuudesta ja eheydestä. Kybertoimintaympäristön turvallisuusriskejä kasvattavat erityisesti globaalin digitalisaation kehityksen mukanaan tuomat uhkakuvat.

Suomen ensimmäisessä kansallisessa kyberturvallisuusstrategiassa (2013) todetaan, että ”kyberturvallisuus käsittää kaikki ne yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia tilanteissa, joista voi aiheutua merkittävää haittaa tai vaaraa Suomelle tai sen väestölle” (Turvallisuuskomitea, 2013). Euroopan unionin kyberturvallisuusstrategia samaiselta vuodelta painottaa kyberturvallisuutta EU:n kykynä ”turvata verkkoympäristö, joka tarjoaa mahdollisimman laajan vapauden ja tietoturvan kaikkien hyödyksi” (Euroopan unioni, 2013). Kyberturvallisuuden sanastossa kyberturvallisuudesta todetaan seuraavasti: (Turvallisuuskomitea, 2018)

> ”Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”

Kyberturvallisuus voidaankin määritellä tiivistetysti digitalisaation kehityksen kautta mahdollistuneen tietojärjestelmien, -laitteiden, -varantojen, -verkkojen ja niiden käytön muodostaman kokonaisuuden toiminnan ja omaisuuden suojaamiseksi erilaisilta häiritseviltä tapahtumilta ja hyökkäyksiltä, sekä niiden vaikutuksia vastaan toteutettaviksi vastatoimenpiteiksi. Kyberturvallisuuteen liittyy

oleellisesti käsitteenä myös tietoturvallisuus. Kyberturvallisuus on tietoturvallisuutta laajempi kokonaisuus. Se kattaa tietojen ja niitä käsittelevien laitteiden lisäksi myös niiden käyttäjät, ja niihin luottavat ihmiset aina yhteiskunnan kokonaisetuun ja kriittiseen infrastruktuuriin saakka (Von Solms & Van Niekerk, 2013). Organisaatiotasolla kyberturvallisuuden kyvykkyystekijät muodostuvat ihmisistä, prosesseista ja teknologioista (Jacobs, von Solms & Grobler, 2016). Yhteiskunnan kokonaisturvallisuuden näkökulmasta tarkasteltuna kyberturvallisuus rakentuu laajasti koko yhteiskunnan ja sen organisaatioiden kyvykkyydelle tunnistaa kyberturvallisuuteen liittyviä uhkatekijöitä ja riskejä, sekä toimia niitä sisältävässä toimintaympäristössä.

Suomen kyberturvallisuuden toimenpideohjelma vuosille 2017 - 2022 pitää sisällään toimenpiteitä, joilla strategisten linjausten toteutumista hallitaan ja mitataan. Siinä painottuvat näkökulmat, joissa kansalaiset ovat julkisen hallinnon palveluiden asiakkaina, kansalliset elintärkeät toiminnot turvataan, julkisen ja yksityisen sektorin sekä tiede- ja tutkimusmaailman välistä yhteistyötä kehitetään. Toimenpideohjelma pitää sisällään kaksikymmentäkaksi aluetta, jossa on huomioitu muun muassa se, että huoltovarmuuskriittisten yrityksen kyberturvallisuutta on edistetty, sähköenergian toimintavarmuuden riittävä taso on saavutettu ja EU-tason tietoturvallisuuden sekä tietosuojan lainsäädäntö on selkiytetty ja täydennetty kansalliseen lainsäädäntöön. (Turvallisuuskomitea, 2017a)

Tutkimuksessa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” (2017) todettiin, että kyberturvallisuus on kehittynyt viime vuosina kyberturvallisuusstrategian määrittämien strategisten linjausten ja strategiatyön ohessa laaditun toimeenpanosuunnitelman takia suotuisasti. Tutkimus osoitti myös, että edelleen tarvitaan merkittäviä kehittämistoimia useissa kohteissa, joita ovat tähän väitöstutkimukseen liittyen muun muassa kansallisen tilannetietoisuuden ja havaintokyvyn parantaminen, elintärkeiden toimintojen turvaamisen edistäminen, tutkimuksen ja yleisen tietoisuuden vahvistaminen sekä kyberturvallisuuden kehittäminen osana kokonaisturvallisuutta. Lisäksi esillä olivat tarpeet, jotka liittyivät toimenpiteisiin kyberturvallisuuden vahvistamiseksi kansallisena kilpailuetuna, osaamisen, sekä toimenpiteiden tehokas seuraaminen ja kansallisen kypsyysmallin luominen. Jatkotutkimuksen osalta raportissa suositeltiin ainakin seuraavia aiheita: ”kyberturvallisuuden strateginen johtaminen Suomessa, kybertilannekuvan ja analysointikyvykkyyden kehittäminen sekä yhteiskunnan elintärkeiden toimintojen, kriittisen infrastruktuurin ja kyberomavaraisuuden määrittely osana kansallista kyberresilienssiä”. (Lehto, ym., 2017)

Christian Fjäder on antanut Huoltovarmuuskeskuksen asiantuntijalausunnon eduskunnalle otsikolla ”Huoltovarmuuden toimintaympäristön muutos ja uhkakuvat” hallituksen esityksestä siviilitiedustelua koskevaan lainsäädäntöön vuonna 2018. Lausunnossa on painotettu yksityinen sektorin ja julkinen sektori yhteistyön merkitystä tuotettaessa yhteiskunnan vastuulla olevia kriittisiä tuotteita ja palveluja. Toimintaan liittyy myös markkinaehtoisesti toimivia ulkomaalaisia tahoja. Tämän vuoksi Suomen kansalliseen kriittiseen infrastruktuuriin

kytkeytyy rajojemme ulkopuolella sijaitsevia ”rakenteita, resursseja ja prosesseja”, jotka vaikuttavat toimintaan. Lausunnossa korostetaan erityisesti digitalisaation kehityksen merkitystä siihen, että toimintaan liittyvät tietojärjestelmät ja -varannot vaikuttavat integroitumiseen ylikansallisiin toimintaprosesseihin ja siten erilaisiin kyberympäristössä tapahtuviin ilmiöihin. (Fjäder, 2018)

Lainsäädännön osalta Euroopan neuvosto hyväksyi 17. toukokuuta 2016 säännöt verkko- ja tietojärjestelmien turvallisuuden parantamiseksi koko EU:ssa. Verkko- ja tietoturvadirektiivin (NIS-direktiivi) tavoitteina todetaan, että sen toimenpiteillä ”lisätään yhteistyötä jäsenvaltioiden kesken ja asetetaan turvallisuuteen liittyviä velvoitteita keskeisten palvelujen tarjoajille (kriittiset toimialat kuten energia, liikenne, terveys ja rahoitus) ja digitaalisten palvelujen tarjoajille (verkossa toimivat markkinapaikat, hakukoneet ja pilvipalvelut)”. (Euroopan unioni, 2016)

Tämä väitöstutkimus liittyy osaltaan kyberturvallisuuden jatkotutkimustarpeisiin kohdistuen kansalliseen kriittiseen infrastruktuuriin lukeutuvien yritysten ja muiden organisaatioiden kyberturvallisuuden kehittämiseen johtamisen näkökulmasta. Tutkimuksessa painottuu niiden toimintaprosessien jatkuvuuden hallinta kaikissa toimintaympäristöissä. Se on osa Jyväskylän yliopiston kriittisen infrastruktuurin suojaamiseen liittyvää kyberturvallisuuden tutkimusohjelmaa, joka lähtökohdiltaan tukeutuu alueen kansallisiin strategioihin, ja tukee osaltaan yhteiskunnan huoltovarmuuskriittisten organisaatioiden kyberturvallisuuden edistämistä sekä kansallista kyberomavaraisuutta. Tutkimusongelmien ratkaisemiseksi väitöstyössä on sovellettu pehmeää systeemimetodologiaa (Soft Systems Methodology, SSM). Asiaa on tarkasteltu sekä energia-alaan kuuluvan sähköyhtiön että terveydenhuoltoalaan kuuluvan sairaalaympäristön kyberturvallisuuteen liittyvien järjestelyjen tutkimisen kautta. Ne edustavat yksityisen sektorin liiketaloudellista näkökulmaa ja julkisen sektorin palvelunäkökulmaa. Yhdessä ne muodostavat laajan kirjon erilaisia digitaalisia verkkoja, järjestelmiä, laitteita, niiden käyttökohteita ja käyttötapoja, jolloin tutkimustuloksia ja kehittämisehdotuksia voidaan soveltaa laajasti sekä kriittisen infrastruktuurin että muihinkin organisaatioihin. Tutkimus tukee myös tutkimusperioodin aikana käyttöön tulleita NIS-direktiivin asettamia vaatimuksia. Asian ajankohtaisuuteen voidaan kuvata alla referoitujen Suojelupoliisin katsauksen 5.12.2019 ja Helsingin seudun kauppakamarin viimeisimmän tutkimusraportin 27.9.2019 avulla.

Suojelupoliisin katsauksessa (5.12.2019) on kiinnitetty huomiota siihen, että ulkomaiset tiedustelupalvelut ovat aiempaa kiinnostuneempia Suomen kriittisestä infrastruktuurista, jonka seurauksena todetaan muun muassa seuraavasti:

> ”Kriittisen infrastruktuurin päätyminen kybervakoilua tai -vaikuttamista aktiivisesti harjoittavan valtion hallintaan aiheuttaa uhkan kansalliselle turvallisuudelle jo ennen kuin vakoilua harjoittava valtio päättää käyttää voimaansa.”

Helsingin seudun kauppakamarin on toteuttanut vuosien 2015-2019 aikana kolme valtakunnallista kyberturvallisuuden toteutumisen selvitystä yksityisen

sektorin eri toimialoilla ja organisaatioissa. Viimeisimmässä tutkimuksessa (27.9.2019) todetaan kyberturvallisuuden toteutumisesta seuraavasti:

> ”Yritysten kybervarautumisen tilanne ei juurikaan ole muuttunut – uhat ovat yleistyneet.”

Selvityksen mukana olleiden yritysten valmiudet tunnistaa kohdistettuja kyberhyökkäyksiä ovat heikot ja erityisesti yritysten toiminnassa torjua kyberuhkia on paljon kehitettävää. Vuoden 2015 jälkeen suurien yritysten toiminnassa on tapahtunut jonkin verran edistystä, mutta muissa kokoluokissa tilanne ei juurikaan ole parantunut. Noin 40 % vastaajayrityksistä ei osaa arvioida tunkeutujan motiiveja yrityksensä osalta. Suojattavia arvoja ei tunnisteta. Lisäksi elinkeinoelämän keskuudessa ei tunnisteta kyberturvallisuuteen liittyviä ja toiminnassa avustavia viranomaistahoja. Selvityksessä todetaankin, että kyberuhat ovat pahimmillaan kansallisen turvallisuuden uhkia. (Helsingin seudun kauppakamarin, 2019)

Väitöstutkimuksen ensisijaisena tavoitteena on tuoda uutta tutkimustietoa kansallisen kriittisen infrastruktuurin organisaatioiden kyberturvallisuuden kehittämiseen ja johtamiseen toiminnan jatkuvuuden varmistamiseksi muuttuvassa kybertoimintaympäristössä. Niillä haetaan merkittävää yhteiskunnallista vaikuttavuutta kokonaisturvallisuuden näkökulmasta tarkasteltuna. Väitöstutkimuksen tuloksien laaja-alainen soveltaminen kehittää yritysten ja muiden organisaatioiden ja koko yhteiskunnan kilpailukykyä, palvelujen toimivuutta, huoltovarmuutta ja kybertoimintaympäristön resilienssiä. Väitöstutkimus täydentää aiemmin todettua kyberturvallisuuden teknillisiin ratkaisuihin keskittynyttä kansallista tutkimusprofiilia (Pelkonen ym., 2016) huomioimalla organisaatioiden toiminnassa strategisia, operatiivisia ja taktillisia kyberturvallisuuden näkökulmia. Tutkimuksessa ja sen ratkaisujen hahmotellussa on myös hyödynnetty tutkijan koulutustaustaa ja aikaisempaa kokemusta Ilmavoimien tiedustelun, valvonnan ja johtamisen järjestelmien kehittämisessä ja ylläpitämisessä, sekä organisaatioiden eritasoisista johtamis- ja kehittämistehtävistä.

## 1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tutkimus ”Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen” osoittaa, että Suomessa on korkeatasoista kyberturvallisuuteen liittyvää tutkimus-, kehitys- ja innovaatiotoimintaa ja -osaamista. Vahvuuksista huolimatta alan osaamispohjaa pidetään varsin kapeana ja kärkiosaaminen keskittyy harvoille toimijoille. Kyberturvallisuuteen liittyvää tutkimusta leimaa kuva, että ”tutkimus on teknologisesti orientoitunutta ja tekniikkaan painottunutta”. Alan tutkijat ovat valtaosin tietotekniikan, tietoliikennetekniikan tai tietojärjestelmätieteiden alueilta. Muista tutkimusaloista voidaan mainita matematiikka. Lisäksi muutamia tutkijoita on ollut mukana muun muassa politiikan tutkimuk-

sesta, sotatieteistä ja kognitiotieteistä. Tutkimusalue on myös volyymiltään varsin marginaalinen muihin tieteen tutkimusalueisiin verrattuna. Alueen suppeudesta riippumatta kyberturvallisuuteen liittyy kapeita kärkiosaamisalueita. Tällaisia ovat esimerkiksi kryptologia, haavoittuvuustutkimus, tietoturvan hallinta ja mobiililaitteiden tietoturva. Suomessa tarvitaankin määrätietoisia toimenpiteitä kyberturvallisuusosaamisen edelleen kehittämiseksi niin, että lähes pelkästään teknologisia erityisosaamisalueita voidaan laajentaa tutkimusalueen tarpeiden edellyttämällä tavalla. (Pelkonen ym., 2016)

Jyväskylän yliopiston kyberturvallisuuden koulutus ja tutkimus ovat muodostaneet yhden yliopiston viime vuosien profiloitumisalueista. Alueen koulutuksen ja tutkimuksen kehittämistä on toteutettu vuodesta 2009 lukien. Yliopiston Informaatioteknologian tiedekunnassa opintoja voi suorittaa tietojärjestelmätieteiden, tietotekniikan, kognitiotieteen ja kyberturvallisuuden aloilla. Näistä valmistuu kauppatieteen tai filosofian kandidaatteja, maistereita ja tohtoreita. Jyväskylän yliopistossa on kyberturvallisuudesta oma maisteriohjelma. Informaatioteknologian tiedekunnan päätutkimusaluetta ovat laskennallinen tiede, ohjelmistot ja tietoliikennetekniikka, tietojärjestelmätiede, kognitiivinen tiede ja koulutusteknologia. Kyberturvallisuus tutkimusalana risteää edellä mainittujen päätutkimusalojen kanssa. Kyberturvallisuuden tutkimus puolestaan jakautuu neljään päätutkimusalueeseen, jotka ovat kyberturvallisuus ja verkottuminen, informaatioturvallisuuden hallinta, kyberpuolustus ja kriittisen infrastruktuurin suojaaminen. Tutkimusalueilla on mahdollisuus suorittaa kyberturvallisuuden jatko-opintoja. (Lehto, Niemelä, 2019)

Vuodesta 2013 lukien Suomen kyberturvallisuusstrategia ja sen toimenpideohjelmat ovat muodostaneet perustaa koulutukselle ja tutkimukselle. Edellä mainittuja kyberturvallisuuden koulutus- ja tutkimusohjelmia on toteutettu vuodesta 2013 lähtien. Toiminta tukee kansallisen kyberturvallisuuden strategisia tavoitteita. Suomen kyberturvallisuuden strategiassa 2019 yhdeksi kolmesta strategia-alueesta on valittu osaamisen kehittäminen, josta todetaan seuraavasti: (Turvallisuuskomitea, 2019)

> ”KYBERTURVALLISUUDEN OSAAMISEN KEHITTÄMINEN – arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina.”

Jyväskylän yliopiston kyberturvallisuuden tutkimusalueen nykyistä laajuutta kuvaavat esimerkiksi professori Martti Lehdon kriittisen infrastruktuurin suojaamiseen ja kyberpuolustuksen ilmiöihin sijoittuvat tutkimusohjelmat, professori Timo Hämäläisen teknillisiin ratkaisuihin painottuvat tutkimusohjelmat ja professori Mikko Siposen organisaatioiden informaatioturvallisuuteen painottuvat tutkimusohjelmat. Väitöstöihin liittyvinä konkreettisina esimerkkeinä edellä mainituista alueista, ja osin myös tähän väitöstutkimukseen liittyen, ovat muun muassa Martti Karin väitöstyö ”Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats” (2019), Aarne Hummelholmin väitöstyö “Cyber Security and Energy Efficiencies in the Infrastructures of Smart Societies” (2019), Tero Kokkosen väitöstyö ”Anomaly-Based Online Intrusion Detection System as a

Senor for Cyber Security Situational Awareness System" (2016) sekä Jouko Selkälän väitöstyö "CIO decision making: Issues and a process view" (2016).

Tämä väitöstutkimus on osa Jyväskylä yliopiston kyberturvallisuuden tutkimusohjelmaa ja se liittyy kriittisen infrastruktuurin suojaamisen tutkimusalueeseen täydentäen edellä mainittuja tutkimustarpeita. Väitöstutkimuksen keskeisenä tavoitteena on määritellä kriittisen infrastruktuurin organisaation kyberturvallisuuden kehittämisen ja johtamisen menettelyjä edellä esitetyin tavoittein. Tähän liittyen väitöstyössä luodaan malli eri tasoisista toimenpiteistä tavoitteen saavuttamiseksi. Tavoitteiden saavuttamiseksi esitettävä pääkysymys kuuluu seuraavasti:

> Millaisia ja miten kyberturvallisuuden menettelyjä voitaisiin hyödyntää kriittisen infrastruktuurin organisaation kyberturvallisuuden kehittämisessä ja johtamisessa?

Tutkimustyön aikana nousi esille useita pääkysymystä tukevia osakysymyksiä, joihin on haettu vastauksia eri tutkimushakkeisiin osallistumalla. Artikkelit ja raportit pitävät sisällään vastauksia seuraaviin osakysymyksiin:

Osakysymys 1:

> Millaisia tekijöitä liittyy kriittisen infrastruktuurin organisaation kyberturvallisuuden muodostumiseen?

Osakysymykset 2-4:

> Millaisia toimenpiteitä voidaan liittää organisaation kyberluottamuksen edistämiseen? Miten organisaation kyberturvallisuuden systeeminäkökulma voidaan rakentaa? Miten organisaation kyberturvallisuuden arkkitehtuuri voidaan muodostaa?

Osakysymys 5:

> Miten kriittisen infrastruktuurin organisaation toiminnan jatkuvuuden hallintaa voidaan kehittää häiriöihin varautumiseksi haasteellisessa kybertoimintaympäristössä?

Osakysymykset 6-8:

> Millaisia menettelyjä kriittisen infrastruktuurin organisaation tilannetietoisuuden kehittämiseen liittyy? Kuinka organisaatiot vaihtavat kyberturvallisuuteen liittyviä tietojaan? Voidaanko organisaation kyberturvallisuusvalmiuksia hyödyntää laajemmin kriittisessä infrastruktuurissa?

Osakysymys 9:

> Millaisia kyberturvallisuuden tilannetietoisuuden haasteita liittyy organisaation ICT-varantoihin ja automaatiojärjestelmiin?

Osakysymys 10:

> Mitä standardeja, ohjeita ja suosituksia voidaan hyödyntää organisaation kyberturvallisuuden hallinnan kehittämisessä?

## 1.3 Väitöstutkimukseen liittyvät tutkimushankkeet

Väitöstutkimuksen kysymyksiin on haettu vastauksia ja tutkimustuloksia kyberturvallisuutta käsitelleistä tutkimushankkeista, joita Jyväskylän yliopisto on hallinnut tai joissa yliopisto on ollut osallisena vuosien 2015-2019 aikana. Väitöstutkija on ollut näissä hankkeissa projektitutkijana. Tutkimushankkeina ovat olleet kansallinen ”CyberTrust-tutkimushanke”, Valtioneuvoston kanslialle tehdyt kaksi tukimusta; ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” ja ”Kyberturvallisuuden strateginen johtaminen Suomessa”, Jyväskylän yliopiston ja IBM:n yhteistyönä toteutettu ”Watson Health Cloud Finland tutkimushanke”. Autojen automaatioväylän tietoturvallisuutta käsitelleessä ”AaTi-tutkimushankeessa” väitöstutkija toimi loppuvaiheen projektipäällikkönä. Lisäksi tutkimusperiodin aikana on laadittu edellä mainittujen tutkimusten perusteella artikkeli DIGILIENCE 2019-konferenssiin, joka käsitteli aihetta ”Digital Transformation, Cyber Security and Resilience” muun muassa teemalla ”Cyber Security Situational Awareness” sekä artikkeli konferenssiin ”Cyber Security of Critical Infrastructure 2020 (SYSEC2020)” teemalla ”Situational awareness and security metrics”.

Tutkimushankkeissa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” (2017) ja ”Kyberturvallisuuden strateginen johtaminen Suomessa” (2018) suoritettiin puolistrukturoidut teemahaastattelut. Hankkeissa haastattelujen lähtökohtana oli haastateltavien täysi anonymiteetti. Ensiksi mainitussa tutkimushankkeessa oli haastateltavina seitsemältä kriittisen infrastruktuurin osa-alueelta yksityisen ja julkisen sektorin organisaatioiden tieto-/kyberturvallisuudesta vastaavia henkilöitä yhteensä 31 (SWOT-teemat). Haastattelussa kartoitettiin myös kohdeorganisaatiota laajemmin kunkin toimialan kyberturvallisuuden tilaa ja kehittämistarpeita. Jälkimmäisessä tutkimushankkeessa haastateltiin yhteensä 40 yksityisen ja julkisen sektorin organisaatioiden johtohenkilöä tai tieto-/kyberturvallisuudesta vastaavaa henkilöä kahdestakymmenestäviidestä organisaatiosta (johtamisen ja tilannetietoisuuden teemat). Haastattelutiedoista on väitöstutkimukseen muodostettu kyberturvallisuuden kokonaiskuvaa kriittisestä infrastruktuurista ja sen organisaatioista. Sähköyhtiön eli tutkimuskohteen yksi osalta organisaation nykytila-analyysissä on hyödynnetty erityisesti energia-alan haastattelumateriaalia. Suomen kyberturvallisuuden strategista johtamista käsitelleen tutkimushankeen haastattelutiedoilla on täydennetty edellä mainituista tutkimushankkeista saatuja tietoja. Lisäksi hanketietojen perusteella on muodostettu kriittisen infrastruktuurin organisaation kyberturvallisuuden tilannetietoisuuden ja toiminnan mittaamisen osiot. CyberTrust-tutkimushankeen työpajoista saaduilla tiedoilla on täydennetty tietoja erityisesti sähköyhtiön osalta. Muilta osin väitöstyössä ja sen taustatutkimuksissa on hyödynnetty tapauskohtaisesti alueeseen liittyvän aineiston sisällönanalyysiä.

Oheisessa taulukossa 1 on lueteltu väitöstyöhön liittyvät tutkimushankkeet, tiedonhankintamenetelmät ja kohdistettu niistä muodostetut vertaisarvioidut

tieteelliset julkaisut. Taulukossa 2 on vastaavat tiedot kohdistettu tutkimushankkeisiin raportteineen ja loppuraportteineen. Taulukkoihin on myös merkitty väitöstutkijan rooli niissä.

TAULUKKO 1 Tutkimushankkeet, tiedonhankinta, vertaisarvioidut julkaisut.

| AJAN-KOHTA | TUTKIMUSHAKE/ TIEDONHANKINTA | VERTAISARVIOIDUT JULKAISUT |
|---|---|---|
| 2016-2017 | VNK-tutkimushanke: Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.<br>• teemahaastattelu, SWOT<br>• aineiston sisältöanalyysi | P1<br>- 1. kirjoittaja<br>- konferenssiesitys<br>- projektitutkija<br>- raportointi |
| 2015-2017 | Cyber Trust tutkimushanke.<br>• teemahaastattelu<br>• aineiston sisältöanalyysi | P2<br>- 1. kirjoittaja<br>- konferenssiesitys<br>- projektitutkija<br>- raportointi |
| 2016-2018 | Ajoneuvoalustojen tietoturva (AaTi) -tutkimushanke.<br>• aineiston sisältöanalyysi<br>• tapaustutkimus | P3<br>- 1. kirjoittaja<br>- konferenssiesitys<br>- raportointi |
| 2019 | Digital Transformation, Cyber Security and Resilience. Teema: Cyber Security Situational Awareness. Konferenssi.<br>• teemahaastattelu<br>• aineiston sisältöanalyysi | P4, P5<br>- 1. kirjoittaja<br>- projektitutkija |
| 2020 | The 19th European Conference on Cyber Warfare and Security ECCWS2020, 25-26 June 2020, Chester, UK, University of Chester, Konferenssi.<br>• aineiston sisältöanalyysi | P6<br>- 1. kirjoittaja<br>- projektitutkija |
| 2020 | Cyber Security of Critical Infrastructure 2020 (SYSEC2020) conference, October 27th, 2020 - October 28th, 2020. Dubrovnik. Croatia. Konferenssi.<br>• aineiston sisältöanalyysi | P7<br>- 1. kirjoittaja<br>- projektitutkija |

TAULUKKO 2 Tutkimushankkeet, tiedonhankinta, tutkimusraportit.

| AJAN-KOHTA | TUTKIMUSHAKE/ TIEDONHANKINTA | TUTKIMUSRAPORTIT |
|---|---|---|
| 2015-2017 | Cyber Trust tutkimushanke.<br>• teemahaastattelu<br>• aineiston sisältöanalyysi | RR1-RR5<br>- 1. kirjoittaja<br>- projektitutkija<br>- raportointi |
| 2016-2017 | VNK-tutkimushanke: Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.<br>• teemahaastattelu, SWOT<br>• aineiston sisältöanalyysi | RR6<br>- kirjoittaja<br>- projektitutkija<br>- raportointi |
| 2017-2018 | VNK-tutkimushanke: Kyberturvallisuuden strateginen johtaminen Suomessa.<br>• teemahaastattelu<br>• aineiston sisältöanalyysi | RR7<br>- kirjoittaja<br>- projektitutkija<br>- raportointi |
| 2016-2018 | Watson Health Cloud Finland tutkimushanke.<br>• aineiston sisältöanalyysi | RR8, RR9<br>- kirjoittaja<br>- projektitutkija<br>- raportointi |

## 1.4 Tutkimuksen rakenne

Väitöskirjan rakenne muodostuu seitsemästä pääluvusta, jotka pitävät aluksi sisällään johdannon tutkimuksen aihealueeseen, katsaukset kyberturvallisuuteen käsitteenä ja johtamiseen toiminta-alueena, tekniikan tutkimukseen, systeemiajatteluun, kriittisen infrastruktuuriin, kyberturvallisuuden tutkimukseen, alan normeihin ja tilannetietoisuuteen. Lisäksi ne pitävät sisällään tutkimusmenetelmän ja tiedonhankinnan kuvaukset, tapaustutkimukset ja niiden tulokset, kehittämisehdotukset sekä johtopäätökset, jossa on esitetty yhteenveto tutkimuksesta, pohdittu tutkimuksen toteutusta, rajoitteita ja esitetty jatkotutkimustarpeita. Tutkimustulokset rakentuvat tutkimuksessa käytetyn pehmeän systeemimetodologian vaiheista. Tutkimustyön reilun neljän vuoden aikana on korostunut tutkimusmenetelmän eri vaiheiden tuottaman lisäarvon merkitys siten,

että työssä on voitu edetä johdonmukaisesti menetelmää seuraten. Tutkimustyössä on lähdetty liikkeelle hahmottelemalla tulkinnan lähtökohdat kohdealueesta ja kartoittamalla siitä hallussa olevia tietoja, jonka jälkeen väitöstyön aikaisissa eri tutkimushankkeissa on tarkasteltu alueeseen liittyviä näkökulmia, tiedonhankintaa ja haettu vastauksia tutkimuksellisia tavoitteita vasten. Väitöstyön muodostama kokonaisuus on täydentynyt vaiheittain työn aikana. Tutkimustulosten keskeinen sisältö on työ eri vaikeissa esiin nousseiden osakysymysten osilta väitöskirjan artikkeleissa ja pääkysymyksen osalta itse väitöskirjassa.

Luku yksi pitää sisällään tutkimusalueen keskeisimpiä lähtökohtia, jotka auttavat hahmottamaan työn perusteita. Niissä korostuu kyberturvallisuuden muun muassa tutkimuksellinen tarve. Kansallisen kriittisen infrastruktuuri organisaatioiden johtaminen ja toiminnan kehittäminen verkottuneen toimintaympäristön muodostamassa kyberavaruudessa liittyy osaltaan tarpeen täydentämiseen. Tästä lähtökohdasta on muodostettu tutkimuskysymykset.

Luku kaksi käsittelee kyberturvallisuutta käsitteenä, kybermaailman uhkia ja kyberturvallisuuteen liittyvää luottamuksen merkitystä organisaatiolle ja koko yhteiskunnalle sekä ilmentymänä että johtamisen näkökulmasta tarkasteltuna.

Luvun kolme aluksi on kuvattu tutkimuksen viitekehys ja käsitelty tutkimuksen teoreettisia lähtökohtia johtamisen kehittymisen, teknologian ja systeemin tutkimuksen osilta. Lukuun sisältyvät myös katsaukset kriittiseen infrastruktuuriin sekä siihen liittyviin resilienssin ja huoltovarmuuden käsitteisiin, kyberturvallisuuteen tutkimuskohteena, sen tilannetietoisuuteen ja normipohjaan. Osat tukeutuvat oleellisesti tutkimusasetelmaa ja tutkimusmenetelmän valintaan. Luvussa on käsitelty aluetta tutkimustarpeen kuvaamiseksi, jolloin on voitu myös taustoittaa työn keskeisiä attribuutteja ja niiden välisiä suhteita.

Luvussa neljä on kuvattu tutkimustilannetta pehmeän systeemimetodologian muodostamassa kokonaisuudessa. Lisäksi luvussa on kuvattu teemahaastattelujen muodostuminen ja laadittu tutkimusmenetelmään liittyviä analyysejä.

Luvussa viisi on tutkimuksen empiirinen osuus, jonka avulla on muodostettu yleiskuvaa kansallisesta kriittisen infrastruktuurin organisaatioiden kyberturvallisuuden tilasta. Aluksi luvussa on selvitetty organisaatioiden kyberturvallisuuden kokonaistilannetta. Sen jälkeen on pureuduttu alueeseen tarkemmin ja syvennetty sitä kyberturvallisuuden nykytilakuvauksilla kahden toimialan esimerkin kautta. Ne ovat yksityisen sektorin energia-alan sähköyhtiö ja julkisen sektorin terveydenhuollon sairaala. Tällä empiirisellä osuudella ja systeemikuvauksilla tutkimusalue on voitu jaotella siten, että ensiksikin on saatu tuloksia, ja toisaalta niitä on ollut mahdollista käsitellä viitekehyksessä ja johtaa organisaation kyberturvallisuuden kehittämistavoitteita vastauksina tutkimuskysymyksiin. Tutkimuksen empiirinen osuus koostuu osallistumisesta viiteen tutkimushakkeeseen, joista on muodostunut samalla väitöstyön taustatutkimukset. Jokaiseen väitöstyön taustatutkimukseen on liittynyt myös teoreettista tarkastelua kohteen osalta.

Luvussa kuusi on esitetty kehittämistoimenpiteet vastauksena tutkimuskysymyksiin ja esitetty malli kehitystoimenpiteiden käytännön implementointiin

organisaatiossa. Väitöstyössä korostuu digitalisaation kehityksestä johtuva organisaation kyberturvallisuuden kompleksisuus ja siitä seurannut organisaatioihin kohdistuvien uhkien arvaamattomuus. Se on johtanut väitöstyön kuluessa vakavaan pohdintaan suojaustoimenpiteiden kattavuudesta. Pohdinnan perusteella on tehty kyberturvallisuuden kehittämiseksi menetelmällisiä valintoja, joissa korostuu systeemiajattelu. Sen tarkoituksena on ollut muodostaa kokonaisvaltainen – holistinen – käsitys organisaation kyberturvallisuuteen liittyvästä toiminnasta ja kyvystä ylläpitää toimintaprosessejaan kaikissa toimintaympäristön tilanteissa.

Luvussa seitsemän on esitetty johtopäätökset tutkimuksen tuloksista, avattu edellä mainittua pohdintaa, tarkasteltu tutkimuksen rajoituksia ja esitetty tutkimuksellisia tarpeita jatkoa ajatellen.

Liitteessä yksi on käsitemäärittelyjä, liitteenä kaksi katsaus kyberturvallisuuden normipohjaan ja lopussa ovat väitöstyöhön liittyvät artikkelit, joissa on esitetty vastauksia tutkimuksen aikana esiin tulleisiin kysymyksiin.

Tutkimusjakson aikana on julkaistu kaksi EU-tason säädöstä kyberturvallisuuden alalta. Ne ovat EU:n tietosuojalaki GDPR (General Data Projection Regulation, GDBR) ja EU:n verkko- ja tietoturvadirektiivi NIS (Network and Information Security, NIS). Näistä erityisesti NIS-direktiivi painottaa kriittisen infrastruktuurin organisaatioiden tuottamien palvelujen turvallisuutta ja eurooppalaista kilpailukykyä, mikä on huomioitu väitöstutkimuksessa.

# 2 KYBERTURVALLISUUS KÄSITTEENÄ JA JOHTAMISEN TOIMINTA-ALUEENA

## 2.1 Kyberturvallisuus käsitteenä

Digitalisaation vaikutukset heijastuvat laajasti koko yhteiskuntaan. Se on johtanut digitaalitekniikan integroitumiseen osaksi yhteiskunnan jokapäiväisiä toimintoja: (Lehto & Neittaanmäki, 2016, 56-64.)

> ”Digitalisaatiossa on kyse yhteiskunnallisesta prosessista, jossa hyödynnetään teknologisen kehityksen uusia mahdollisuuksia. Digitalisaatio on luonut spesifisiä ilmiöitä, erilaisia toimintaympäristöjä ja mahdollistanut käyttäytymistä, joita ei ole ennen digitaalista aikaa.”

Kyberturvallisuus liittyy digitalisaation mukanaan tuomaan jokapäiväiseen kybertoimintaympäristöömme. Digitalissa järjestelmissä ja laitteissa esiintyvät häiriöt johtuvat usein niihin kohdistuneista tietoturvauhkista, joten kyberturvallisuuskäsitteeseen liittyy myös tietoturva-käsite. Kyberturvallisuuden sanastossa kyberturvallisuudesta siihen liittyvästä tietoturvasta todetaan seuraavasti: (Turvallisuuskomitea, 2018)

> ”Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”

> ”Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.”

Kyber-sana tulee kreikankielisestä sanasta ”kybereo” tarkoittaen ohjaamista, opastamista ja hallitsemista. Amerikkalainen matemaatikko Norbert Wiener (1894–1964) otti käyttöön kreikankielisestä sanasta muodostetun kybernetiikka-

sanan 1940-luvun lopulla kuvaamaan tietokoneita käyttäviä ohjausjärjestelmiä. Sanalla oli tarkoitus kuvata tieteitä, jotka käsittelevät koneiden ja organismien ohjausta ja hallintaa informaation avulla. (Lehto, 2019, 7)

Kyberturvallisuuden sanastossa kyber-sanasta ja kyberturvallisuudesta todetaan seuraavasti: (Turvallisuuskomitea, 2018)

> ”Kyber-sanaa käytetään yleensä yhdyssanan määriteosana. Sanan merkityssisältö liittyy yleensä digitaalisessa muodossa olevan informaation käsittelyyn: tietotekniikkaan, digitaaliseen viestintään (tietoverkkoihin), tietojärjestelmiin tai tietokonejärjestelmiin. Yleensä vasta koko yhdyssanalla (määriteosan ja perusosan yhdistelmällä) voidaan ajatella olevan oma merkityksensä.”

Jatkossakin tekniikan nopea kehittyminen perustuu digitalisaation aikaan saamaan ”kierteeseen”, kuten edellä on todettu. Tulevaisuuden digitaalisessa toimintaympäristössä, tai toisin sanoen kybertoimintaympäristössä, erilaiset prosessit kuten esimerkiksi tuotantoprosessit digitalisoituvat ja siten mahdollistuvat automatisoidut toiminnot yhä laajemmin. Kehitystä on monissa yhteyksissä kutsuttu Teollisuus 4.0:ksi. Siihen liittyvät oleellisina osina kyberfyysiset järjestelmät (Cyber-physical system, CPS) ja asioiden internet (Internet of Things, IoT). Kyberfyysinen järjestelmä on järjestelmä, jossa verkon avulla yhteen liitetyt ohjelmistot kontrolloivat fyysisiä laitteita ja siten muodostavat yhä laajempia ja reaaliaikaisempia järjestelmien järjestelmiä. Kyberfyysiset järjestelmät ovat informaatioteknologiaan lukeutuvia ohjelmistoalustoja, jotka valvovat, ohjaavat ja suojaavat fyysisiä toimintaprosesseja (Sadeghi, Wachsmann & Waidner, 2015, 1.).

Digitalisaatio kehityksen myötä on muodostunut verkottunut toimintaympäristö, joka on mahdollistanut yritysten ja ihmisten arkea ja elämää helpottavien toimintojen ja palvelujen kehittymisen. Osittain palveluista on myös kehittynyt yhteiskunnan kannalta katsottuna keskeisiä ja kriittisiä toimintoja. Digitaalisuuteen pohjautuvia informaatioteknologian innovaatiomahdollisuuksia syntyy jatkuvasti yhä enemmän. Tavaroista ja palveluista tulee älykkäämpiä ja ne liittyvät toisiinsa sekä ihmisiin aivan uusilla tavoilla. Yritysten osalta kehitys on merkinnyt aiempaa syvempää ja reaaliaikaisempaa vertikaalista integraatiota niiden toimintaverkostoissa. Kehityksen seurauksena on myös syntynyt uudenlaisia uhkia. Samalla myös niiden tunnistaminen on vaikeutunut erityisesti verkottuneen toiminnan pitäessä sisällään alueita, joihin ei ole välttämättä näkyvyyttä. Verkostoitunut toiminta voi myös pitää sisällään toimijoita ja tekniikoita, jolla kyberturvallisuuden ratkaisut eivät ole kaikilta osin riittävällä tasolla. Verkottumisen kautta muodostunut kybermaailma houkuttelee rikollisia toimijoita, jotka etsivät uusia mahdollisuuksia varastaa, hyödyntää ja myydä tietoa tai aiheuttaa uhkia yhteiskunnan keksisille ja kriittisille palveluille. Tiedusteluorganisaatioille ja teollisuusvakoilijoille informaation siirtyminen verkkoon on tuonut kybermaailmasta uuden toiminta-alueen. Terroristeille toimintaympäristö mahdollistaa esimerkiksi anonyymin verkon kautta tapahtuvan yhteydenpidon, viestinnän ja vaikuttamisen. Toimintaympäristö on myös terroristeille houkutteleva hyökkäyskohde. Asevoimien digitalisaatio on luonut sotilaallisen kybermaailman, jossa verkottuneiden sotilaiden lisäksi vaikuttavat älykkäät ja aiempaa itsenäisemmät asejärjestelmät. (Lehto & Limnéll, 2017, 181,182)

Kyberturvallisuus onkin kokonaisturvallisuuden osa-alue, jolla pyritään digitalisoituneen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuus liittyy tällöin myös yhteiskunnan kriittisiin toimintoihin ja siinä yhdistyvät niiden tietoturva, toimintojen jatkuvuuden hallinta ja häiriötilanteisiin varautuminen. Organisaatioiden kyberturvallisuus muodostuu kyvykkyyksistä, kuten ihmisten osaamisesta ja käytänteistä, prosesseista ja teknologioista, joilla voidaan suojata verkkoja, järjestelmiä, laitteita, ohjelmia ja dataa hyökkäyksiltä, vahingoilta tai luvattomalta käytöltä.

## 2.2 Kybermaailman uhkia

Kyberuhkiksi voidaan katsoa toimenpiteet, joilla yritetään vahingoittaa tai tuhota tietoverkkoa, -järjestelmää tai päätelaitetta tai vaikuttaa niiden käyttömahdollisuuksiin tai tietosisältöihin. Tutkimuksessa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” (2017) selvitettiin kyberuhkien merkittävimpiä trendejä. Tuloksena olivat seuraavat trendit: ”Kiristyshaittaohjelmien kasvu, haavoittuvuuksien hyödyntäminen, laitteistoihin kohdistuvat uhkat, yrityksen sisäpiiri hyökkäyskanavana, liiketoiminnan tuhoamiseen tähtäävät hyökkäykset sekä henkilötietojen varastamiseen tähtäävät hyökkäykset. Lisäksi myös huijaukset ja tietojen kalastelut, palvelunestohyökkäykset, kohdistetut hyökkäykset sekä jatkuvat hyökkäykset mainittiin useassa raportissa”. Myös kiristyshaittaohjelmat ovat yleistyneet ja niiden määrän on ollut nopeassa kasvussa vuodesta 2016 lukien. Kiristyshaittaohjelmia muunnellaan jatkuvasti ja siten ne uusia kehittyneempiä muotoja. Kiristyshaittaohjelma voidaan toteuttaa niin, että se voi levitä koko yrityksen sisäverkkoon. Uhkana saattaa olla, että sen avulla pahimmillaan salataan kaikki verkkolevyt sekä pilvipalvelujen tiedostot. (Lehto, ym., 2017, 12)

Yhteiseurooppalainen verkko- ja tietoturvasta vastaavan organisaation, ENISA:n kyberturvallisuuden uhkatilannetta käsittelevässä raportissa ”Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends” on todettu edellä mainittujen merkittävimpien uhkien pysyneen edelleen lähes ennallaan. Lisäksi uutena uhkana on tullut esille ns. ”Cryptojacking”, joka on salaustekniikka, jota voidaan käyttää tietokoneiden tietojen luvattomaan salaamiseen esimerkiksi haitallisen sähköpostilinkin avulla (ENISA, 2018 a, 9).

Tietojärjestelmien ja -laitteiden erilaiset haavoittuvuudet ovat merkittävin syy kyberuhkien muodostamiselle tietoverkoissa, -järjestelmissä tai päätelaitteissa. Haavoittuvuudet ovat usein vaikeasti havaittavissa ja siten vaikeasti torjuttavissa. Niiden avulla hyökkääjät saavat aikaa kehittää toimintaansa verkoissa. Rikolliset voivat käynnistää hyökkäyskampanjoita ja haitallisen toiminnan mahdollistavat hyökkäysmenetelmät voivat olla jo pitkällä tietojärjestelmien rakenteissa ennen kuin ne tunnistetaan ja ehditään käynnistämään vastatoimet. Organisaation käytössä olevien tietoverkkojen, -järjestelmien ja päätelaitteiden heikot kohdat löydetään usein liian myöhään. Siitä huolimatta, että palvelun tarjoajat

kehittävät sovelluskehityksen prosessejaan, kyberhyökkääjät kykenevät kuitenkin jatkuvasti löytämään menettelyjä tietoturva-aukkojen havaitsemiseen ja niiden hyödyntämiseen hyökkäyksissä. Rikolliset tekevät yhä enemmän hyökkäyksiä, jotka ovat kohteena olevalle organisaatiolle aiempaa monimutkaisempia sekä haasteellisempia puolustaa. Organisaatioiden tietoturva-asiantuntijoiden on jatkuvasti kehitettävä ja ylläpidettävä tilannetietoisuuttaan ICT-varantojensa haavoittuvuuksista. (Lehto, ym., 2018, 12)

Yleisen digitaalisen osaamisen seurauksena rikolliset ovat voineet kehittää menetelmiään kybertoimintaympäristössä. Toimintaa kuvaa hyvin se, että hyökkääjät kykenevät etsimään sisäänpääsyä organisaatioiden järjestelmiin yhä syvemmältä laitetekniikasta. Hyökkäyksiä on voitu tehdä laitetasolla muun muassa levyasemien laiteohjelmiin, grafiikan prosessointiyksiköihin, tietokoneiden varusohjelmiin ja BIOS-tasolle (Basic Input-Output System, BIOS). Näillä laitatason hyökkäyksillä on mahdollista päästä käsiksi koko fyysiseen tietokoneeseen ilman hälytyksiä tai havaintoja normaalin toiminnan poikkeavuuksista, jolloin virtualisoidut prosessit ja tietokoneen muistialueet jatkavat toimintaansa normaalisti jopa uudelleenkäynnistyksen ja uudelleenasennuksen jälkeen. (Lehto, ym., 2018, 12)

Organisaatioiden toimintaprosessit muodostavat niiden operatiivisen toiminnan perustan. Toimintaprosesseja ovat niin organisaation ydinprosessit kuin tukiprosessitkin. Hyökkääjät etsivät näistä prosesseista heikkouksia ja pyrkivät löytämään väyliä tunkeutumiselle ja suoralle vaikuttamiselle prosessien toimintaan. Tällöin voidaan saada suora yhteys esimerkiksi kyberfyysiseen vaikutukseen ja siten voidaan muodostaa uhkaa organisaatiolle kyseisen toimintaprosessin jatkuvuuteen. Toimintaan liittyy hyökkääjän yksityiskohtainen prosessituntemus kohteesta, mikä on osalta avainasemassa sekä hyökkäyksen suunnittelussa että sen toteutusmahdollisuuksien analysoinnissa. ENISA pitää raportissaan ”Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends” erityisen tärkeänä tunnistaa organisaation operatiivisen tason toimintaprosesseihin kohdistuvat uhkakuvat (ENISA, 2017, 15).

Esimerkkinä operatiiviselta tasolta kyberfyysiseen prosessiin vaikuttamisesta voidaan pitää Ukrainan sähköverkkoihin kohdistettua hyökkäystä joulukuussa 2015, jossa sähköyhtiön toimittajaverkostosta voitiin suunnata hyvin valmisteltu ja teknillisesti vaativa vaikuttaminen alueellisesti toimivan sähköyhtiön sähkönjakelujärjestelmään. Hyökkäyksellä pystytiin katkaisemaan sähköt laajalta alueelta, jolloin yli kaksisataatuhatta kuluttajaa jäi useiden tuntien ajaksi ilman sähköä. Hyökkäyksen analysoinneissa on tunnistettu elementtejä, joiden toteuttamisessa voi epäillä valtiollisen tason toimijan osallisuutta. (CISA, 2016)

Kriittisen infrastruktuurin organisaatioiden osalta merkittävä havainto on, että henkilötietojen varastaminen on erityisesti viime vuosina esiin tullut kyberturvallisuusalueen uhka. Kyberturvallisuuden asiantuntijaorganisaatio Mandiant on raportissaan ”M-Trends 2016” raportoinut, että henkilötietojen varastamiseen tähtäävät hyökkäykset lisääntyivät erityisesti vuoden 2015 aikana. Rapotin mukaan näytti siltä, että tavoitteena oli kerätä mahdollisimman paljon henkilöihin liittyviä tietoja yksittäisten henkilötietojen sijaan. Hyökkäykset kohdentuivat usealle eri toimialalle: terveystoimialaan, matkustamiseen, rahoitusalaan sekä

julkishallintoon. Hyökkääjät tähtäsivät erityisesti sellaiseen tietoon, joiden avulla voidaan todistaa henkilöllisyys erilaisissa palveluissa. (Mandiant Consulting, 2016)

Kriittisen infrastruktuurin turvallisuuteen liittyy oleellisesti verkossa tapahtuva vakoilun uhka, joka kohdistuu valtiollisiin ja myös yksityisiin organisaatioihin. SUPO on vuosikirjassaan vuodelta 2017 todennut asiasta seuraavasti: (SUPO, 2017)

> ”Vuonna 2017 Suojelupoliisin tietoon tuli useita tapauksia, joissa oli ilmeistä, että tunkeutumisen takana oli suunnitelmallisesti toimiva valtiollinen toimija. Yrityksille uhka on erityisen vakava, koska tieto on yhä useammin yrityksen keskeisin tuotantotekijä ja aineeton omaisuus. Kybervakoilulla yritykseltä voidaan pahimmillaan viedä koko tulevaisuus. Kyberavaruudessa tapahtuva vakoilutoiminta ei tunne valtiollisia rajoja, vaan se voidaan toteuttaa suomalaiseen tietojärjestelmään ilman fyysistä läsnäoloa Suomessa. Vakoilu-uhan torjuminen on aiempaa vaikeampaa, koska yritykset ovat usein ulkoistaneet tiedon hallinnointia. Alihankintaketjuista muodostuu helposti monimutkaisia, jolloin poikkeamia voi olla vaikea havaita. Suojelupoliisi arvioi, että usein tämän tyyppisen yritysvakoilun taustalla on valtiotoimija, jolla on halu saada oman maansa teollisuuden käyttöön tuotekehitystietoa helposti ilman omaa panosta ja suurta kiinnijäämisen riskiä. Vakoilun kohteena on myös suomalainen energiasektori sekä energiasektorin tuotekehitysyritykset. Niihin kohdistuu koko ajan valtiotaustaista kartoitusta. Suojelupoliisin arvion mukaan kartoituksen tekijä ei ole kiinnostunut anastamaan näiltä yrityksiltä tietoa. Sen sijaan tarkoituksena on etsiä kriittisen infrastruktuurin järjestelmistä sellaisia haavoittuvuuksia ja -ominaisuuksia, joita hyväksikäyttäen järjestelmät voitaisiin kriisitilanteessa lamauttaa.”

Kyberavaruudessa tapahtuvat erilaiset konfliktit ovat todellisuutta. Tällöin motiiveihin voi liittyä poliittisten, taloudellisten tai sotilaallisten konfliktien elementtejä. (Dunn Cavelty, 2010)

Kyberuhat voidaan jakaa luokkiin toimijoiden motiivien perusteella. Lähtökohtaisesti hyökkääjien kyberavaruudessa suorittavien toimenpiteiden taustalla voidaan tunnistaa viisi keskeisintä motiivia, jotka ovat: (Dunn Cavelty, 2010)

1. Kybervandalismi ja haktivismi.
2. Kyberrikollisuus.
3. Kybervakoilu.
4. Kyberterrorismi.
5. Kybersota.

Jyväskylän yliopiston kyberturvallisuuden professori Martti Lehto on yliopiston ”Johdatus kyberturvallisuuteen” kurssin kirjallisuusaineistossaan ”Kybermaailman ilmiöitä ja määrittelyjä” täydentänyt hyökkäysmotiivit kuusikerroksiseksi määrittelyksi seuraavasti: (Lehto, 2019, 16-19)

- Tason 1 muodostaa kybervandalismi, johon kuuluvat hakkerointi, haktivismi ja kyberparveilu (kyberparveilu, jossa Internet-verkon ja matkapuhelinten avulla kootaan ja johdetaan usein väkivaltaisia mielenosoituksia). Organisaatiotasolla toiminta saattaa aiheuttaa merkittäviäkin taloudellisia vahinkoja.
- Tason 2 muodostaa kyberrikollisuus. EU komissio määrittelee kyberrikollisuuden rikoksiksi, "jotka tehdään sähköisiä viestintäverk-

koja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin". Tietoverkkorikollisuus voidaan komission mukaan jakaa kolmeen alaryhmään; perinteinen rikollisuus, laittoman sisällön julkaiseminen ja rikokset, joita esiintyy ainoastaan sähköisissä verkoissa, kuten hyökkäykset tietoverkkoa vastaan, palvelunesto tai hakkerointi.

- Tason 3 muodostaa kybervakoilu. Kybervakoilu voidaan määritellä toimiksi, joilla hankitaan salaisia tietoja (sensitiivinen, yksityisoikeudellinen tai turvaluokiteltu) yksityisiltä ihmisiltä, kilpailijoilta, ryhmiltä, hallituksilta ja vastustajilta poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi.
- Tason 4 muodostaa kyberterrorismi, jossa tietoverkkoja käytetään hyökkäyksiin kriittisiä informaatiojärjestelmiä kohtaan ja niiden kontrollointiin. Hyökkäysten tavoitteena on tuottaa vahinkoa ja levittää pelkoa ihmisten keskuuteen sekä painostaa poliittista johtoa taipumaan terroristien vaatimuksiin.
- Tason 5 muodostaa kybersabotaasi. Se on toimintaa, jossa hyökkääjä (valtiollinen toimija tai sen tukema ryhmittymä) operoi sotaa alemmalla tasolla. Tavoitteina voivat olla epävakauden aiheuttaminen kohdemaassa, offensiivisten kyberhyökkäyskykyjen testaaminen, hybridioperaatioiden valmistelu tai sodan valmistelu.
- Tason 6 muodostaa kybersodankäynti. Käsitteelle ei ole yleisesti hyväksyttyä määritelmää, mutta sitä käytetään hyvinkin laajasti kuvamaan valtiollisten toimijoiden operaatioita kybermaailmassa. Kyberturvallisuuden sanasto mukaan kybersodankäynti on tietoverkkoja ja niiden haavoittuvuuksia hyödyntävä, valtioiden välinen vihamielinen toiminta (Turvallisuuskomitea, 2018). Varsinainen kybersodankäynti edellyttää valtioiden välistä sotatilaa, jossa kyberoperaatiot ovat osa muita sotilaallisia operaatioita.

Kyberturvallisuuden sanastossa määritetään haavoittuvuus seuraavasti: (Turvallisuuskomitea, 2018)

> ”Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa. Nollapäivähaavoittuvuus on tietojärjestelmässä oleva haavoittuvuus, johon ei ole saatavilla korjausta.”

Richard Hundley ja Robert Anderson jakavat kybermaailman haavoittuvuudet seuraavasti: (Hundley & Anderson, 1995, 237 - 238)

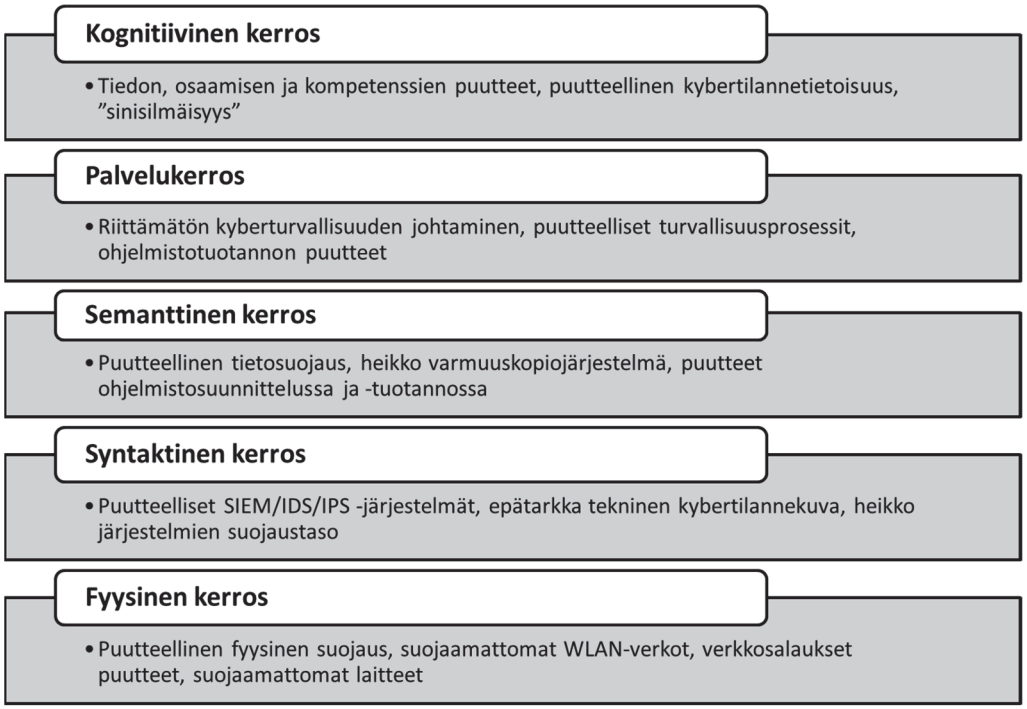
- Toimintoperustaisia, kuten toimintajärjestelmät ja prosessit.
- Käyttäjäperustaisia, kuten autentikointi ja salasanat.
- SW-perustaisia, kuten takaovi, ohjelmistovirheet ja asennusvirheet.
- HW-perustaisia, kuten suunnittelu ja komponenttivirheet.
- Verkkoperustaisia, kuten TCP/IP-protokolla.

Yhteiskunnan toiminnot ovat yhä riippuvaisempia informaatioteknologiasta, jossa ohjelmistot, tietokoneet ja -verkostot muodostavat palveluja tuottavia järjestelmiä. Järjestelmät ja niiden toiminnat ovat jatkuvasti kyberhyökkäysten kohteita. Järjestelmien laajuus ja kompleksisuus tekee mahdottomaksi kokonaan eliminoida haavoittuvuudet sekä havaita ja jäljittää tunkeutumiset systeemin sisälle. Edellä kuvattu luokittelu kybermaailman haavoittuvuuksista voidaan sijoittaa ICT-järjestelmien kyberrakenteeseen (kts. luku 3.1) niin, että ne kohdistuvat sen eri kerroksille. Järjestely mahdollistaa haavoittuvuuksien hahmottamisen järjestelmätasolla.

Haitan aiheuttaja voi toteuttaa kyberhyökkäyksiä kyberrakenteen eri kerroksiin oheisen kuvauksen mukaisesti: (Lehto, 2014, 171, muokattu)

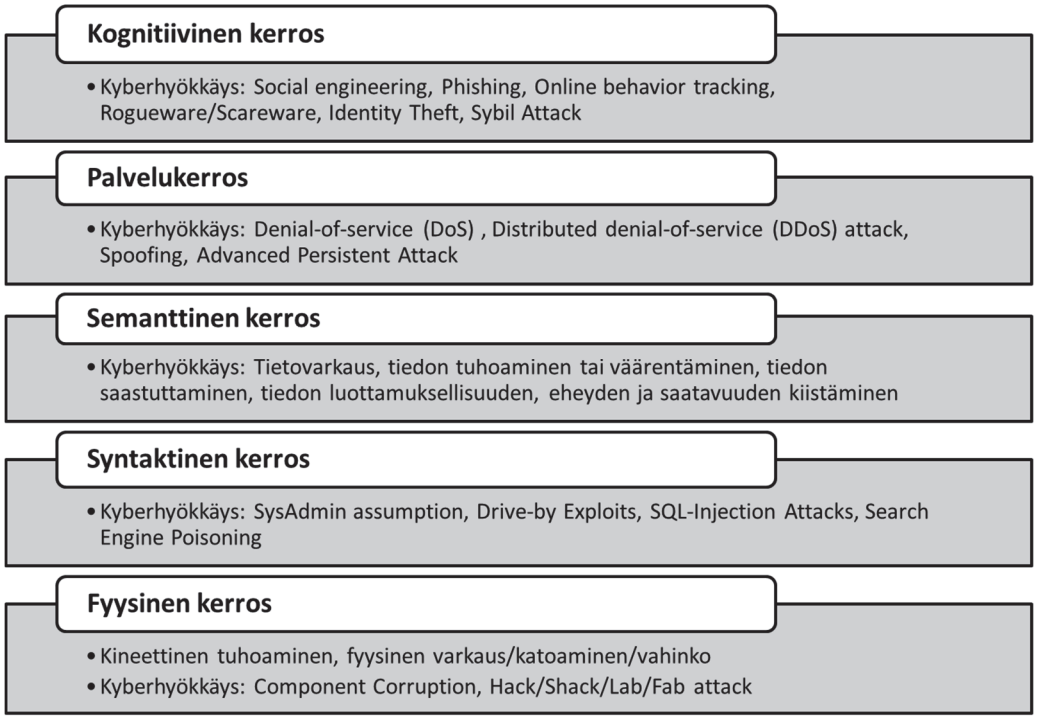
- Kyberrakenteen fyysiseen kerroksen voidaan kohdistaa sekä kineettistä että ei-kineettistä vaikutusta. Kineettisellä asevaikutuksella voidaan tuhota fyysisiä verkkoja, järjestelmiä ja niiden osia sekä tietovarastoja (Data Warehouse). Fyysisen maailman uhkia ovat myös laitejärjestelmien komponenteissa olevat haittaohjelmat ja takaportit.
- Hyökkäyksellä syntaktista kerrosta vastaan tavoitellaan järjestelmän tai sen osien saamista hallintaan. Hyökkäyksillä voidaan esimerkiksi häiritä organisaation teollisuusautomaatioverkon toimintaa tai avata mahdollisuuksia hyökkäyksille muita kerroksia vastaan.
- Kyberhyökkäyksen kohteena semanttista kerrosta vastaan on esimerkiksi informaation hallintaan ottaminen tai sen käyttäminen rikollisiin tarkoituksiin. Muun muassa kybervakoilu voidaan määritellä tällaiseksi toimeksi, jolla hankitaan salaisia tietoja (sensitiivinen, yksityisoikeudellinen tai turvaluokiteltu) yksityisiltä ihmisiltä, kilpailijoilta tai eri ryhmiltä poliittisen tai taloudellisen edun saavuttamiseksi käyttäen laittomia menetelmiä Internet- ja muissa verkoissa, ohjelmistoissa tai tietokoneissa (Liaropoulos, 2010, 177-182).
- Hyökkäyksellä palvelukerrosta vastaan pyritään lamauttamaan verkkopalveluiden toiminta. Tyypillisesti toimintaan vaikutetaan palvelunestohyökkäyksellä (Denial of Service, DoS). Se tarkoittaa verkkohyökkäystä, jossa pyritään estämään verkkosivuston tarkoitettu käyttö.
- Hyökkäys kognitiivista kerrosta vastaan voi kohdistua hyökkäyksenä johtoa tai muita päätöksentekijöitä kohtaan, tai vaikutusyrityksenä jollekin asiantuntijatasolle tai hyökkäyksenä kaikkia järjestelmien käyttäjiä vastaan. Hyökkäyksillä pyritään estämään esimerkiksi toiminnan oikeanlaisen tilannetietoisuuden syntyminen.

Kuvion 1 esimerkissä on esitetty tyypillisiä toimintaan liittyviä haavoittuvuuksia sijoitettuna organisaation viisiportaiseen kyberrakennemalliin (Lehto, 2014, 168).




KUVIO 1 Kybertoimintaympäristön haavoittuvuuksia

Kuvioon 2 on sijoitettu erilaisia käytännön tasolla ilmeneviä hyökkäysmalleja, niistä yleisesti käytetyillä nimillä, organisaation kyberrakenteen eri kerroksiin (Lehto, 2014, 172).




KUVIO 2 Hyökkäysmalleja kybertoimintaympäristön eri tasoille

ENISA käyttää uhka-arvioraportissaan (2012) kyberuhkamallia, joka muodostuu uhkien osatekijöistä, kuten hyökkäysmenetelmistä ja -tekniikoita, haittaohjelmista sekä fyysisen maailman uhkista. Taulukkoon 4 on koottu ENISA:n uhkamallin osatekijät: (ENISA, 2012, 13-26)

TAULUKKO 3 Kyberuhkia

| **Kyberhyökkäykset ja tekniikat** | **Haittaohjelma** | **Fyysiset uhat** |
|---|---|---|
| • Drive-by Exploits<br>• Code Injection Attacks<br>• Botnets<br>• Denial of Service<br>• Phishing Attacks<br>• Compromising confidential information<br>• Targeted Attacks<br>• Identity Theft<br>• Abuse of Information Leakage<br>• Search Engine Poisoning | • Exploit Kits<br>• Worms/Trojans<br>• Rogueware/Scareware<br>• Spam | • Physical Theft/Loss/Damage<br>• Rogue certifigate<br>• Hack- / Shack- / Lab- / Fab -hyökkäys<br>• Komponenttien vioittuminen |

ENISA painottaa kriittisen infrastruktuurin rakennetta monimutkaisena "system of systems" rakenteena. Kriittinen infrastruktuuri asettaa korkeat vaatimukset organisaatioiden järjestelmien käytettävyydelle, toimijoiden resilienssille ja kyberturvallisuudelle. Tasapaino näiden tekijöiden välillä on keskeinen toiminnallinen vaatimus. Tehtävää vaikeuttaa kokonaiskuvan muodostaminen, mikäli kokonaisuus on hajanainen. Esimerkiksi kriittisiin infrastruktuureihin toimijoiden reaaliaikainen tilannetietoisuus on tällöin perusvaatimus. Kyberhyökkäyksiä kohdistetaan jatkuvasti kriittisiin infrastruktuureihin organisaatioihin tunkeutumalla pääasiassa tietoturvapuutteita hyödyntäen tavoitteena saavuttaa hyökkäyksellä toisiinsa kytkettyjä järjestelmiä. Kyberhyökkäyksissä järjestelmien keskinäisriippuvuudet voivat aiheuttaa kaskadi-ilmiön, jossa useat yksittäiset alijärjestelmät voivat altistua hyökkäykselle ja häiriöt voivat ulottua laajalle koko kriittisessä infrastruktuurissa. (ENISA, 2012, 32)

ENISA:n raportin (2012) mukaan kriittisiin infrastruktuureihin kohdistuvat merkittävimmät uhat ovat seuraavat taulukon 3 termeillä lueteltuina: (ENISA, 2012, 32-33)

- Drive-by exploits
- Worms/Trojans
- Code Injection Attacs
- Exploit Kits
- Denial of Service
- Phishing Attacks
- Botnets

- Compromising confidential information
- Targeted Attacks
- Physical Theft/Loss/Damage

## 2.3 Kyberturvallisuus, luottamus ja organisaatio

Organisaatioiden toiminnan luottamus ja sen jatkuva ylläpitäminen tehokkailla toimenpiteillä ovat keskeisiä asioita mietittäessä kyberturvallisuuteen vaikuttavia tekijöitä. Turvallisuus perustuu luottamukseen. Jos ei ole luottamusta, ei ole turvallisuutta, ja päinvastoin. On myös hyvä tiedostaa, että täydellistä turvallisuutta ei voida saavuttaa ylipäätään, joten sitä ei voi saavuttaa myöskään kybermaailmassa toimiessa, joka on dynaaminen ja vaikeasti ennakoitavissa oleva toimintaympäristö. Näin ollen on erityisen tärkeää ymmärtää miten merkittävä asia luottamuksemme kybermaailmaan ja sen turvallisuuteen on. Luottamusta vahvistavien toimenpiteiden merkitys korostuu. Kun rakennamme kybermaailmassa toiminnot mahdollisimman kestävälle pohjalle, niin voimme hyödyntää sen tarjoamat monipuoliset mahdollisuudet. (Limnéll, Majewski & Salminen, 2014)

Suomen ensimmäinen kansallinen kyberturvallisuusstrategia painottaa yleisen kyberluottamuksen lisäämisen tarvetta läpi koko yhteiskunnan. Tasapainoista kyberluottamusta lisäävät toimenpiteet kaikilla yhteiskunnan alueilla vahvistavat tietoyhteiskunnan turvallisia toimintamahdollisuuksia, tuottavat yhteistä lisäarvoa sekä varmistavat ja lisäävät niin julkisen sektorin kuin elinkeinoelämäkin toimintaedellytyksiä. Strategia painottaa, että kullakin toimijalla, yksilöistä yrityksiin ja julkishallintoon asti, on vastuu omasta varautumisestaan kyberuhkien varalle. Myös koulutuksella ja tutkimuksella on keskeinen rooli kyberturvallisuuden ylläpitäjänä, kehittäjänä ja tiedon välittäjänä laajasti läpi koko yhteiskunnan. (Turvallisuuskomitea, 2013)

ISO/IEC 9000 -standardisarja on kasainvälinen organisaatioiden toiminnan johtamiseen liittyvä standardikokonaisuus. Sarjan standardien käyttö organisaatiossa on vapaaehtoista. Niitä voidaan soveltaa kaiken kokoisissa ja kaiken tyyppisissä organisaatioissa, joissa tavoitellaan toiminnalle jatkuvaa menestystä hyödyntämällä johtamisjärjestelmää. ISO/IEC 9000 –standardin lähtökohtana on organisaation menestyksen edistäminen siten, että se saavuttaa ja säilyttää asiakkaiden ja muiden olennaisten sidosryhmien luottamuksen. Niiden nykyisten ja tulevien tarpeiden ymmärtäminen edesauttaa organisaatiota jatkuvaan menestykseen. Yleisen laatuteorian mukaan organisaation tuotteiden ja palveluiden laatu määräytyy asiakaskokemusten kautta siten, että miten asiakas kokee tarpeensa ja odotuksensa täyttyvän. Asiakkaat myös hakevat varmistusta sille, että organisaatio pystyy tuottamaan johdonmukaisesti heidän vaatimustensa mukaisia tuotteita ja palveluja. ISO/IEC 9000-standardi sisältää seitsemän perusperiaatetta, jotka muodostavat yhteisesti hyväksytyn perustan standardisarjan sovel-

tamiselle ja perustelut organisaation hyödyille sisällytettyään ne toimintaperiaatteisiinsa. Seitsemän laadunhallinnan perusperiaatetta liittyvät asiakuuden huomioimiseen, johtamiseen, henkilöstön huomioimiseen, prosessimaiseen toimintaan, toiminnan jatkuvaan parantamiseen, faktoihin perustuvaan toiminnan ohjaukseen ja sidosryhmäviestintään. (Suomen Standardisoimisliitto, 2016)

ISO/IEC 9000-standardisarjan uusin osa (ISO/IEC 9004:2018) painottaa luottamuksen merkitystä organisaation kykyyn saavuttaa jatkuvaa menestystä ja, että johdon kaikilla tasoilla tunnistetaan organisaation toimintaan vaikuttavat tekijät jatkuvasti muuttuvassa toimintaympäristössä (International Standard, 2018). Muutoksiin sopeutuminen on ensiarvoisen tärkeää jatkuvan menestyksen kannalta. Erityisesti organisaation kybertoimintaympäristö on jatkuvassa muutostilassa. Tällöin organisaation toimintaprosessien jatkuvuuden hallinta ja sidosryhmien luottamus sen toimintaan ovat keskeisiä tekijöitä jatkuvan menestyksen aikaan saamiseksi.

### 2.3.1 Kyberluottamus ja prosessijohtaminen

Organisaation kybertoimintaympäristön turvallisuutta ja luottamusta lisäävien toimenpiteiden aikaansaaminen on ensisijaisesti organisaation ylimmän johdon vastuulla. Integroimalla tarvittavat toimenpiteet ajatukseen liiketoiminnan turvaamisesta kasvattaa niiden merkittävyyttä ja hyötyjä parantuneiden toimintaprosessien kautta koko organisaatiolle, sidosryhmille ja yhteiskunnalle. Riskitarkastelun avulla tulevat esille potentiaaliset vahingot, niiden kustannukset ja sosiaaliset seuraamukset, mikäli turvallisuus jätetään huomioimatta. Tarkastelussa esiin tulevilla johdon näkemyksillä ja vaatimuksilla on keskeinen merkitys toimintaprosessin turvallisuussuunnittelua kehitettäessä. Samalla ilmenevät myös toimintaan sitoutuvat kustannukset ja muut resurssit. (Stouffer, Falco & Scarfone, 2011)

Kun johtamista tehdään järjestelmällisesti ja laadukkaasti huomioiden asiakkaat, henkilöstön merkitys, toimintaprosessiensa tehokkuus, faktaperusteinen ohjaus, toiminnan jatkuva kehittäminen ja sidosryhmäviestintä, niin organisaatiolla on tällöin toimintaympäristöönsä yleisesti soveltuva johtamisjärjestelmä. Johtamisjärjestelmää voidaan hyödyntää myös kybertoimintaympäristön toimintaprosessien hallinnassa.

Prosessijohtamisen teoria on kehittynyt teollisen tuotannon myötä. Teollisen massatuotannon kehittyminen johti variaatioteorian hyväksi käyttämiseen kehitettäessä tuotantoprosessin ohjausta. Siinä ohjaustoimenpiteiden suorittamiseksi tuotteiden tasalaatuisuutta alettiin seurata tilastollisien menetelmin. Prosessin tilastollinen tarkastelu johti havaintoon, jonka mukaan vaihtelua esiintyy kaikkialla luonnossa ja ihmisten muodostamissa prosesseissa ja systeemeissä. Vaihtelua sisällään pitävien jakaumien tarkastelusta seurasi jako kahden tyyppiseen vaihteluun niiden syiden mukaan: ne jakautuvat yleisistä syistä johtuvaan eli systeemistä itsestään aiheutuvaan vaihteluun sekä erityisistä syistä eli nimettävistä ja tunnistettavista syistä johtuvaan vaihteluun. Systeemistä itsestään johtuva vaihtelu on satunnaisista syistä johtuvaa ja siksi usein normaalisti jakautunutta Gaussin jakauman mukaisesti. Erityisistä syistä johtuva vaihtelu ei noudata

mitään säännönmukaisuutta. Yleiset vaihtelua aiheuttavat syyt ovat siis prosessissa läsnä kaiken aikaa. Yksittäinen syy aiheuttaa vain vähäistä poikkeamaa. Erityistä vaihtelua aiheuttavat syyt puolestaan eivät ole jatkuvasti läsnä prosessissa. Ne ovat lähtöisin prosessin ulkopuolelta ja aiheuttavat yleensä enemmän vaihtelua prosessiin kuin yleiset syyt. Hallitsemattomissa prosesseissa esiintyy molemmista syistä johtuvaa poikkeamaa samanaikaisesti. (Lillrank, 1998)

Teoria prosessien toiminnan vaihteluihin vaikuttavista syistä on yleistettävissä periaatetasolla organisaation toimintaprosesseihin. Johdon suorittamat toimenpiteet voivat kohdistua molempien edellä esitettyjen syiden aiheuttamien vaihtelujen pienentämiseen. Prosessin suorituskyvyn hyvä suunnittelu ja ohjaus pienentävät satunnaisista syistä johtuvaa vaihtelua. Tavoite pienentää tätä vaihtelua on yleisellä tasolla aina suotavaa. Mikäli erityisesti yrityksen ylin johto keskittyy liikaa satunnaisista syistä johtuvien prosessivaihtelujen tarkasteluun, niin se voi johtaa valittujen toimenpiteiden aiheuttamaan ylireagointiin prosessin ohjauksessa. Pahimmillaan siitä voi olla seurauksena koko prosessin hallinnan menettäminen. Ylimmän johdon toimenpiteiden tulisikin kohdistua ensisijaisesti erityisistä syistä johtuvan vaihtelun ennalta ehkäisemiseen. Toimintaprosessissa esiintyvät vakavat kyberturvallisuuden häiriötilanteet aiheuttavat lähes poikkeuksetta toimintakatkoksia. Ne eivät edusta prosessin normaalia vaihtelua, vaan ovat erityisistä syistä johtuvia poikkeamia eivätkä siten mahdu normaalivaihtelun luonnollisiin vaihtelurajoihin. Erityissyiden huomioiminen johtamistoimenpiteitä suunnittelussa ja ennakoivassa toteutuksessa pienentää niiden aiheuttamien riskien toteutumista ja parantaa koko organisaation toiminnan luotettavuutta.

### 2.3.2 Organisaation kyberluottamusta lisäävät toimenpiteet

Millaisia toimenpiteitä voidaan liittää organisaation kyberluottamuksen edistämiseen?

P6. Pöyhönen, J., Lehto M., (2020) Cyber security; Trust based architecture in the management of an organization security. ECCWS 2020: Proceedings of the 19th European Conference on Cyber Warfare and Security. Abstrakti hyväksytty tammikuussa 2020. Artikkeli hyväksytty 28.4.2020.

Kyberturvallisuuden johtamiseen liittyviä toimenpiteitä voidaan kehittää aiemmin mainitun ISO/IEC 9000-standardin seitsemää perusperiaatetta hyödyntämällä. Standardi antaa läpinäkyvän ja tarvittaessa auditoitavan perustan organisaation luottamusta herättävän toiminnan kehittämiselle.

Organisaation kyberturvallisuuden kattava rakentaminen edellyttää ylimmän johdon määrittelemänä ja ohjaamana toimenpiteitä strategisella, operatiivisella ja teknillisellä/taktillisella tasolla. Strategisella tasolla vastataan kysymyksiin: miksi ja mitä? Operatiivinen ja taktinen taso puolestaan tuottavat vastauksen kysymykseen: miten? Kysymysten ohjaamalla ajattelulla varmistetaan, että tehdään oikeita asioita ja, että asiat tehdään asetetun tavoitetilan suuntaisesti. Teknis-taktisen tason pitää toteuttaa strategisella tasolla määritettyä tavoitteellista toimintaa, ei luoda sitä itse. Organisaation kyvykkyys toimia teknilli-

sen/taktisen tason edellyttämien kyberturvallisuustoimenpiteiden toteuttamisessa ratkaisee lopulta eteen tulevista häiriötilanteista selviytymisen. (Limnéll, Majewski & Salminen, 2014)

Kyvykkyys esiintyy käsitteenä usein organisaatioiden ja niiden henkilöstön yhteydessä. Business Dictionary.com määrittelee käsitettä siten, että yleisellä tasolla se on yksikön (osasto, organisaatio, henkilö, järjestelmä) kyky saavuttaa tavoitteensa erityisesti suhteessa sen yleiseen tehtävään ja laatuajattelussa se liittyy stabiilin prosessin ylläpitämiseen eli kokonaisvaihtelun hallintaan (BusinessDictionary.com, 2020). Kyvykkyys voidaan myös määritellä "kyvyksi saavuttaa haluttu vaikutus määritellyissä standardeissa ja olosuhteissa yhdistämällä toimintatapoja ja -keinoja suorittaa joukko tehtäviä" ja myös "kykyyn suorittaa määritetty toimintatapa" (Dickerson & Mavris, 2010). Kyvykkyydestä on myös todettu, että se on prosessien, työkalujen, taitojen ja toimenpiteiden sekä organisaation yhdistelmä, joka tuottaa määritetyn tuloksen ja muodostaessaan toimialalla erottautumista kilpailijoista, luo yritykselle lisäarvoa (Strategy&, 2012).

Organisaation kyberturvallisuuden johtamisen rakentaminen alkaa visiointi- ja strategiatyön tasoilta. Johdon laatima visiointi toimintansa kyberluottamuksen kehittämiseksi muutetaan strategisiksi tavoitteiksi, operatiivisen tason toimenpiteiksi, ohjeiksi ja toteutuspolitiikaksi. Teknillisellä/taktisella tasolla toteutetaan strategiasta johdettuja käytännön toimenpiteitä. Toimenpiteiden onnistumisen mahdollistavat organisaation kyvykkyystekijät. Visiointia tukevat strategiset valinnat liittyvät ensisijaisesti yhteiskuntavastuun, yritysmaineen, liiketoiminnan ja sen taloudellisuuden varmistamiseen. Johdolta edellytetään konkreettisia strategisia valintoja sekä niiden informointia, toimenpiteiden resurssointia ja tukemista sekä ohjaamista läpi koko organisaation. Valituista toimenpiteitä tulee viestittää kattavasti yrityksen kaikilla sidosryhmille. (Stouffer, Falco & Scarfone, 2011; Suomen Standardisoimisliitto, 2016)

Operatiivisen tason toimenpiteillä edistetään strategisia tavoitteita. Turvallisuutta ja luottamusta lisäävät toimenpiteet liittyvät organisaatiossa ensisijaisesti kokonaisvaltaiseen kyberturvallisuuden hallintaan. Tällöin toimintaprosessien riskiarvioinnit ja arvioinnin perusteella laadittavat toimenpideanalyysit muodostavat keskeisen osan hallintaa. Organisaation on myös tärkeää julistaa ja viestittää kyberturvallisuuden toimintapolitiikka, jolla johto sitoutuu hallinnan kehittämisen edellyttämiin toimenpiteisiin. Kyberturvallisuuteen liittyvä toimintapolitiikka ja toimintatapojen kehittäminen voidaan yhdistää organisaation yleiseen toimintapolitiikkaan. Operatiiviset riskitasot ja niiden hyväksynnät sekä hallintaan liittyvät toimenpiteet ja toimintapolitiikan ovat organisaation ylimmän johdon vastuulla (Stouffer, Falco & Scarfone, 2011). Operatiivisen tason konkreettiset käytännön toimenpiteet tulee kohdistaa tietoturvaratkaisujen varmistamiseen sekä liiketoiminnan jatkuvuus- ja toipumissuunnitelmien laadintaan (Suomen Standardisoimisliitto, 2012). Organisaation toimintaprosessien kybertoimintaympäristön tilannetietoisuuden ylläpitäminen puolestaan mahdollistaa operatiivisten toimenpiteiden vaikutusten seuraamisen ja tarvittaessa tehokkaan reagoinnin tapahtumiin, jotka ovat uhkana toimintaympäristössä. Tavoit-

teena tulee olla toimintaprosessien käytettävyyden jatkuva seuranta ja päätöksenteon tuenta analysointia ja päätöksiä edellyttävissä häiriötilanteissa (Faber, 2015).

Organisaation taktisella tasolla ovat ICT/ICS-järjestelmät, -laitteet ja toimintaprosessit. Niiden osalta toimintaperiaatteesta voidaan todeta, että: ”Johdonmukaiset ja ennustettavissa olevat tulokset saavutetaan vaikuttavammin ja tehokkaammin, kun toimintoja käsitellään ja hallitaan toisiinsa liittyvinä prosesseina osana yhtenäistä järjestelmää” (Suomen Standardisoimisliitto, 2016). Kyberturvallisuuden uhkat asettavat niille erityisiä vaatimuksia muiden toiminnallisten vaatimusten lisäksi. Yleisellä tasolla toimintaprosessien suorituskyvyt muodostuvat niille asetettujen asiakasvaatimusten mukaan. Tärkeimpänä vaatimuksena voidaan pitää keskeytyksetöntä tuotantoa, joka saavutetaan toimintaprosessien korkealla käytettävyysasteella. Kybertoimintaympäristössä tavoitteen saavuttaminen edellyttää suojattavien prosessien määrittämistä, prosessien ohjausmekanismien onnistunutta valintaa sekä tarkoituksenmukaisia prosesseja suojaavia teknillisiä ratkaisuja ja palveluja (Stouffer, Falco & Scarfone, 2011). Onnistuneen toiminnan edellytyksenä on organisaation henkilöstön toimintaa ohjaavien arvojen omaksuminen (Lillrank, 1998). Edellä mainituista kybertoimintaympäristöön soveltuvista ratkaisuista muodostuu kokonaisuus, jota voidaan kutsua teknilliseksi/taktiseksi tasoksi.

Kyberturvallisuuteen liittyvällä toiminnan jatkuvalla parantamisella ja henkilöstön osaamisen kehittämisellä luodaan organisaatioon aiempaa parempaa kyvykkyyttä ennalta ehkäistä häiriöitä ja tarpeen vaatiessa sietää niiden aiheuttamaa prosessin toiminnan vaihtelua. Henkilöstön huomioiminen kaikilla organisaation eri tasoilla, osaaminen ja sitä kautta avautuva mahdollisuus vaikuttaa täysipainoisesti organisaatiossa kehittää koko organisaation toimintaa (Suomen Standardisoimisliitto, 2016). Toiminnan jatkuvan parantamisen ja henkilöstön osaamisen kehittäminen tukevat strategisen, operatiivisen ja teknillisen/taktisen tason toimenpiteitä.

Jatkuvan parantamisen lähtökohtana on tarkasteltavan prosessin hyvä tuntemus. Tällöin toimenpiteet perustuvat ajatukseen, että havaitsemme prosessin vaihtelun ja pienennämme sen merkittävimpiä vaihteluja puuttumalla erityissyistä johtuvaan vaihteluun. Erityissyistä johtuvaan vaihteluun puuttuminen edellyttää usein erilaisten laadun perustyökalujen käyttöä. Niitä joudutaan yleensä käyttämään etsittäessä syitä poikkeamien muodostumiseen. Kyberturvallisuuden kehittämisen osalta organisaation prosessein jatkuva parantaminen voidaan nähdä myös ennakoivana toimenpiteenä ja siten toimintaympäristöön liittyvänä luottamusta lisäävänä toimenpiteenä. Prosessin jatkuva parantamien perustuu toiminnan jatkuvaan arviointiin. Tuotantoprosessien osalta keskeisin arviointikriteeri on sen käytettävyys. Korkean käytettävyyden toteutuminen edellyttää prosessimittareiden jatkuvaa seurantaa ja prosessien suorituskyvyn parantamisen ottamista jatkuvaksi toimintatavaksi. Oppivan ja kehityshakuisen organisaation tunnuspiirre on, että se etsii jatkuvasti kohteita parannustoimille.

Suorituskyvyn mittaamisen ja erilaisten laatutyökalujen käytön lisäksi prosessien jatkuvassa parantamisessa voidaan hyödyntää organisaation palautejärjestelmiä ja benchmarking-toimintaa. Organisaation perinteiset palautejärjestelmät, kuten organisaation sisäiset itsearvioinnit, auditoinnit ja katselmoinnit sekä ulkoiset auditoinnit tuloksineen voivat tuottaa aineistoa toiminnan kehittämiseen ja jatkuvaan parantamiseen myös kyberturvallisuuden osalta. Edellytyksenä on, että kyberturvallisuus ja siihen liittyvät luottamusta edistävät toimenpiteet liitetään toiminnan mittaamisen yhdeksi näkökulmaksi. Benchmarking-toimintaa puolestaan voidaan edistää tehokkaasti esimerkiksi perustamalla yritysten kesken toimialakohtaisia käyttäjäryhmiä ja ylläpitämällä säännöllistä tiedonvaihtoa niiden toimijoiden välillä erityisesti toimenpiteistä, jotka ovat olleet tehokkaita häiriötilanteiden selvittelyssä ja niistä toipumisessa.

Organisaation keskeisimmät resurssit ovat yleisesti ymmärrettyinä sen henkilöstö ja rahoitusvarat. Laajemmin tarkasteltuna yrityksen kokonaisresurssit muodostuvat monimutkaisesta yhdistelmästä aineellisia ja aineettomia resursseja. Edellisiä ovat näkyvät ja mitattavissa olevat resurssit, kuten rahoitus-, toimitila- ja henkilöstöresurssit sekä organisaatio. Aineettomat resurssit puolestaan muodostuvat patenteista, tuotemerkeistä, ”brändi”-nimestä, tutkimuksesta, tiedosta ja osaamisesta, toimintaverkostoista sekä organisaatiokulttuurista ja maineesta. (Hitt, Ireland & Hoskisson, 1997, 85-87.)

Organisaation aineettomien resurssien hallinta ja kehittäminen edellyttävät henkilöstön kouluttamistarpeen ja osaaminen jatkuvaa ylläpitoa. Henkilöstön osaaminen puolestaan voi määrittää lopulta koko organisaation toiminnan tason. Henkilöstöresurssien kapasiteettia voidaan kasvattaa työntekijöiden tietoja ja taitoja lisäämällä ja siten kehittämällä organisaation kyvykkyyksiä. Kyvykkyyksiin liittyvät haasteet kasvavat yrityksen toimintaympäristön monimutkaistuessa ja sen muodostuessa aina kompleksisemmaksi globalisoitumisen ja teknillisen kehityksen myötä. (Hitt, Ireland & Hoskisson, 1997, 89-82.)

Henkilöstön osaamiseen panostettavat toimenpiteet voivat muodostaa kohdeorganisaation kyvykkyydestä ydinosaamista, jolla voidaan tavoitella kilpailuetua ainutlaatuisen lisäarvon tuottamisen myötä sekä yritykselle itselleen että sen asiakkaille. Henkilöstön osaamisen kautta tapahtuva toiminnan onnistunut kehittäminen ja ylläpito voi parhaimmillaan johtaa jopa pitkäkestoiseen lisäarvon ja kilpailukyvyn tuottamiseen toimintaympäristön nopeasta muutoksesta huolimatta. Arvokkaat kyvykkyydet auttavat uhkien ja sitä kautta riskien hallinnassa ja siten ne voivat auttaa erityisesti taloudellisesti kannattavien mahdollisuuksien hyödyntämistä. (Hitt, Ireland & Hoskisson, 1997, 99-105.)

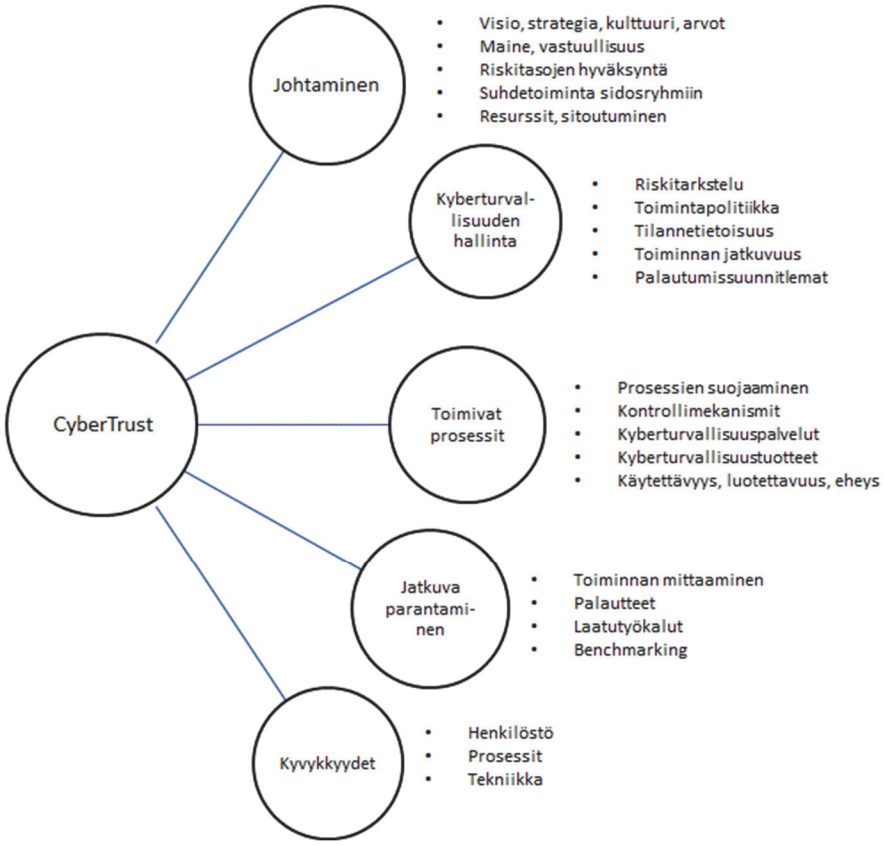
Myös kybertoimintaympäristössä organisaation kyvykkyydet liittyvän muun muassa liiketoiminnan turvaamiseen. Kyvykkyyksien katsotaan koostuvan ihmisistä, prosesseista ja tekniikasta. Niiden avulla on tarkoitus saavuttaa tuloksia tai vaikutuksia toiminta-alueella. (Jacobs, ym., 2016)

Edgar H. Shein on tutkinut yrityskulttuurin vaikutusta kehitettäessä organisaatioiden toimintaa. Hänen mukaansa kulttuurilla on merkitystä organisaatioiden kaikessa toiminnassa, koska ”kulttuuri on vahva ja usein myös tiedostamaton sarja voimia, jotka määrittävät sekä yksilö- että ryhmäkäyttäytymistämme,

käsitystapojamme, ajatusmallejamme ja arvojamme". Näin ollen kulttuurin elementit määrittävät kunkin organisaation strategiaa, päämääriä ja toimintatapoja. Organisaatioiden kehitystoimenpiteissä on siten tärkeää tiedostaa ja ymmärtää kulttuurin rooli niissä. (Shein, 2009, 29.)

Sheinin mukaan organisaatiokulttuuri muodostuu kolmesta eri tasosta, jotka ovat artefaktit, ilmaistut arvot ja pohjimmaiset perusoletukset. Artefaktit ovat organisaation näkyvät rakenteet ja prosessit. Ne on helppo havaita esimerkiksi käyttäytymismalleista, mutta niiden merkitystä on vaikea tietää. Ilmaistut arvot puolestaan koostuvat organisaation strategioista, päämääristä ja muista toiminnalle ilmaistuista perusteista. Ilmaistut arvot mahdollistavat artefaktien selittämisen tiedustelemalla miksi ihmiset tekevät asioita. Usein tässä tarkastelussa tulee esille ristiriitaisuuksia artefaktien ja ilmaistujenarvojen välillä. Näitä ristiriitaisuuksia voidaan selvittää ainoastaan pohjimmaiset perusoletusten kautta, jotka ovat tiedostamattomia, itsestään selviä uskomuksia, käsityksiä, ajatuksia ja tunteita, joista muodostuu organisaation arvojen ja toiminnan perimmäinen lähde. Ne muodostavat kunkin organisaation kulttuurin ytimen, joka pohjautuu ryhmän yhteisen oppimisprosessin kautta menestyneen toiminnan ohjaamana. Tämä kulttuurin syvin taso pohjimmiltaan selittää näkyvää käyttäytymistä. (Shein, 2009, 30-35.)

Organisaation laadunhallintastandardissa ISO/IEC 9001:2015 painopiste on luottamuksen kasvattamisessa organisaation tuotteisiin ja palveluihin (https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_9000_laadunhallinta). CyberTrust-tutkimushankkeen yhteydessä CIRP-työpaketissa kehitettiin ymmärrystä organisaation luottamuksen muodostumisesta kybertoimintaympäristössä. Vastaavasti standardissa ISO/IEC 9004:2018 painopiste on luottamuksen kasvattamisessa organisaation kykyyn saavuttaa jatkuvaa menestystä (https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_9000_laadunhallinta). Luottamuksen ylläpitäminen on siten organisaation jatkuvan menestyksen osatekijä. Väitöstutkimuksen yhteydessä on kehitetty edellä esitettyjen tekijöiden kautta organisaation kyberluottamusta lisäävistä toimenpiteistä kuvion 3 mukainen kokonaisuus. Luottamusta lisäävien toimenpiteiden tunnistamisella on ollut keskeinen merkitys koko väitöstutkimuksen osalta. Luottamukseen vaikuttavia tekijöitä on hyödynnetty myöhemmin tutkimuksessa muun muassa muodostettaessa organisaation kyberturvallisuusarkkitehtuuria.




KUVIO 3 Organisaation kyberluottamusta lisääviä toimenpiteitä.

## 2.4 Kyberturvallisuuden merkitys yhteiskunnassa

Yhteiskunnan turvallisuusstrategiassa, YTS, (2017) todetaan, että: (Turvallisuuskomitea, 2017b)

> ”Suomalaisen yhteiskunnan häiriötilanteisiin varautuminen toteutetaan kokonaisturvallisuuden periaatteella, mikä tarkoittaa yhteiskunnan elintärkeiden toimintojen turvaamista viranomaisten, elinkeinoelämän sekä järjestöjen ja kansalaisten yhteistoimintana. Suomalaisen kokonaisturvallisuuden yhteistoimintamallin vahvuus on, että se kattaa kaikki yhteiskunnan tasot ja tahot. Muuttuvan uhkadynamiikan myötä laaja-alainen yhteistyö riskianalyysissä ja tilanteenmukaiset ratkaisut korostuvat. Keskiössä on valmius joustaa yllättävissä muutoksissa ja varautua vastaamaan yhteiskuntaan kohdistuvan hybridivaikuttamisen ja kyberuhkien erilaisiin muotoihin sekä vahvistaa niissä vaadittavia suorituskykyjä.”

Kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta. Suomen ensimmäisen kansallisen Kyberturvallisuusstrategian (2013) toimintamalli noudattaa Yhteiskunnan turvallisuusstrategiassa (YTS) määritettyjä periaatteita ja toimintatapoja. Strategian mukaan kybertoimintaympäristöön tulee voida luottaa ja siinä tapahtuvat toiminnot tulee turvata. Kyberturvallisuuden kehittämi-

sen strategiset tavoitteet liittyvät tutkimukseen, koulutukseen ja tuotekehitykseen sekä siihen, että Suomi voisi toimenpiteiden avulla kehittyä yhdeksi kyberturvallisuuden johtavista maista. (Turvallisuuskomitea, 2013)

Kyberturvallisuusstrategian toimeenpano-ohjelmassa vuosille 2017-2020 todetaan, että ”valta osa yhteiskunnan digitaalisista palveluista ja niiden kyberturvallisuudesta tuotetaan elinkeinoelämän toimesta kansallisissa ja kansainvälisissä palvelukokonaisuuksissa ja verkostoissa”. Lisäksi toimeenpano-ohjelma painotetaan tavoitetta, jossa ”kansalaisten, elinkeinoelämän ja hallinnon kyberosaaminen edistää digitalisaation kehitystä”. (Turvallisuuskomitea, 2017a)

Suomen kansallisen tietoturvastrategian mukaan tietoturvallisuuden osaamiseen ja markkinoiden kehittämiseen panostaminen edistää vaikutusmahdollisuuksiamme ja asemaamme nopeasti muuttuvassa maailmanjärjestyksessä. ”Digitaalisen itsenäisyyden” turvaaminen on strategian mukaan välttämätöntä, koska sen avulla on mahdollista luoda edellytyksiä kansainvälisille markkinoille ponnistamiseen. Tietoturvastrategian mukaan ”Suomi voisi toimia kansainvälisesti turvallisen ja luotettavan kyberympäristön sillanrakentajana”. Kansallisen tietoturvastrategian visiona on se, että ”maailman luotetuin digitaalinen liiketoiminta tulee Suomesta”. Strategian tavoitteina on, että: (Liikenne- ja viestintäministeriö, 2016, 8)

- ”Suomessa on digitaalisen liiketoiminnan kannalta kilpailukykyinen ja edistyksellinen lainsäädäntö;
- EU:n sisämarkkinat toimivat nykyistä luotettavammin;
- Suomalaiset yritykset hyötyvät kansainvälisistä standardeista ja markkinoilla on saatavilla digitaalisia hyödykkeitä, joiden tietoturva on sisäänrakennettua;
- Tietoturvaa ja siihen liittyvää osaamista tutkitaan, mitataan, seurataan ja kehitetään;
- Viranomaiset auttavat yhteisöjä ja kansalaisia tietoturvan parantamisessa.”

Tutkimuksessa ”Kyberturvallisuuden strateginen johtaminen Suomessa” (2018) kyberturvallisuutta pidetään kiinteänä osana yhteiskunnan kokonaisturvallisuutta seuraavasti: (Lehto, ym., 2018, 11)

> ”Kansallinen kyberturvallisuus perustuu koko yhteiskunnan tietoturvallisuuden järjestelyihin eli kyberturvallisuuden edellytyksenä on jokaisen kybertoimintaympäristössä toimivan tahon toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut. Kyberturvallisuuden toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteistoimintaan varautumisessa. Kyberturvallisuuden strategisessa johtamisessa oleellista on digitaalisesta toimintaympäristöstä ja sen arvioidusta kehityksestä johdettujen tavoitteiden tunnistaminen ja asettaminen. Kyberturvallisuuden kansallinen strateginen johtaminen tarkoittaa Suomen kyberturvallisuusstrategian ja suomalaisen kyberturvallisuuden pitkän tähtäimen toimeenpanoa. Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista.”

Suomi on tietoyhteiskunta, jonka kriittinen infrastruktuuri ja sen palvelut ovat pitkälti riippuvaisia tietoverkkojen ja -järjestelmien toiminnasta. Nämä elintärkeät toiminnot ovat yhä useimmin kyberhyökkäysten kohteina, joten niiden toiminnan turvaaminen kaikissa tilanteissa on siten keskeistä. Martti Lehdon ja Jarno Limnéllin artikkelissa ”Kybersodankäynnin kehityksestä ja tulevaisuudesta” Tiede ja Ase lehdessä (2017) on todettu, että: ”Kyberympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella.” Toteamus kuvastaa kyberturvallisuuden merkitystä yhteiskunnan elintärkeiden toimintokojen suojaamisessa. (Lehto & Limnéll, 2017, 201)

Modernin yhteiskunnan toiminta perustuu kansallisen kriittisten infrastruktuurin useiden eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän kyberturvallisista ja siten korkean toimintavarmuuden omaavista organisaatioista ja niiden tietojärjestelmistä ja tiedonsiirtoverkostoista. Hallinnon ja kansalaisten palveluiden tietosisältöjen käytettävyys, luotettavuus ja eheys korostuvat. Kriittinen infrastruktuuri muodostaa toimintaympäristön, jonka kyberturvallisuusriskejä digitaalisen maailman uhkakuvat jatkuvasti muuttavat. Digitalisaation kehitys muuttaa globaalia toimintaympäristöä ja modernin yhteiskunnan toiminta on siten sidoksissa dynaamiseen kybertoimintaympäristöön. (Lehto, ym., 2018)

Kriittiset infrastruktuurit ovat rakenteiltaan yhä monimutkaisimpia, kompleksia ja yhä vahvemmin keskinäisriippuvaisia järjestelmäkokonaisuuksia, jonka vuoksi häiriöt yhden järjestelmän prosesseissa voivat heijastua useisiin muihin järjestelmiin. Infrastruktuurien prosessien toiminnan jatkuvuuden varmistamien ohella tuleekin eri toimijoiden kiinnittää yhä laajemmin huomiota häiriöihin varautumiseen sekä sietokyvyn (resilienssin) parantamiseen ja järjestelmäuudistuksia tehdessä uusien haavoittuvuuksien minimointiin. (Lehto, ym., 2018, 37)

Esimerkiksi EU-tasolla on tunnistettu kyberturvallisuuden laajan yhteistyön välttämättömyys terveydenhuoltoalalla. Marraskuussa 2018 ENISA:n (European Union Agency for Network and Information Security, ENISA) organisoima konferenssi (eHealth Security Conference) päätyi yhteiseen päätelmään, jonka mukaan terveydenhuoltoala on erityisen alttiina kyberturvallisuustapahtumille ja, että kyberturvallisuus on kaikkien yhteinen vastuu. Kaikkien sidosryhmien on työskenneltävä yhdessä parannettaessa potilaiden turvallisuutta. (ENISA, 2018 b)

Kyberturvallisuuden kansallisten strategiaohjelmien ja niiden johtajuuden, tavoitteiden sekä toimeenpano-ohjelman lisäksi EU-tasolle on laadittu kansallisvaltioita sitovat verkko- ja tietoturvadirektiivi. Toimenpiteet kuvastavat kyberturvallisuuden merkitystä yhteiskunnassa.

Esimerkiksi ”Verkko- ja tietoturvadirektiivi” lisää jäsenvaltioiden välistä yhteistyötä kyberturvallisuuden tärkeällä alalla. Se edellyttää toimenpiteitä myös yksityisen sektorin toimijoilta. Direktiivissä asetetaan turvallisuuteen liittyviä velvoitteita yhteiskunnan keskeisille palvelujen tarjoajille. Direktiivin so-

veltamisalueista löytyy lisäksi kohta, jonka seurauksen otetaan käyttöön keskeisiä palvelujen tarjoajia koskevat turvallisuus- ja ilmoitusvaatimukset. (Euroopan unioni, 2016)

# 3 TUTKIMUKSEN TEOREETTINEN PERUSTA

## 3.1 Tutkimuksen teoreettinen viitekehys

Open Systems Interconnection (OSI) määrittelee standardit avointen järjestelmien tietojen vaihtoon. Open Systems Interconnection Reference Model (OSI-RM) eli OSI-malli kuvaa avoimien järjestelmien tiedonsiirtoa seitsemässä kerroksessa. Kukin kerroksista käyttää yhtä alemman kerroksen palveluista ja tarjoaa palveluja yhtä kerrosta ylemmäs. OSI-malli on ISO/IEC -standardiorganisaation kehittämä kansainvälinen standardi ISO/IEC 7498-1 tietoliikennejärjestelmien suunnitteluun. Määrittely on myös saatavilla International Telecommunication Union (ITU) standardiorganisaation X.200 suosituksena. OSI-mallin kerrokset ovat: (International Telecommunication Union, 1994)

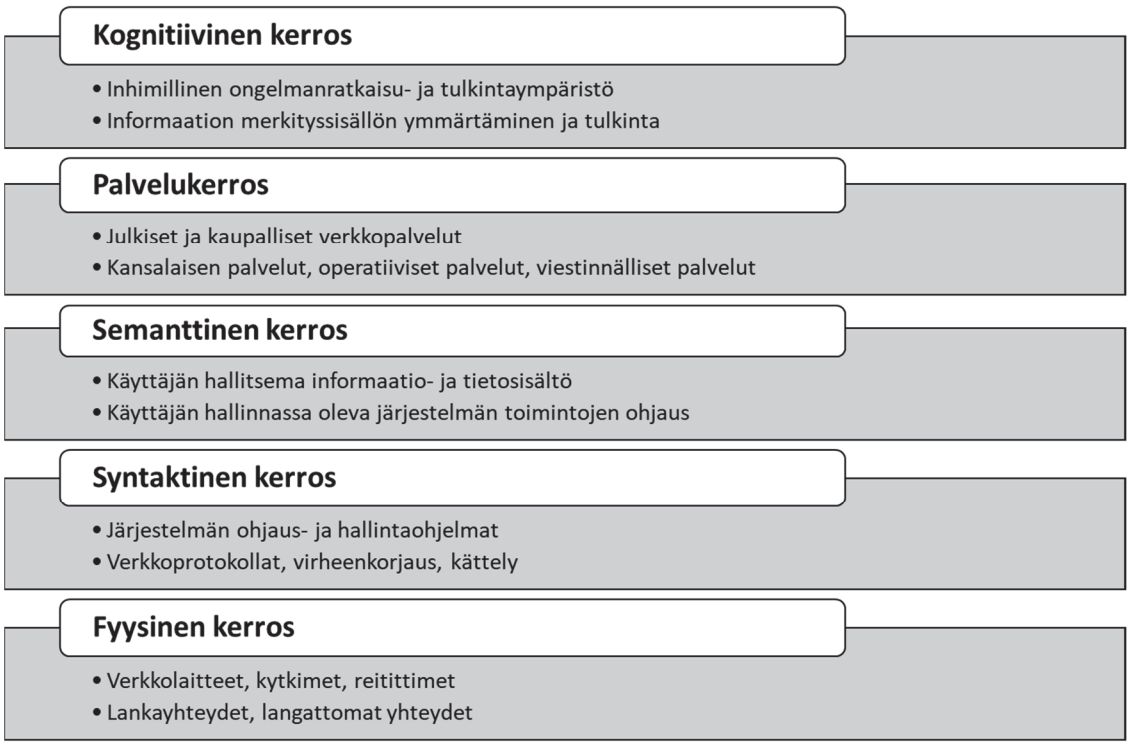
- Sovelluskerros (Application layer)
- Esitystapakerros (Presentation layer)
- Istuntokerros (Session layer)
- Kuljetuskerros (Transport layer)
- Verkkokerros (Network layer)
- Siirtokerros (Data Link layer)
- Fyysinen kerros (Physical layer)

Martin C. Libicki on luonut kybermaailmaan neljä kerroksisen hierarkkisen kyberrakenteen, jonka idea perustuu OSI-malliin (Libicki, 2007, 236-240). Libickin rakenteen kerrokset ovat:

- Kognitiivinen kerros
- Semanttinen kerros
- Syntaktinen kerros
- Fyysinen kerros

OSI-malliin pohjautuvasta Libickin kybermaailman mallista on muokattu viisikerroksinen hierarkkinen kyberrakennemalli, jossa kerroksina ovat kognitiivinen, palvelu, semanttinen, syntaktinen ja fyysinen kerros (Lehto, 2019, 14).

Rakenteen kerrokset pitävät yhdessä sisällään kokonaisuuden, jossa jokaisessa kerroksessa vaikuttavat omat digitalisaation ja kybertoimintaympäristön muokkaamat sääntönsä ja lainalaisuutensa. Kerroksien avulla kokonaisuudesta muodostuu järjestelmätasoinen rakenne, jota on pidetty tutkimuksen teoreettisena viitekehyksenä organisaation digitaalisia rakenteita tarkastellessa. Viitekehys on toiminut väitöstyön aikana siten organisaation kyberturvallisuuden käsitemallina, jonka avulla on koko tutkimusperiodin ajan (2015-2019) haettu vastauksia tutkimuskysymyksiin ja osaltaan täyttämään johdannossa esitettyä tutkimusvajetta. Rakennemalli on esitetty oheisessa kuviossa 4 (Lehto & Neittaanmäki 2018, 11, Lehto, 2019, 14).




KUVIO 4 Organisaation kybertoimintaympäristön hierarkkinen rakennemalli

Viitekehyksen rakenteen kerrokset ovat: (Lehto, 2019, 13,14)

- Kognitiivinen kerros kuvaa organisaation päätöksentekijän ja toimijan informaation ongelmanratkaisu- ja tulkintaympäristöä, maailmaa, jossa informaatiota tulkitaan ja muodostetaan henkilökohtainen tilanneymmärrys.
- Palvelukerros sisältää verkkopalvelukokonaisuudet.
- Semanttiseen kerroksen muodostavat käyttäjien eri järjestelmissä oleva informaatio ja tietosisällöt sekä erilaiset käyttäjän hallinnassa olevien toimintojen ohjaus.
- Syntaktinen kerroksen muodostavat erilaiset järjestelmien valvonta-, ohjaus- ja hallintaohjelmistot, liityntäteknologiat sekä toiminnot,

joilla verkkoon kytketyt laitteet ovat vuorovaikutuksessa keskenään, kuten verkkoprotokollat, virheenkorjaus, kättely, jne.
- Fyysiseen kerrokseen kuuluvat tietoteknilliset laitteet ja tiedonsiirtoverkon osalta sen fyysiset osat, kuten palvelimet, verkkolaitteet, kytkimet, reitittimet sekä kiinteät että langattomat yhteydet.

Väitöstutkimuksen teoreettista perustaa on seuraavissa luvuissa kuvattu organisaation johtamiseen liittyviä paradigmoja ja tämän päivän johtamismenettelyjä, avattu tutkimusaluetta teknologian ja systeemikäsityksen osilta, kuvattu kansallista kriittistä infrastruktuuria käsitteenä ja tutkimusalueena, kuvattu kyberturvallisuutta tutkimusalueena sekä avattu resiliessiä ja huoltovarmuutta käsitteinä. Lisäksi on luotu katsaus alueen normistoon ja kyberturvallisuuden edellyttämään tilannetietoisuuden tarpeeseen.

## 3.2 Johtaminen organisaatiossa

Väitöstutkimuksessa selvitetään menettelyjä kriittisen infrastruktuurin organisaation ICT-järjestelmien ja -laitteiden kyberturvallisuuden kehittämiseen tavoitteena organisaation toimintaprosessien jatkuvuuden hallinta verkottuneessa kybertoimintaympäristössä. Menettelyt liittyvät lopulta koko organisaation toiminnan johtamiseen ja sitä kautta saavutettavaan toiminnan luotettavuuteen. Hannele Seeck on teoksessaan ”Johtamisopit Suomessa” (2008) kuvannut liikkeenjohdon johtamisopeista kehittyneitä paradigmoja taylorismista 2000-luvun alkupuolen innovaatioteorioihin. Seuraavissa kappaleissa on tiivistetysti kuvattu paradigmoja ja niiden kehittymistä. Paradigmojen kehittyminen liittyy teknologiseen kehitykseen massatuotannosta tämän päivän digitalisaation muodostamaan verkottuneeseen kybertoimintaympäristöön. Johtamisen paradigmojen kehittymisen tunnistaminen auttaa ymmärtämään muun muassa organisaatioiden johtamiseen liittyvän systeemikäsitteen ja verkottuneen toimintaympäristön muodostumista. Luvun loppuosassa on perusteltu prosessijohtamisen tarpeellisuutta organisaation johtamisessa nopeasti muuttuvassa kybertoimintaympäristössä.

Hannele Seeck toteaa, että organisaatioiden johtamisoppeja kehittämistä käsittelevässä kirjallisuudessa nousee nopeaan tahtiin esille erilaisia johtamismuoteja, jotka näyttäytyvät rationaalisina, innovatiivisina ja toiminnallisina menettelyinä tavoitteenaan parantaa organisaation suoritusta. Organisaation käytäntöjä pysyvästi muokatessaan ne voivat järjestäytyä johtamistrendeiksi. Lopulta, kun johtamismuodit ja -trendit sisäistetään organisaation toimintafilosofiaan ja kulttuuriin, niistä muodostuu kollektiivista viisautta. Johtamisen opista muodostuu paradigma, kun teoriasta tulee yleisesti hyväksytty ja vuosikymmeniä hallitseva oppisuunta. (Seeck, 2008, 25-27)

Tieteellinen liikkeenjohto perustuu 1900-luvun alussa Frederick Winslow Taylorin esittämiin oppeihin työn rationalisoimisesta teollisen tuotannon tuottavuuden ja tehokkuuden parantamiseksi. Hän pyrki maksimoimaan tuottavuuden perustamalla kaiken toiminnan johtamisessa tieteelliseen tietoon työstä ja luopumaan pitkään käytössä olleista kokemukseen perustuvista, mutta epätarkoista säännöistä. Tässä niin sanotussa taylorismissa työ piti jakaa yksinkertaisiin tehtäviin, mikä aiheutti uusia menettelytapoja toimintojen koordinointiin. Koordinointi edellytti suunnittelua. Tieteellisen liikkeenjohdon tekniikkoina olivat muun muassa välineiden ja menetelmien standardisointi, hierarkkisiin osastoihin perustuva organisoituminen, aikaa säästävät työvaiheet ja -välineet, aika- ja liiketutkimukset sekä ohjekorttien käyttöä. (Seeck, 2008, 53-54)

Myöhemmin, erityisesti 1940- ja 1950-luvuilla, työ tehostamisen lisäksi alettiin tuotannossa kiinnittämään huomiota työyhteisön vuorovaikutusten kehittämiseen. Muodostui ihmissuhdekoulukunta, jonka yhteneväisyydet tieteellisen liikkeenjohdon suuntauksen kanssa liittyivät tuottavuuden lisäämiseen, yhteistyön parantamiseen työpaikoilla ja johtajan auktoriteetin oikeuttamiseen. Tieteellinen objektiivisuun oli vallitseva molempien suuntausten johtamisen oppi, mutta niissä ei juurikaan huomioitu vallitsevaa toimintaympäristöä. Ihmissuhdekoulukunta kritisoi tieteellisen liikkeenjohdon oppia työprosessien paloittelusta liian pieniin osiin ja pyrki päinvastoin laajentamaan ja rikastamaan työntekijöiden toimenkuvia sekä kierrättämään työtehtäviä yksitoikkoisuuden välttämiseksi. Nähtiin, että teknillisen kehityksen seurauksena työntekijöistä oli tulossa pikemminkin koneen osia kuin yksilöllisiä työntekijöitä. Lisäksi työntekijöitä rohkaistiin aikaisempaa enemmän vuorovaikutukseen työyhteisössä. Ihmissuhdekoulukunta näkee johtamisen työyhteisöä tasapainottavana sekä yhteistyötä ja vuorovaikutusta lisäävänä toimintana. Johtajan tärkeimpiä kykyjä ovat tavoitteiden täsmentäminen, kommunikaatiotaidot, yhteistyökyky ja siihen rohkaiseminen. Ihmissuhdekoulukunnan perintönä Suomeen muodostui 1970-luvulla henkilöstöhallintoa ja henkilöstöjohtamista korostava johtamistapa. Henkilöstöjohtamiseen liittyvät tärkeät käsiteet ovat muun muassa työmotivaatio ja työtyytyväisyys. Aiheet herättävät edelleen tieteellistä keskustelua sekä Suomessa että kansainvälisesti. (Seeck, 2008, 103-105, 120, 151-153)

Taylorismin ja ihmissuhdekoulukunnan opeilla oli pyritty kehittämään tuotannon tehokkuutta sekä työntekijöiden ja työnantajien välisiä kontakteja. Organisaatioiden kasvaessa syntyi uudenlaisia byrokratiasta aiheutuvia ongelmia. Niitä pyrittiin ratkaisemaan rakenneanalyyttisin keinoin paneutumalla suurten yritysten toiminallisiin kokonaisuuksiin. Tuottavuutta haettiin rakenteita muokkaamalla, jolloin tarkasteltiin toiminnan suunnittelua, tehtävien ryhmittelyä osastoiksi ja yksiköiksi, viestintäkanavien muodostusta sekä hierarkian ja kontrollien järjestämistä. Rakenneanalyysistä muodostui paradigma, joka pitää sisällään monia suuntauksia, joille kaikille on yhteistä rationaalinen lähestyminen organisaatioon. Organisaatio mielletään järjestelmäksi ja työntekijä järjestelmän yhdeksi osaksi. Kehitykseen vaikutti erityisesti teknologian kehittyminen ja siihen liittyvä tietokoneen tuleminen käyttöön. Toisen maailmansodan jälkeen kehittyi myös yleinen järjestelmäteoria, josta rakenneanalyyttinen paradigma sai

vaikutteita. Järjestelmäteoria pitää sisällään avoimen järjestelmän käsitteen ja toimii siten yleisenä pohjana laajalti ilmiöiden tutkimuksessa. Siitä muodostui kehittyvän johtamistieteen taustatekijä. Rakenneanalyyttinen paradigma kytkeytyy myös yhteiskunnalliseen tilanteeseen, jossa erityisesti suurten organisaatioiden osalta tarvittiin oppeja ja tekniikoita organisaation rakenteellisten ongelmien ratkaisemiseen. Tämän takia operaatioanalyysit ja johdon koulutusohjelmat yleistyivät. Rakenneteoria rantautui Suomeen 1970-luvulla ja sen vallitessa aloitettiin johdon koulutusohjelmat muun muassa Master of Business Administration eli MBA-koulutusohjelmilla 1980- luvulla. Samaan aikaan strateginen johtaminen nousi ohi rakenneteorioiden tärkeimmäksi johtamisen suuntaukseksi ja vahvistui erityisesti 1990-luvulla. (Seeck, 2008, 155-159, 180)

Kulttuuriteoriaparadigma on tuoreimpia käyttöön vakiintuneita paradigmoja organisaatio- ja johtamistutkimuksessa. Siinä organisaatioita ja johtamista tarkastellaan organisaatioiden symboleita ja merkitysjärjestelmiä tutkimalla. Lähtökohtana on, että jokaisella organisaatiolla on oma toimintaa ja ajattelua määrittävä kulttuurinsa. Kulttuuriteoriaparadigman juuret ovat 1980-luvulla, jolloin teollisuuden globaaliin kilpailuun vastaaminen alkoi muokata työyhteisöjä joustaviksi, luoviksi ja paremmin työntekijöitä motivoivaksi. Väitettiin, että organisaatiot kehittäessään rationaalisia kontrollisjärjestelmiä olivat unohtaneet moraalisen auktoriteettiasema, sosiaalisen yhtenäisyyden, laadun ja toiminnan joustavuuden merkitykset toiminnassaan. Kulttuuriteoriassa keinot liittyivätkin organisaatiokulttuurin, työntekijöiden sitoutumisen ja laadun ideologioihin. Toiminnan kulttuuria voidaan pitää organisaation ominaisuutena, jota kautta toimintaa voidaan selittää ja ymmärtää. Nähtiin myös, että aiempaa paremmin koulutettu henkilöstö sitoutuu työtehtäviin asiantuntijuuden kautta. Lojaalisuutta organisaatioon ei sinänsä voitu enää pitää itsestään selvänä. Lisäksi organisaatiokulttuurin merkitys toiminnan kehittämisessä on merkittävä, vaikka sen muuttaminen on haasteellista. Kulttuurinen muutos vaatii asioille sellaisia yhteisesti hyväksyttyjä merkityksiä, jotka voidaan sisäistää ja toteuttaa organisaation kaikilla tasoilla. Suomessa yrityskulttuuriteoriaan liittyvä tieteellisten artikkelien julkaisu on ollut vähäistä, vaikka niiden arvo onkin tunnustettu. Käännösartikkelissa korostetaan muun muassa työntekijöiden motivointia toiminnan visioinnin avulla, ihmisiä organisaation tärkeimpänä voimavarana ja johtajan sanomaa organisaation arvojen ja normien kiteyttämisessä. Kotimaisissa artikkeleissa on pohdittu erityisesti tietointensiivistä työtä, tiimityötä ja työn muuttuvia vaatimuksia. (Seeck, 2008, 203-217, 221-226, 241)

Innovaatioteoriat ovat muodostumassa nykypäivän paradigmaksi. Organisaatioilla on jatkuva tarve uusiutua ja tuoda markkinoille uusia tuotteita ja palveluja pysyäkseen mukana kilpailukykyisinä jatkuvasti ja nopeasti muuttuvassa toimintaympäristössä. Innovaatioteorioissa työntekijät nähdään yksilöinä, joilla on tarve oppia ja kehittyä pysyäkseen hyvässä markkinakunnossa. Korkea koulutustaso, asiantuntijuus ja luovuus korostuvat. Tämä pätee erityisesti tietointensiivisiin organisaatioihin, joissa hyödynnetään tietotekniikkaa. Innovaatiot liitetään pääosin tuotekehitystyöhön, johon otetaan mukaan myös kumppaneita ja asiakkaita. Teoriaa voidaankin määrittää siten, että yksilöt ja ryhmät pyrkivät

toimimaan innovatiivisesti saavuttaakseen innovatiivisen muutoksen kautta hyötyjä markkinoilla vallitsevassa kilpailutilanteessa. Paradigmaan liittyy tiimi- ja ryhmätyön käsitteet, prosessimainen toiminta ja kehitysprojektit. Suomessa innovaatioteorioista on kirjoitettu eniten 1990- ja 2000-luvulla. Tiedon, tuotekehityksen ja innovaatioiden korostaminen nähdään yritysten kilpailukyvyn ja menestyksen keksisinä edellytyksinä. (Seeck, 2008, 243-249, 259, 262-263)

Organisaatioiden toimintaympäristö ja yleisesti ottaen pärjäämisen haasteet ovat pysyvällä tavalla muuttumassa. Toimintaympäristö on kansainvälistynyt globalisaation seurauksena ja kiristänyt kilpailua. Tässä yhteydessä muina merkittävinä asiaan vaikuttavina tekijöinä voidaan mainita muun muassa digitalisaatio, Internetin ja muiden tietoverkkojen kehitys ja Internet-pohjaiset liiketoimintamallit. Organisaation menestymiseen liittyvät yhä tärkeämpinä tekijöinä kyvykkyydet, kuten osaaminen, nopeus, joustavuus ja innovatiivisuus. Toimintaympäristön osalta voidaankin puhua monimutkaisuuden lisääntymisestä. Yhä kasvavaa monimutkaisuutta ei voi hallita järjestelemällä organisaatiorakenteita yhä uudelleen tai laatimalla jatkuvasti uusia toimintasuunnitelmia. Tarvitaan uudenlaista lähestymistapaa johtamiseen. Kysymys kuuluukin: ”Miten organisaatiossa pystytään hyödyntämään kaikkien ihmisten luova potentiaali uusien parempien palveluiden ja tuotteiden luomiseksi ja tehokkaamman toiminnan kehittämiseksi?” Yksi lähestymistapa tähän haasteeseen vastaamisessa on organisaation toiminnan ymmärtäminen arvoa luovana prosessien verkkona. Ajattelu pitää sisällään muun muassa organisaation avainprosessien tunnistamisen, niiden kuvaamisen ja jatkuva intensiivinen parantamisen lisäarvon luomiseksi asiakkaalle. Siihen liittyviä toimenpiteitä suoritettaessa puhutaan prosessijohtamisesta. (Laamanen, Tennilä, 2013, 6)

Prosessijohtamisessa organisaation tavoitteet ovat edelleen samoja kuin aiemminkin. Ne liittyvät hyvään taloudelliseen tulokseen, asiakastyytyväisyyteen, tuottavuuteen ja henkilöstön huomioimiseen. Prosessijohtamisessa keinot näiden tavoitteiden saavuttamisessa liittyvät kustannustehokkuuden ohella myös toiminnan nopeutena ja joustavuutena. Keinoissa korostuvat yhteistyömenettelyt läpi organisaatiorakenteiden sekä tiimien kehittäminen ja yhteistyö kumppaneiden kanssa muodostuvissa lisäarvoa luovissa verkostoissa. Verkostomaisessa toiminnassa on luonteenomaista organisaatiorajat ylittävät toimintaketjut eli prosessit. Prosessijohtamisessa on aluksi tarve mallintaa liiketoimintaa näihin prosesseihin ja kehittää niitä. Kehitystyön ansiosta asiakkaita voidaan palvella aiempaa peremmin ja toimintaketjuja voidaan kehittää ja liiketoimintaa voidaan hallinnoida kokonaisuutena. (Laamanen, & Tennilä, 2013, 7)

Suomen ensimmäisessä kansallisessa kyberturvallisuuden strategiassa (2013) todetaan kyberturvallisuuden johtamisesta seuraavasti: (Turvallisuuskomitea, 2013, 19)

> ”Organisaation kyberturvallisuuden toteuttaminen on jatkuvan kehittämisen ja oppimisen prosessi. Se on myös johtamisen prosessi, jota toistamalla säännöllisesti turvataan tietoturvan ylläpito ja kehittäminen.”

Kyberturvallisuuden johtamisen prosessi liittyy organisaation ylimmän johdon tasolta lähtevään strategiaprosessiin, joka toimii päätöksentekomallina ja implementoi siten toiminnan päämäärät. Päämäärät ovat parhaimmillaan kirjattu organisaation visioon, joka ohjaa strategiaa, organisaation toimintapolitiikkaa ja tehtäviä. Strategiaprosessi on myös tärkeä kulttuurin muodostumisessa ja kestävässä johtamisessa. Visio on merkittävässä roolissa organisaation kehityksessä ohjaamalla toiminnan toteuttamista ja prioriteetteja. (Liao, & Huang, 2015)

Pauli Juutin ja Mikko Luoman teoksessa ”Strateginen johtaminen” (2009) todetaan, että organisaation strategian luomiselle voidaan nähdä johtamiseen liittyvää kolme pääasiallista tarkoitusta. Strategia antaa organisaatiolle suunnan, se kohdistaa ja yhtenäistää organisaation tekemistä. Sitä tarvitaan myös määrittämään organisaatiota, rakentamaan sille identiteettiä ja edelliseen liittyen strategiaa tarvitaan tuomaan johdonmukaisuutta organisaation toimintaan. Strateginen johtaminen on siten moniulotteinen ja jatkuvasti kehittyvä toiminta. Organisaatiolla voi olla useita strategioita tai strategian suuntauksia. Joka tapauksessa nykyisen näkemyksen mukaan strategiatyön tulee olla osallistavaa, henkilöstön mukaan kytkevää ja houkuttavaa. Organisaation strategiatyö on teoksessa määritelty parhaimmillaan tapahtuvaksi rationaalisen, kompleksisen ja postmodernin maailmakuvan kautta, joiden hahmottaminen edesauttaa menestymään tulevaisuuden strategiatyössä. Rationaalinen maailmankuva painottaa strategiaa johdon määrittämänä tarkoituksellisena toimintana ja tietoisena valintana organisaation menestyksen aikaansaamisessa. Kompleksinen maailmakuva puolestaan näkee organisaation johtamisen systeemisenä kokonaisuutena. Postmodernin maailmakuvan mukaan strategiatarkastelu luo merkityksiä, joita ihmiset tuottavat ja muodostavat käsitellessään organisaation toimintaa kokonaisuutena, ja ennen kaikkea se huomio asiakkaan. (Juuti, & Luoma, 2009, 26-27,29).

Juuti ja Luoma ovat määritelleet strategian ja strategisen johtaminen seuraavasti: (Juuti, & Luoma, 2009, 279)

> ”Strategia on se, mitä organisaatio tahtoo, tekee ja puhuu. Strateginen johtaminen on tuon tahtomisen, tekemisen ja puheen aikaansaamista.”

Määrittelyssä ”organisaatio” merkitsee johdon lisäksi organisaation jäseniä, sen rajapinnalla olevia ja siitä riippuvaisia tahoja (sisäisiä ja ulkoisia sidosryhmiä). ”Tahtominen” puolestaan viittaa rationaalisen ajattelun kautta tapahtuvan ideaalin muodostamiseen ja sen toteuttamispyrkimykseen. ”Tekeminen” on kompleksisuusajattelun tuottamaa vuorovaikutusta. ”Puhuminen” tarkoittaa identiteettiä rakentavien merkitysten tuottamista ja viestintää. (Juuti, & Luoma, 2009, 279)

Organisaatioiden toimintapolitiikat ovat strategioista ja perusarvoista johdettua viestintää organisaation ulkoisille ja sisäisille sidosryhmille käytännön toiminnasta. Toimintapolitiikan tarkoituksena on kertoa keskeisimmät toimintaperiaatteet ymmärrettävällä tavalla, lyhyesti ja ytimekkäästi.

Kyberturvallisuuteen liittyvän strategiatyön osalta organisaatioiden tulisi kiinnittää erityistä huomiota tietoturvapolitiikkaan, jolla se viestittää kyberturvallisuuteen ja tietoturvaan liittyvistä menettelyistä. Kyber- ja tietoturvallisuus

nähdään usein yritysstrategisella tasolla vain teknisenä asiana, jonka toteuttaminen jää yrityksen tietohallinnon vastuulle. Myös muita tiedonhallinnan menetelmiä ja käytäntöjä tarvitaan. Henkilöstöllä on merkittävä vaikutus organisaation kybertuvallisuuden toteutumisessa. Koulutuksen ohella tietoturvapolitiikan noudattaminen on turvallisuuden näkökulmasta oleellista. Ylimmän johdon, esimiesten ja tietoturvahenkilöstön tulisi viestittää tietoturvapolitiikan merkityksestä turvallisten menettelyjen ylläpitämisessä ja siten luoda organisaatiossa sosiaalista painetta kohti tietoturvapolitiikan noudattamista. Henkilöstön motivaatiolla on merkittävä vaikutus politiikan toteuttamiseen. Mitä vahvempi motivaatio on, sitä todennäköisemmin tietoturvaan liittyviä toimenpiteitä toteutetaan. (Siponen, Mahmood & Pahnila, 2014)

Kansainvälisessä organisaatioita koskevassa ISO/IEC 9000-standardisarjassa tuodaan esille, että laadunhallinta (Quality Management, QM) kuuluu osaksi laadukasta organisaation johtamista. Se on silloin osana organisaation johtamisjärjestelmää. Johtamisjärjestelmä on organisaation toiminnan ja johtamisen kuvaus. Johtamisjärjestelmä ei ole sama kuin standardi. Sen sijaan standardit tarjoavat kehyksen organisaation toiminnan tehokkaalle johtamiselle ja jatkuvalle parantamiselle. Toiminnan jatkuva parantaminen ja laadunhallinta tulee toteuttaa ensisijaisesti organisaation toiminnallisten prosessien hallinnan kautta (ISO/IEC 9000: 2015, 11). Tällöin toiminnan laatua voidaan myös arvioida ja mitata prosessien kautta. Myös organisaation ICT-järjestelmien ja -laitteiden kyberturvallisuuteen liittyvien prosessien ja menettelyjen osalta väitöstutkimuksessa on ollut tarve kartoittaa käyttöön soveltuvia alan standardeja, joiden perusteella toimintaa voidaan kehittää ja, joita vasten toiminnan sertifiointi voidaan rakentaa. Sertifiointi antaa laadunvarmistuksen näkökulmasta organisaatiolle ulkopuolisen toimijan, auditoijan, todentamana käsityksenä kehitystoimien tilanteesta. Auditointien ja sertifioinnin kautta toiminta ja sen kehittäminen kytkeytyvät myös organisaation johtamisjärjestelmään.

Väitöstyössä organisaation johtamiseen liittyviä kyberturvallisuuden kehittämisen menettelyjen mittaamista ja tilannetietoisuutta on tarkasteltu organisaation strategiselta, operatiiviselta ja taktiselta päätöksentekotasolta.

Väitöstyön tavoitteena on luoda kriittisen infrastruktuurin organisaatiolle edellytyksiä kyberturvallisuuden edellyttämien kehittämis- ja oppimisprosessien liittämiselle koko organisaatioin johtamiskäytäntöihin. Johtamisen näkökulmasta luotu toimintamalli sen ja kyberturvallisuuden kehittämisen välinen menettelykuvaus, joka voi toimia geneerisenä mallina kansallisen kriittisen infrastruktuurin organisaatiokentässä.

## 3.3 Teknologia ja systeemi tutkimuskohteena

Organisaation toimintaympäristöä muokkaavat erityisesti globalisaatio ja teknologian kehitys. Globalisoituminen merkitsee toimimista avoimilla kilpaillulla markkinoilla kansainvälisiä normeja noudattaen. Teknologia puolestaan on muokannut markkinoita ainakin kolmella tavalla. Ensinnäkin se on lyhentänyt

tuotteiden elinkaaria, toisaalta teknologia on luonut informaatioyhteiskunnan uusine markkinoineen ja kolmanneksi tiedon määrä ja tiheys yhteiskunnassa ovat kasvaneet nopeasti. (Hitt, Ireland & Hoskisson, 1997, 9.)

W. Brian Arthur on pyrkinyt rakentamaan kuvausta teknologian evoluutiota teoksessaan ”The nature of technoly” (2009). Hänen ajatuksensa mukaan uudet teknologiat eivät synny tyhjästä keksintöjen muodossa, vaan ne koostuvat aiemmista teknologioista. Ajattelu pitää sisällään kolme perusperiaatetta, joista ensimmäinen on, että kaikki teknologiat ovat kombinaatioita käytettävistä olevista komponenteista tai kokonaisuuksista tai alajärjestelmistä. Toiseksi kukin teknologian osa-alue on sellaisenaan pienoisteknologia, jolloin teknologian rakenteesta muodostuu rekursiivinen. Kolmannen periaatteen mukaan kaikki teknologiat valjastavat ja hyödyntävät jotakin ilmiötä, ja yleensä useita ilmiöitä. (Arthur, 2010, 28)

Evoluutiossaan uudet teknologiat muodostuvat siten, että ne käyttävät suoritettavaan tehtävään jotakin uutta tai aiemmasta poikkeavaa periaatetta. Teknologioiden lukumäärän kasvaessa myös kombinaatioiden lukumäärät kasvavat. Kehittyessään ne muodostavat uudessa kokoonpanossaan aiempaa syvempiä rakenteita. Uusissa teknologioissa otetaan käyttöön uusia komponentteja tai alajärjestelmiä ja siten parannetaan perustason suorituskykyä, sopeudutaan aiempaa laajempaan tehtäväkenttään tai parannetaan teknologian turvallisuutta ja luotettavuutta. Teknologioiden rakenteet monimutkasituvat. (Arthur, 2010, 104-105, 129, 188-189)

### 3.3.1 Teknologia käsitteenä

Teknologia ja tekniikka käsitteiden käyttö on muotoutunut suomen kielessä tilannekohtaiseksi ilman, että niitä kumpaakaan olisi varattu tarkasti ja ehdottomasti tiettyyn tarkoitukseen. Tässä tutkimuksessakin käsitteitä käytetään yleisesti vakiintuneen käytännön mukaisesti asiayhteyteen ja sanojen normaaliin käyttöön liittyen.

Tarmo Lemolan kokoamassa teknologian ja yhteiskunnan suhdetta käsittelevässä teoksessa ”Näkökulmia teknologiaan” (2000) on myös käsitelty edellä mainittujen sanojen käyttöä teoksen eri kirjoituksissa. Hän on todennut niiden esiintyvän synonyymeinä tai, että erotuksena teknologiasta tekniikalla tarkoitetaan artefakteja. Samaiseen teokseen kirjoittanut Ilkka Niiniluoto on määritellyt tekniikan olevan sellaisten välineiden käyttöä, joilla uskomme olevan arvoa tavoitteidemme saavuttamisessa (Niiniluoto, 2000, 25). Niiniluodon määritelmä tekniikasta tukee sen artefaktista luonnetta.

Timo Airaksinen (2003) on määritellyt teknologian tarkoittavan tekniikan järjestelmien suunnittelua, rakentamista, käyttämistä ja tutkimista; kaikkia yhdessä. Teknologiaan liittyy siten kokonaisuuden käsitys ja kokonaisnäkemys tekniikan maailmasta, joten se pitää sisällään systeemi- tai järjestelmäajatuksen. Teknologia on samaa asiakokonaisuutta kuin tekniikka, joten sen avulla ei tutkita tekniikkaa kohteesta irrallisen ja ulkopuolisena toimiojana kuten tiede tekee vas-

taavassa tilanteessa tutkiessaan jotakin erityistä tutkimusaluetta. Näin ollen teknologia ei sanan luonteesta huolimatta kuitenkaan merkitse tekniikan tutkimusta tieteenä. (Airaksinen, 2003, 17.)

Airaksinen (2006) toteaa lisäksi, että tekniikan on totalisoiva resurssi. Se tarkoittaa, että jos tekniikka on käyttäjällä käytössä, niin se on sitä koko laajuudessaan. Muuta vaihtoehtoa ei ole. Tekniikka ei siten ole pelkästään työkaluja ja koneista eli artefakteja, vaan se muodostaa järjestelmän, joka on luonteeltaan laajasti ajateltuna heterogeenisten järjestelmien järjestelmä. Airaksisen mukaan se koostuu talouden, politiikan ja muiden järjestelmien yhdistämisestä monimutkaiseen tekniikan järjestelmien verkostoon. (Airaksinen, 2006, 233-234)

Järjestelmien järjestelmä voi olla määritelty myös teknillisten järjestelmien järjestelmäksi (System-of-Systems, SoS). SoS:lle on olemassa kirjallisuudessa runsaasti määritelmiä, jotka rakentuvat asiayhteyteen liittyvän näkökulman mukaan. Yleistettynä ja käytännön läheisenä määritelmänä voidaan pitää seuraavaa kuvausta: (Jamshidi, 2008, 4)

> ”Järjestelmien järjestelmä (System of Systems) koostuu alisysteemien muodostamista elementeistä, jotka ovat jo itsessään itsenäisesti ja monimutkaisesti toimivia järjestelmiä, ja toimiessaan keskenään vuorovaikutuksessa ne saavat aikaan yhteisen päämäärän mukaisen toiminnon.”

Informaatioteknologiasta löytyy runsaasti esimerkkejä järjestelmien järjestelmästä. USA:n puolustusministeriön alueen suunnitteluohje luokittelee ne neljäksi eri tyypiksi, jotka ovat ohjattavat, vastaanottavat, yhteiskäyttöiset ja virtuaalit järjestelmäkokonaisuudet. Konkreettisena esimerkkinä SoS:sta toimii eri asevoimien tilannekuva- ja johtojärjestelmät, jotka tyypillisesti sisältävät valvonnan, tiedustelun, johtamisen ja tiedonsiirron elementtejä. Jokainen näistä elementeistä toimii itsenäisesti, mutta niiden toiminnan lopputuloksena on johdolle muodostuva reaaliaikainen päätöksenteon ja johtamisen mahdollistava yhteinen tilannetietoisuus. (Department of Defense (DoD) USA, 2008, 4-5)

Airaksisen (2003) mukaan teknillinen kehitys on tapahtunut teknologian ja tekniikan välineistämässä maailmassa. Hänen tekniikan kehitystä luotaavassa filosofisessa raportissa todetaan, että tekniikan muutoksen luonteen voidaan katsoa olevan hyvin pitkälle deterministinen. Tällä tarkoitetaan sitä, että muutokset ovat määräytyneet yleisesti ottaen joistakin tekniikan näkökohdista käsin. Hänen mukaansa determinismiä ei kuitenkaan pidä ajatella voluntarismin vastakohdaksi. Ne voivat vaikutta yhdessä, koska esimerkiksi yhteiskunnallisilla valinnoilla voidaan joissakin tapauksissa vaikuttaa realistisesti teknillisiin ratkaisuihin vaikkakin determinismissä on kausaalista kehitystä, joka tekee joissakin tapauksissa valinnat mahdottomiksi. Kehityskulkua, jossa kausaalisen määräytyneisyyden lisäksi myös vapaa tahto on olemassa, hän kutsuu kausaalisen determinismin ja vapaan tahdon yhteensopivuuden teoriaksi. (Airaksisen, 2003)

Mikäli jokin valittu teknillinen ratkaisu johtaa toisaalla tai myöhemmin toisen alueen teknillisen ratkaisun käyttöönottoon, niin näin muodostuva suhde on teknodeterministinen. Airaksisen mukaan tekniikan kehityskulkuja kuvaavat myös käsitteet internalistinen ja eksternalistinen kehitys. Internalistinen teesi sanoo, että tekniikan sisäiset syyt ohjaavat tekniikan kehitystä. Eksternalistinen

teesi puolestaan sanoo kehitykseen vaikuttavan tekniikan ulkopuolisia syitä, joiden pakottamana joudutaan luomaan uusia ratkaisuja. (Airaksinen, 2003, 152-153.)

Deterministisestä kehityskulusta on Airaksisen mukaan lähiajan historiassa kylläkin ollut myös erilaisia näkemyksiä. Katsantokannat ovat vaihdelleet erityisesti toisen maailman sodan jälkeisessä tekniikan kehityksen tutkimuksessa. Viime vuosien informaatioteknologian nopea ja voimakas kehitys puoltaa ainakin alueen kehityksen olevan osin deterministinen. Se tarkoittaa kehitystä, jossa tekniikka muuttaa yhteiskuntaa, sen arvoja ja toimintatapoja väistämättömästi.

Airaksisen esittämillä tekniikan filosofiaan liittyvillä ajatuksilla ja määritelmillä on tärkeä merkitys digitalisaation aikaansaaman informaatioteknologian kehityksen ymmärtämisessä kohti globaalia kyberavaruutta ja -maailmaa. Kehityskulkuun ovat vaikuttaneet eri teknologiaohjelmien ja -hankkeiden kautta kehitetyt tekniikat, joista on jatkokehittynyt järjestelmiä ja laitteita, joita vuorostaan on integroitu aina vaan isommiksi kokonaisuuksiksi ja niiden muodostamiksi verkostoiksi. On helppo ennustaa kehityksen jatkuvan edelleen kohti yhä laajempaa informaatioteknologista integraatiota kaikkine tarvittavine palveluineen ja säätelyineen. Kehitys on siten ollut ainakin aluksi valinnainen ja internalistinen, kun etenemispolkuja on etsitty muun muassa vaikkapa eri teknillisiä standardeja valitessa. Tämän jälkeen kehitys on ollut nopeaa ja se on saavuttanut tason, jota hyvin kuvaa tilastot esimerkiksi Internetin nykyisestä käyttölaajuudesta. Se todistaa, että perusratkaisut sekä informaatioteknologia, että siihen liittyvien eri tekniikoiden osalta ovat toimivia. Alueen kehityksen voi nykyään siten arvioida olevan pitkälti determinististä ja sen voi arvioida olevan sitä myös tästä eteenpäin, koska on vaikea nähdä jatkossa merkittävimpien teknillisten muutosten määräytyvän muutoin kuin informaatioteknologian omista lähtökohdista käsin. Eksternalistista kehityksestä ei kuitenkaan voi unohtaa. Siitä on näkyvissä merkkejä ainakin yhteiskunnan säätelyn lisääntyessä kehityksen edetessä ja tietoverkostojen saavuttaessa yhä laajempia käyttäjäkuntia ja -määriä. Turvallisuuskysymykset ovat tästä esimerkkinä. Yhteiskunta on määritellyt kyberturvallisuuteen kuuluvia toimenpiteitä strategiatasolla, alueelle on perustettu viranomaisorganisaatioita ja toimintaan ohjaavia lakeja on valmistelussa ja osin jo käytössä. Kehitys on globaalia ja sen vuoksi sillä on väistämättä vaikutuksia teknillisiin ratkaisuihin.

### 3.3.2 Systeemi ja systeemiajattelu

Sanalle ”systeemi” on suomen kielessä synonyymi ”järjestelmä” (suomisanakirja.fi). Käsitteen systeemi tausta on kreikankielisessä sanassa ”systema”, joka tarkoittaa osista muodostuvaa kokonaisuutta; aineellista tai aineettomaa.

Systeemi voi olla kokonaisuus tai koostua rajatusta määrästä omista pienemmistä systeemeistä eli alasysteemeistä. Systeemin ominaisuus on määriteltävissä oleva yhtenäinen kokonaisuus, jonka osat ovat hierarkkisessa suhteessa toisiinsa. Systeemi voi olla joko luonnon tai ihmisen luoma fyysinen, abstrakti tai inhimillisen toiminnan muodostama kokonaisuus, jolla on selvät rajat toimin-

tansa ympäristöön. Suunnitellut fyysiset systeemit muodostuvat tietoisen toiminnan tuloksena. Esimerkiksi sähkönjakeluverkosto on tietoisen suunnittelun tuloksena syntynyt järjestelmä. Suunnitellut abstraktit systeemit ovat laajempia ihmisen tekemiä kokonaisuuksia, jotka voivat koostua myös tietoisesti rakennetuista käsitteellisistä kokonaisuuksista. Esimerkiksi yhteiskunnan poliittinen järjestelmä on suunniteltu, mutta abstrakti. Inhimillisen toiminnan tuloksena syntyy toiminnallisia järjestelmiä tietoisesti. Ihmiset muodostavat järjestelmiä jotain tarkoitusta varten ja jolla on jonkin päämäärä. (Checkland, 1985, 110-121)

Pääasiallisesti systeemit voidaan jakaa kahteen pääryhmään; luonnollisiin systeemeihin (natural systems) ja suunniteltuihin systeemeihin (designed systems). Luonnolliset systeemit käsittävät kokkonaisuuksia, jotka ulottuvat alkuainejärjestelmästä aina aurinkokuntaamme, galaksijärjestelmiin ja lopulta koko maailmankaikkeuteen. Suunnitellut systeemit ovat ihmisten aikaan saamia kokonaisuksia. Ne voidaan jakaa edelleen useisiin tyyppeihin: (Banathy, 2004)

- ”Rakennetut, mekaaniset, fyysiset järjestelmät eli ihmisen tekemät artefaktit.”
- ”Hybridijärjestelmät, jotka ovat yhdistelmiä fyysisistä rakenteista ja luonnosta, joita ovat esimerkiksi vesivoimalat.”
- ”Suunnitellut käsitteelliset järjestelmät, kuten muun muassa teoriat, filosofiat, logiikat ja matematiikka. Niiden esitykset kirjojen, levyjen sekä kuvan deskriptiivisten ja preskriptiivisten mallien muodossa.”
- ”Ihmisen toimintajärjestelmät.”

Systeemit voidaan jakaa myös avoimiin ja suljettuihin systeemeihin ja niiden määritelmiin seuraavasti: (Peltoniemi, ym., 2004)

> “Avoin systeemi on jatkuvassa vuorovaikutuksessa ympäristönsä kanssa. Se vaihtaa ympäristönsä kanssa materiaalia, informaatiota ja energiaa, jota se käyttää järjestyksensä ylläpitämiseen. Suljettu systeemi ei vaihda ympäristönsä kanssa energiaa, materiaalia eikä informaatiota. Se on täysin eristetty ulkopuolisesta maailmastaan.”

Systeemi muodostama kokonaisuus koostuu hierakisesti eritasoisista osista, osajärjestelmistä. Mitä ylempänä systeemin hierarkiassa ollaan, sitä abstraktisemmiksi ja holistisemmiksi kokonaisuus muuttuu, ja sitä enemmän ilmiöiden osiin ja yksityiskohtiin liittyvää informaatiota menetetään. Alemmilla tasoilla voidaan erottaa monimuotoisuutta, joka ei havaita systeemin ylemmällä tasolla. Toisaalta alimmilla tasoilla voidaan menettää näkymän ylemmältä tasolta ja siten tilannekuva kokonaisuudesta. Tämä johtuu siitä, että aina ei ole mahdollista saada yhtenäistä informaatiota koko systeemistä eikä siten hahmottaa jokaiselta tasolta systeemissä esiintyviä riippuvuuksia kokonaisuuteen ja muihin järjestelmiin. (Lehto, 2008)

Systeemitarkastelun aihepiiri määrittää pitkälti myös sen, miten tutkittavaa asiaa lähestytään. Teknologia avulla muodostuu systeemejä (Airaksinen, 2006, 18-19). Systeemeiksi voidaan käsittää, teknillisten järjestelmien muodostavien kokonaisuuden lisäksi, erilaista olioista tai ilmiöistä koostuvina kokonaisuuksina

tarkastelu- tai tutkimusnäkökulman mukaan. Tämän tutkimuksen näkökulma on teknillisten järjestelmien muovaamissa systeemeissä.

Rauno Pirinen ja Jyri Rajamäki ovat todenneet teknilliseen systeemikäsitykseen ja tämän tutkimuksen alueeseen liittyen, että yhteiskunnan kriittisen infrastruktuurin digitaaliset palvelut muodostavat teknillisesti monimutkaisen ja kompleksisen verkottuneen kokonaisuuden. He ovat määritelleet sen systeemiksi, joka on ohjelmistointensiivisten alajärjestelmien järjestelmä. Siinä alustakerrokset muodostavat fyysisen verkon, ohjelmistokerrokset käsittävät ohjelmistoverkon ja ihmiskerrokset muodostavat sosiaalisen verkon. Fyysinen verkko on perusta, jolla informaation jakaminen eri sidosryhmien välillä voidaan toteuttaa ohjelmistokerrosta hyödyntämällä. Sosiaalinen verkosto määrittelee verkon ja informaation käyttöä. Näin muodostuvan digitaalisen systeemin kyber- ja tietoturvan suunnittelu on haastavaa, koska tekniikat muokkaavat jatkuvasti digitaalisen datan jakamista. Uudet teknilliset edistysaskeleet laitteistoissa, verkottumisessa, informaation käsittelyssä ja ihmisen käyttöliittymissä vaativat turvallisuuteen uusia ajattelu- ja toteutustapoja. Niissä korostuvat esimerkiksi suunnittelun, rakentamisen, toiminnan arvioinnin ja käsitteellistämisen merkitykset resilientin digitaalisen palvelun ja systeemin aikaansaamiseksi. Luottamuksen ja kyberturvallisuuden näkökohtien huomioiminen tulisi toteuttaa järjestelmän kaikille tasoille ja toimintaan liittyville verkostoille. (Pirinen & Rajamäki, 2015)

Peter Checkland on teoksessaan ”System thinking, System practice” (1981) käsitellyt systeemiajattelun hyväksikäyttöä tieteellisessä tutkimuksessa klassisen tiedeajattelun lisäksi. Hän toteaa, että laajoissa systeemeissä, jota on muun muassa teollisuudessa, liiketoiminnassa, hallinnossa ja puolustuksessa, esiintyy usein monitahoisia, kompleksisia ongelmia. Tällöin näihin liittyvissä ongelmaratkaisuissa ratkaiseva lähestymistapa voidaan löytää tieteellisen mallin muodostamisesta tarkastelun kohteena olevasta systeemistä. Hän käsittelee samaisessa teoksessa pehmeän systeemitarkastelun teoriaa tapauksiin, joissa maailma muodostuu ihmisistä, jotka tekevät erilaisia asioita prosessissa.

Pehmeässä systeemiajattelussa ihmisien muodostamassa toiminnassa jokaisella yksilöllä on oma tulkintansa tarkasteltavasta maailmasta. Jakamalla se osiin ja kutsumalla näitä osia järjestelmiksi voimme välittää ymmärrystämme tästä maailmasta. Tämän rationaalisen ajattelun avulla voimme oppia jotain osajärjestelmiin jaetusta maailmasta ja tämän jälkeen voimme hyödyntää tekniikkaa auttamaan ihmisiä tekemään asioita paremmin. Pehmeän systeemiajattelun vastakohtana voidaan pitää kovaa systeemiajattelua, jonka mukaan maailma koostuu järjestelmistä, jotka voidaan kuvata formaalien notaatioiden avulla. Tällöin rationaalista analyysiä voidaan käyttää järjestelmien ymmärtämiseen, jolloin niihin liittyvät ongelmat voidaan tunnistaa ja ratkaista teknisesti. Kovassa systeemiajattelussa muuttujat esitetään määrillisessä muodossa ja ihmisiä pidetään passiivisina ja ilman tahtoa olevina objekteina, jolloin voidaan olettaa, että ”päätöksentekijöillä on valtaa ottaa käyttöön mitä tahansa ratkaisuja”. (Peltoniemi ym., 2004)

Perinteinen klassinen tiede perustuu käsitykseen, jonka mukaan jokainen järjestelmän muutos voidaan esittää järjestelmässä eräänlaisena tilojen ketjuna,

jotka noudattavat muuttumattomia luonnon lakeja niin sanottujen siirtofunktion mukaisesti. Perinteinen klassinen tiede soveltuu kovan systeemiajattelun ongelmien ratkaisemiseen. Pehmeän järjestelmäajattelun mukaan klassisen tieteen ”syy ja seuraus -periaate” on riittämätön kompleksisten järjestelmien tarkasteluun (Banathy, 2004). Kompleksisten järjestelmien muutokset eivät aina noudata ennustettavia ja jäljitettävissä olevia luonnon lakeja. Järjestelmäajattelun mukaan monimutkaisten ja siten usein myös kompleksisten prosessien käyttäytyminen ei ole koskaan täysin ennustettavissa.

Systeemiä tarkasteltaessa on huomionarvoista, että se sisältää hierarkiaa, jossa kukin osa voi muodostaa oman systeeminsä. Osista muodostuva systeemi on sellaisenaan jotain enemmän kuin osiensa summa. Hierarkkisuuden lisäksi osat muodostavat myös prosesseja ja niiden väleillä on vuorovaikutusta. Avoimena systeemissä hierarkian ylläpitäminen edellyttää sen prosesseissa informaation vaihtoa ympäristönsä kanssa toiminnan säätämiseen tai ohjaamiseen. Tämä johtaa systeemin muutoksiin, joita sitä tulee tarkastella kokonaisuutena. (Checkland, 1981, 74-92)

Systeemin teknilliseen konfiguraatioon liittyy lähes aina suunnittelun mukanaan tuomaa monimutkaisuutta. Systeemin hierarkkisuus, avoimuus ja informaation vaihto ”system of systems”-rakenteessa kasvattaa teknillisen järjestelmän monimutkaisuutta. Systeemin tarkastelu kokonaisuutena merkitsee myös siihen liittyvien sidosryhmien huomioimista. Tällöin systeemin toiminnallisuuden ennakoitavuus vaikeutuu, koska eri sidosryhmien käyttäytymistä ei voi täysin tietää. Monimutkaisuuden lisäksi järjestelmään muodostuu kompleksisuutta. (Kuusisto, 2018)

Anita Rubin on artikkelissaan Pehmeä systeemimetodologia (SSM) 2014 todennut, että ”kompleksisella systeemillä, tilalla tai kokonaisuudella tarkoitetaan erilaisista osista, kuten systeemin elementeistä, tapahtumista, vaikutus- tai tapahtumaketjuista erottamattomaksi kietoutunutta kokonaisuutta, johon liittyy informaation ja, jota on työlästä eritellä, analysoida tai ratkaista”. Hänen mukaansa systeemin toimintojen osalta kaikki informaatio ei ole saman arvoista. Sen sijaan ”kriittisellä informaatiolla tarkoitetaan sellaista informaatiota, joka vaikuttaa systeemiin ja jonka käsittelemiseksi siinä ei välttämättä ole valmiita keinoja”. Informaation määrä ja lisääntyminen systeemissä voi luoda epävakautta ja sen takia systeemi voi vähitellen lähestyä kaoottista tilaa. ”Systeemin kyky itsensä säätelyyn määrää sen järjestyksen asteen”. (Rubin, 2014)

Systeemiajattelussa kaoottiselta tuntuva kokonaisuus ei ole erillinen ilmentymä eikä omien lakiensa mukaan toimiva kokonaisuus. Kaoottinen tilaa liittyy pikemminkin keskenään vuorovaikutuksessa olevien kompleksisten systeemien kokonaisuuteen. (Checkland, 1985, 102)

Lähtökohtana on, että ihmisen tekemä systeemi kehittyy aina kohti suurempaa kompleksisuutta. Systeemin elementit, tapahtumat, vaikutus- tai tapahtumaketjut ovat muutoksenkin jälkeen edelleen nähtävissä, mutta niiden lisäksi muutos tuo siihen uusia ominaisuuksia, joka muuttavat näiden elementtien merki-

tyksen ja keskinäisen suhteen toisenlaiseksi. Ongelmaksi muodostuu se, että miten systeemiä ja sen muutosta hallitaan. Erityisesti tämä koskee sosiaalista muutosta. (Checkland, 1985, 94)

Avoimen systeemin osalta muutokseen liittyy informaation määrän kasvaminen, joka avaa monia vaihtoehtoisia polkuja systeemin kehitykselle tulevaisuudessa. Erityisesti sen ohjausjärjestelmässä (johtamisessa), sisäisissä järjestelmissä, alasysteemeissä ja sitä kautta totutuissa toiminnan muodoissa tapahtuu muutoksia. Samalla ennakoimattomuus, hämmennys ja epävarmuus lisääntyvät. Kaiken kaikkiaan muutoksessa edelleen kasvavat sekä systeemin sisäinen kompleksisuus että siitä johtuvat kompleksiset ongelmat. Pehmeä systeemimetodologia kehitettiin erityisesti laajojen ja kompleksisten ongelmien ymmärtämiseksi. Tähän pehmeä systeemimetodologia (Soft Systems Methodology, SSM) antaa hyvän työkalun. (Rubin, 2014)

## 3.4 Kansallinen kriittinen infrastruktuuri

Kansallista kriittistä infrastruktuuria ei ole määritelty Suomessa erikseen lainsäädännön tasolla. Yhteiskunnan elintärkeät toiminnot on kuitenkin määritelty yhteiskunnan turvallisuusstrategiassa (YTS) vuodelta 2017. Se on valtioneuvoston periaatepäätös, joka yhtenäistää varautumisen kansallisia periaatteita ja ohjaa hallinnonalojen varautumista. Turvallisuusstrategiassa todetaan, että ”suomalaisen yhteiskunnan elintärkeitä toimintoja ovat valtion johtaminen, kansainvälinen ja EU-toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys”. Turvallisuusstrategian mukaan elintärkeät toiminnot rakentuvat muun muassa tieto- ja viestintäjärjestelmien ja digitaalisten palvelujen varaan. (Turvallusuuskomitea, 2017b).

Valtioneuvosto on käsitellyt maan huoltovarmuuden tavoitteista vuonna 2013. ”Valtioneuvoston päätös huoltovarmuuden tavoitteista” pitää sisällään keskeisiä yhteiskunnan toimintakykyä vaarantavia uhkia, jotka liittyvät informaatioteknologiaan, energia-alaan, terveyteen ja infrastruktuurin toimivuuteen. Päätöksessä kriittisen infrastruktuurin turvaaminen on jaoteltu seuraavasti: (Valtioneuvosto, 2013)

> ”Energian tuotanto-, siirto ja jakelujärjestelmät, tieto- ja viestintäjärjestelmät, -verkot ja -palvelut, finanssialan palvelut, liikenne ja logistiikka, vesihuolto, infrastruktuurin rakentaminen ja kunnossapito sekä jätehuolto erityistilanteissa."

Päätöksessä todetaan lisäksi, että kriittisimmät ja keskeisimmät tietotekniikan varassa olevat yhteiskunnan toiminnot tulee tunnistaa ja niihin liittyvät tietojärjestelmäratkaisut ja -palvelut tulee varmistaa erilaisia vakavia häiriöitä ja poikkeusoloja kestävillä järjestelyillä. (Valtioneuvosto, 2013)

Euroopan neuvosto hyväksyi 17. toukokuuta 2016 virallisesti uudet säännöt verkko- ja tietojärjestelmien turvallisuuden parantamiseksi koko EU:ssa. Verkko-

ja tietoturvadirektiivi (NIS-direktiivi) lisää jäsenvaltioiden välistä yhteistyötä kyberturvallisuuden tärkeällä alalla ja siinä asetetaan turvallisuuteen liittyviä velvoitteita keskeisten palvelujen tarjoajille ja digitaalisten palvelujen tarjoajille. Direktiivin määrittelemä luettelo yhteiskunnan toimintojen edellyttämistä keskeisitä palveluntarjoajista ja digitaalisten palvelujen tarjoajista muodostuu 1) energia-alasta, 2) liikenteestä, 3) pankkialasta 4) finanssimarkkinoiden infrastruktuurista, 5) terveydenhuoltoalasta, 6) juomaveden toimittamisesta ja jakelusta sekä 6) digitaalisesta infrastruktuurista (verkossa toimivat markkinapaikat, hakukoneet ja pilvipalvelut). (Eurooppa-neuvosto, 2016)

Yhdysvalloissa kriittiseen infrastruktuuriin sisällytetään kuusitoista sektoria seuraavasti: 1) Kemikaalit, 2) Kauppa, 3) Tietoliikenne, 4) Kriittinen valmistus, 5) Puolustusteollisuus, 6) Padot, 7) Hätäpalvelut, 8) Energia, 9) Rahoituspalvelut, 10) Ruokahuolto / maatalous, 11) Valtion laitokset, 12) Kansanterveys, 13) Tietotekniikka (IT), 14) Ydinvoima, 15) Kuljetukset ja 16) Vesi / jätevedet. (Weed, 2019, 3,4)

Taulukossa 4 on yhteenveto edellä mainituista kriittisen infrastruktuurin määriteistä.

TAULUKKO 4 Kriittisen infrastruktuurin määritteitä.

| **Huoltovarmuus** | **NIS-direktiivi** | **Yhdysvallat** |
|---|---|---|
| Energia | Energia | Kemikaalit |
| Tieto- ja viestintäjärjestelmät | Liikenne | Kauppa |
| Finanssaalan palvelut | Pankkiala | Tietoliikenne |
| Liikenne ja logistiikka | Finanssimarkkinoiden infrastruktuuri | Kriittinen valmistus |
| Vesihuolto | Terveydenhuolto | Puolustusteollisuus |
| Infrastruktuurin rakentaminen ja kunnossapito | Juomavesi/jakelu | Padot |
| Jätehuolto erityistilanteissa | Digitaalinen infrastruktuuri | Hätäpalvelut |
| | | Energia |
| | | Rahoituspalvelut |
| | | Ruokahuolto/maatalous |
| | | Valtion laitokset |
| | | Kansanterveys |
| | | Tietotekniikka |
| | | Ydinvoima |
| | | Kuljetukset |
| | | Vesi/jätevedet |

Yhteiskunnan turvallisuusstrategia, päätös maan huoltovarmuudesta ja Euroopan unionin verkko- ja tietoturvadirektiivi määrittävät väitöstutkimuksen kohteena olevaa kriittistä infrastruktuuria.

Kriittisillä infrastruktuurin osilla on yksi yhteinen omaisuus; ne ovat kaikki kompleksisia järjestelmäosia, jolloin koko kriittinen infrastruktuuri on vuorovaikutteisten kompleksisten osien kokonaisuus, joissa muutokset tapahtuvat usein oppimisprosessien seurauksena. Osat muodostavat kompleksisen mukautuvan

järjestelmäkokonaisuuden (Complex Adaptive systems, CASs). Tästä näkökulmasta katsottuna on merkittävää mallintaa ja analysoida jokainen infrastruktuurin osa osana monimutkaista verkkoa, joka muodostaa yleisen infrastruktuurin. Siihen liittyvät hierarkiset elementit voidaan määritellä seuraavasti: järjestelmän pienin toiminnallinen osa on komponentti, yksikkö on toiminnallisten osien kokoelma, alajärjestelmä on yksikköjoukko, järjestelmä on alajärjestelmien ryhmittely, infrastruktuuri on kokoelma samankaltaisia järjestelmiä ja yleinen infrastruktuuri on toisiinsa kytkettyjen infrastruktuurien verkosto. (Rinaldi, ym., 2001, 13)

Kansallista kriittistä infrastruktuuria voidaan pitää siis useista eri järjestelmistä koostuvana kompleksisena kokonaisuutena. Myös siihen kuuluvat organisaatiot pitävät sisällään kompleksisia järjestelmiä. Näin ollen on edeltä käsin nähtävissä, että vastausten hakeminen tutkimuskysymyksiin johtaa tarkastelun kohteena olevien organisaatioiden kybertoimintojen seikkaperäisen selvittämisen lisäksi niissä esiintyvän monimutkaisuuden ja kompleksisuuden huomioimiseen.

## 3.5 Kriittinen infrastruktuuri ja kyberturvallisuus

Käsitys kriittisen infrastruktuurin rakenteesta on johtamassa systeemiajattelun hyödyntämiseen kohteen tarkastelussa. Kyseessä on kompleksinen järjestelmistä koostuva järjestelmä - System-of-Systems (SOS). Kriittiseen infrastruktuuriin kohdistuu kyberhyökkäyksiä, joihin reagointi perustuu viime kädessä yhteiskunnan kyvykkyyteen mukautua kompleksisuuteen ja sen aiheuttamaan epävarmuuteen. Keskeistä on ymmärtää kriittiseen infrastruktuuriin liittyvää tekniikkaa, riskejä sekä toimijoita ja tästä toimintaympäristöstä muodostuvaa ja yhä kasvavaa kyberturvallisuustarvetta. (Weed, 2019, 3)

Kriittisen infrastruktuurin kyberturvallisuuden suojausohjelmissa ollaan keskittymässä organisaatioiden resilienssin rakentamiseen. Se on organisaation kokonaisvaltaisen lähestymistapa kyberturvallisuuden toimenpiteisiin liiketoiminnan jatkuvuuden hallitsemiseksi. Organisaation resilienssin rakentaminen on varautumista sopeutumaan, selviytymään ja mahdollisesti myös menestymään sen kyberturvallisuutta uhkaavissa kriiseissä. (Australian Covernment, 2009, 20)

Yhteiskunnan turvallisuusstrategiassa (YTS) varautuminen määritellään toiminnaksi, jolla ”varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa”. (Turvallisuuskomitea, 2017)

Kriittisen infrastruktuuri koostuu useista järjestelmistä ja ne muodostavat teknillisesti monimutkaisen ja kompleksisen kokonaisuuden. Organisaatioiden toimintaprosessien jatkuvuuden hallintaan liittyvät käsitteet resilienssi ja varautuminen.

### 3.5.1 Varautuminen ja toiminnan jatkuvuuden hallinta

Organisaatioiden kybertoimintaympäristön huomioiminen ja siitä aiheutuvien uhkien ja häiriötilanteiden ennakointi edellyttävät varautumistoimenpiteitä teknillisten suojautumisratkaisujen ja riskitarkastelujen lisäksi. Tässä ajatuksessa on lähtökohtana se, että varautuminen kattaa myös kaikki ennalta tuntemattomat häiriötilannemahdollisuudet. Varautumalla niihin ja huolehtimalla ennakoidusti toimenpiteistä, jolla organisaation toimintaprosessien jatkuvuutta voidaan hallita kaikissa tilanteissa, vahvistetaan organisaation resilienssiä. Varautuminen tarkoittaa siten toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen poikkeustilanteissa. Varautumisprosessi sitoo yhteen toiminnan häiriötilanteita ennakoivan suunnittelun ja toiminnan. Valmiussuunnittelun, etukäteisvalmistelun, koulutuksen ja harjoitustoiminnan avulla voidaan kehittää organisaation prosessien toiminnan jatkuvuuden hallintaa. Yhteiskunnan turvallisuusstrategiassa todetaan, että julkisen hallinnon varautumisvelvollisuuden ohella tarvitaan laajasti koko yhteiskunnan toimijoiden omatoimista varautumista osana yhteiskunnan kriisinkestävyyttä. (Turvallisuuskomitea, 2017, 9)

Varautumisprosessin keskiössä on organisaation toimintaprosessien jatkuvuuden hallinta. Toimintoina varautumisprosessiin liittyvät seuraavat kokonaisuudet: koulutus ja harjoittelu, testaus, kriisijohtaminen, viestintä, itse jatkuvuudenhallinta, resurssien käyttö ja toipuminen sekä häiriötilanteiden analysoinnit ja niistä saatavat opit. Yhteiskunnan turvallisuusstrategiassa jatkuvuuden hallinta on määritetty seuraavasti: (Turvallisuuskomitea, 2017, 94)

> ”Huoltovarmuutta parantava organisaation prosessi, jolla tunnistetaan toiminnan uhat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa vakavien häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle. Jatkuvuudenhallinta on organisaation ylimmän johdon hyväksymää strategista ja operatiivista toimintaa, jolla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla. Jatkuvuudenhallinnan painopiste on normaaliolojen häiriöissä, mutta prosessiin voi sisältyä myös poikkeusoloihin varautumista. Jatkuvuudenhallinta on yleensä omaehtoista toimintaa, mutta joillakin aloilla organisaatiot ovat myös lailla velvoitettuja varmistamaan toimintansa jatkuvuuden eri olosuhteissa. Jatkuvuudenhallinnan käsite on peräisin elinkeinoelämästä, mutta se on yleistymässä myös muiden organisaatioiden toiminnassa.”

### 3.5.2 Kriittisen infrastruktuurin resilienssi

#### 3.5.2.1 Resilienssi käsitteenä

Resilienssistä on tullut nopeasti kansainvälisen turvallisuuskeskustelun muotikäsite. Tapio Juntunen on käsitellyt resilienssiä artikkelissaan ”Kohti varautumisen ja selviytymisen kulttuuria? Kriittisiä näkökulmia resilienssiin” (2014). Artikkelin mukaan useiden valtioiden ja organisaatioiden turvallisuusstrategisessa ajattelussa resilienssi ilmentää uutta hallintamentaliteettia, jossa turvallisuus kytketään varautumiseen, ennustamattomien riskien kohtaamiseen sekä epävar-

muuden kanssa elämiseen. Resilienssin määritelmät ja käsitteen merkitys vaihtelevat käyttöyhteydestä ja toimintakulttuurista riippuen. Artikkelissa todetaan kuitenkin, että ”käsitettä käytetään teknisenä ja heuristisesti arvokkaana apuvälineenä sektorikohtaisesti määriteltävissä turvallisuusratkaisuissa, esimerkiksi kriittisen infrastruktuurin sieto- ja palautumiskykyä tai turvallisuusjohdon kriisiherkkyyttä arvioitaessa”. Käsitteen käyttö turvallisuusstrategioiden yhteydessä kuvaa myös viimeisten vuosien aikana tapahtunutta entistä syvällisempää turvallisuusajattelun muutosta, jossa yhteiskunnan kokonaisturvallisuuden strategisen tason perusteita on uudelleen määritelty. Artikkelin mukaan Suomen turvallisuuspoliittisessa keskustelussa resilienssi on tuore ja toistaiseksi varsin ”sektorikohtaisesti ja teknisesti sovellettu käsite”. Nykyään käsite on yhdistetty muun muassa kyberturvallisuuden tavoitteiksi. (Juntunen, 2014, 4)

Juntunen toteaa, että ”resilienssi voidaan teoreettisena käsitteenä paikantaa kahteen varsin erilaiseen tieteelliseen traditioon: psykologiaan ja ekologiseen systeemiajatteluun. Psykologiassa resilienssiä liittyy yksilön trauma- ja kriisinsietokykyyn sekä traumoista selviytymiseen vaikuttavia tekijöitä arviointiin. Ekologisessa systeemiajattelussa resilienssi viittaa puolestaan ekosysteemien epälineaariseen palautumis- ja mukautumisdynamiikkaan”. Resilienssiin yhdistetäänkin usein joustavuuden, ketteryyden ja kimmoisuuden kaltaisia ominaisuuksia. Juntusen mukaan yhteiskunnan turvallisuusajatteluun ”resilienssin käsite on kuitenkin kulkenut poliittisen ekologian ja kompleksisuusajattelun kautta”. Näin ollen käsite on muokkautunut yksilötasolta, psyykkisen ja sosiaalisen hyvinvoinnin alueelta, yhteisöjen ja niiden materiaalisten systeemien fyysisten resurssien turvaamiseen. Käsitteen ekologiaan palautuva alkuperä mahdollistaa resilienssin varaan rakentuvan turvallisuuskäsityksen tutkimisen tieteen filosofisista lähtökodista käsin. (Juntunen, 2014, 6)

Resilienssikäsitteeseen liittyy toimijan muodostama tietoinen ja proaktiivinen kyky sopeutua häiriötilanteisiin, toimia niissä joustavasti sekä lopulta toipua ja kehittyä niiden jälkeen. Reaktiivisen toiminnan sijaan se on toimijan yleisempää ominaisuutta ja kyvykkyyttä. Näin ollen resilienssin voidaan erottaa riskien- ja jatkuvuudenhallinnasta, joissa uhkiin katsotaan voitavan varautua. Suomen huoltovarmuuspolitiikkaan liittyy toimintojen resilienssin edistäminen. Se näkyy esimerkiksi julkisen ja yksityisen sektorin yhteistyön kasvamisena sekä alueellisen ja paikallisen varautumisen edistämisenä . (Juntunen, 2014, 25)

#### 3.5.2.2 Kansallinen huoltovarmuus ja resilienssi

Suomen turvallisuus, hyvinvointi ja huoltovarmuus ovat aiempaa riippuvaisempia yhteiskunnan keskeisten, useasti rajat ylittävien ja kansallisen toimivallan ulottumattomissa olevien toimintojen jatkuvuudesta. Huoltovarmuusajattelussa onkin alettu painottamaan organisaatioiden toimintaprosessien jatkuvuuden varmistamista ja kriittisen infrastruktuurin turvaamista jo normaalioloissa. Tämän lisäksi huoltovarmuusajattelussa korostuu kansainvälinen ulottuvuus. Toimintaympäristöön liitettynä kansalliseen huoltovarmuusmäärittelyyn voidaan katsoa kuuluvan seuraavia toimintoja: ”materiaalinen varautuminen, kriittisen

infrastruktuurin suojelu, viestintä- ja tietoverkkojärjestelmien ja -palveluiden turvaaminen, logististen järjestelmien ylläpito, vesi- ja ruokahuolto, kriittisten lääkkeiden ja terveydenhuollon palveluiden saatavuuden turvaaminen sekä sotilaallisen huoltovarmuus". Näiden elintärkeiden toimintojen globalisoituminen on siis tarkoittanut yhä kasvavaa kansainvälistymistä ja verkottumista. Tällöin huoltovarmuuden uutena ulottuvuutena on tarve ymmärtää siihen liittyviä ylikansallisia riippuvuuksia sekä kehittää tähän tietoisuuteen pohjautuvia varautumisratkaisuja mahdollisten häiriötilanteiden varalle. Raportissa "Huoltovarmuus muutoksessa" (2016) todetaan, että "globaalissa toimintaympäristössä yhteiskunnan kriittisten toimintojen voi nähdä yhä useammin olevan ensisijaisia kohteita ulkoisen toimijan harjoittamalle poliittiselle, taloudelliselle ja/ tai sotilaalliselle painostukselle". Kehityksen seurauksena painottuvat erityisesti viranomaisten riittävä tilannetietoisuus sekä varautumisen kansainvälinen yhteistyö. Raportissa mainitaan yhteiskunnan elintärkeiden toimintojen kriisinkestävyyden (resilience) korreloivan entistä enemmän yhteiskunnan yleisen puolustuksellisen pelotteen (deterrence) kanssa ja siitä todetaan seuraavasti: (Aaltola, ym., 2016, 47, 104)

> "Mitä toimivampia prosessit ja infrastruktuurit ovat, sitä suuremmalla todennäköisyydellä yhteiskunta välttää painostustoimet."

Raporin mukaan tämä turvallisuusajattelun laventuminen tarkoittaa entistä suuremman painoarvon asettamista yhteiskunnan elintärkeiden toimintojen turvaamiseen, kokonaisturvallisuusmallin kehittämiseen ja yhteiskunnan yleiseen kriisinkestävyyteen. Näiden toimintojen materiaalisten ja prosessuaalisten edellytysten takaamisessa on jatkossa oltava entistä suurempi painoarvo. Yhteiskunnan kriittisten toimintojen kansainvälistyminen merkitsee siis myös siitä saatavien etujen lisäksi keskinäisriippuvuuksien tuomia uhkia. Yksi kiinnostava vastaus edellä mainittu asetelmaan on resilienssiajattelun hyödyntäminen kansallisessa turvallisuustoiminnassa yleensä ja yhteiskunnan huoltovarmuuden turvaamisessa. (Aaltola, ym., 2016, 47, 104)

Resilienssi-termin käyttö turvallisuusdiskurssissa ei kuitenkaan ole aivan ongelmatonta. Ensinnäkin se voi johtaa painopisteen siirtymiseen riskienhallinnasta ja turvallisuuden tuottamisesta kohti reaktiivista toimintaa, jossa painottuvat häiriöistä selviytymiseen ja toipumiseen liittyvät toimenpiteet. Äärimmillään tämä voisi tarkoittaa sitä, että turvallisuusviranomaiset pyrkisivät keskittämään huomiota yhä enemmän kattavasta uhkiin painottuvasta ennalta ehkäisystä varmistamaan ainoastaan häiriötilanteissa toimisen. Toiseksi resilienssiajattelu voi johtaa turvallisuuden tuottamisen vastuun siirtymiseen yhteiskunnalta kohti yksilöitä tai yhteisöjä. Silloin näiden tahojen kyvykkyys toimia häiriötilanteissa olisi uuden turvallisuusajattelun ytimessä. Raportissa "Huoltovarmuus muutoksessa" todetaankin, että "resilienssi-käsitteen vastuullinen käyttö turvallisuusdiskurssissa näyttäisi siis edellyttävän riittävää ja ymmärrettävää määrittelyä sille, mitä käsitteellä tavoitellaan, kenelle ja kenen toimista". Nykyistä laajempi asiantuntijoiden ja tutkijoiden osallistuminen käsitteen avaamiseen ja selkeyttämiseen sekä yhteisen käsityksen muodostamiseen edesauttaisi käsitteen soveltuvuutta eri

konteksteihin. Siihen tulisi liittää myös julkista keskustelua siitä, minkälainen ”turvallisuus” ja ”turvallisuuden tuottaminen” on hyväksyttävää kriisinkestävässä yhteiskunnassa. Eräs mahdollinen pohja keskustelulle voisi olla Huoltovarmuuskeskuksen (HVK) epävirallinen resilienssin määritelmä: ”tietoinen ja ennakoiva kyky sopeutua ja toimia joustavasti häiriötilanteissa sekä toipua ja kehittyä niiden jälkeen”. (Aaltola, ym., 2016, 79-81)

Kuten edellä on todettu globalisaatio pitää sisällään epävarmuuden, joka muodostuu verkottuneen maailman kansainvälisistä uhkista. Epävarmuuden käsite viittaa siihen, että uhkia on yhä vaikeampi tunnistaa ja, että niiden luonne on ennakoimattomuus. Kaikkiin kuviteltavissa oleviin uhkiin ei ole siten mahdollista valmistautua tehokkaasti ja kustannustehokkaasti. Tämä puolestaan on luonut suotuisat olosuhteet resilienssiin perustuvalle lähestymiselle kansallisen turvallisuuden edistämiselle erityisesti kriittisen infrastruktuurin suojaamisessa. Resilienssi-käsitteelle on tässä yhteydessä ominaista kyky kestää äkillisiä iskuja ja toipua (tai 'palautua takaisin') niistä. (Fjäder, 2014, 114-115)

Systeemiajattelussa sen eri osien sisäkkäisyyden takia kokonaisen ekosysteemin resilienssin katsotaan rakentuvan osien ketteryyden ja mukautumiskyvyn varaan tavoitteena esimerkiksi koko ekosysteemien hallinta. Käytännössä resilienssin ekologiasta juontuva merkitys yhdistetään turvallisuusajattelussa ennakoimattomuuteen. Esimerkiksi kriittisen infrastruktuurin sisältämien eri järjestelmien keskinäisten vaikutusten takia sekä toiminnan epälineaarisesta muutosdynamiikasta seuraa vaikeuksia ennakoida kaikkia mahdollisia uhkatilanteita. Kyberturvallisuuden kansallisissa järjestelyissä noudatetaan julkisen ja yksityisen sektorin toimijoiden välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön. Kyky reagoida toimintaympäristön nopeisiin muutoksiin edellyttää näiltä toimijoilta resilienssi-käsitteeseen liittyvää strategisen ketteryyden periaatteiden ymmärtämistä ja toimenpiteiden noudattamista toimien kehittämisessä ja johtamisessa. (Juntunen, 2014, 7)

Kyberturvallisuus ja siihen liittyvä resilienssi on keskeinen tekijä yhteiskunnan elintärkeiden toimintojen jatkuvuuden sekä erityisesti sen kriittisen infrastruktuurin toimivuuden varmistamisessa. Kyberhuoltovarmuuden turvaamisen toimintalogiikka poikkeaa perinteisestä huoltovarmuuden turvaamisesta. Kybertoimintaympäristössä korostuvat erityisesti prosessi- ja palveluhuoltovarmuus ja siten toimintaympäristö poikkeaa perinteisestä materiaalisesta huoltovarmuudesta. Kyberturvallisuudesta puhuttaessa on syytä muistaa, ettei se tiivisty pelkkään tekniikkaan tai teknologisiin ratkaisuihin. Laajemmin ajateltuna kybertoimintaympäristössä tehdään arkipäivälle olennaisia käytännön asioita. Siinä useat kansalliset kriittiset prosessit ovat integroituneet erilaisiin ylikansallisiin toimintaprosesseihin. Tyypillisinä käytännön esimerkkeinä toiminnasta ovat ulkomailla sijaitsevat palvelimet, pilvipalvelut ja finanssialan varmennusketjut. Toimintaverkoston huoltovarmuutta on mahdotonta ylläpitää tai hallita kansallisin toimin. Toiminta edellyttää rajat ylittävää verkostokyvykkyyttä ja kansainvälistä yhteistyötä. Kyberturvallisuuden varmistamista ja kyberhuoltovarmuuden turvaamista haastavat lisäksi toimintaympäristön hajanaisuus, muutosten nopeus ja vaikeasti ennustettava kehitys. (Aaltola, ym., 2016, 123-125)

## 3.6 Kyberturvallisuus tutkimuskohteena

### 3.6.1 Kyberturvallisuuden tutkimuksen tila

Kansallisessa keskustelussa termi ”kyberturvallisuus” on 2010-luvulla tullut aiemmin käytetyn termin ”tietoturvallisuus” rinnalle. Määritelmällisesti termit tarkoittavat hieman eri asioita, mutta liittyvät oleellisesti kyberturvallisuuden tutkimukseen. Kyberturvallisuus voidaan pitää tietoturvallisuutta laajempana käsitteenä. Se kattaa tietojen ja niitä käsittelevien laitteiden lisäksi myös niiden käyttäjät, ja niihin luottavat ihmiset aina yhteiskunnan kokonaisetuun ja kriittiseen infrastruktuuriin saakka (Von Solms & Van Niekerk, 2013, 101). Kun selvitetään alan tutkimus- ja julkaisutoimintaa ennen kyberturvallisuuskäsitteen käyttöä, niin käsitettä tietoturvallisuus voidaan pitää hakuehtona.

Robert Willison ja Mikko Siponen (2007) ovat selvittäneet alan julkaisu- ja tutkimustoimintaa aikavälillä 1990-2004 artikkelissa ”A Critical assesment if IS Security Research Between 1990-2004”. Tutkimuksessa on käytetty aineistona merkittävimpiä alan tietoturvalehtiä, joista tunnistettiin 1280 tietoturva-artikkelia. Niitä on tutkimuksessa analysoitu tutkimusaiheidensa, teorioiden ja käytettyjen tutkimusmenetelmien perusteella. Tutkimuksessa tuloksien todetaan viittaavat siihen, että tuona aikana suurin osa tutkimuksista oli subjektiivisia ja teoreettisesti kehittymättömiä. Tämän seurauksena artikkelissa esitetään, että jatkossa tarvitaan alalle teoreettisesti perusteltua tutkimusta, joka hyödyntää empiirisiä tutkimusmenetelmiä, mukaan lukien esimerkiksi tapaustutkimukset ja toimintotutkimukset. (Willison & Siponen, 2007)

”Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen” selvityksen mukaan alan tutkimuksen volyymi on kasvanut 1990-luvun puolivälistä lähtien. 1990-luvun lopulla Suomessa julkaistiin keskimäärin muutamia kymmeniä alan tieteellisiä julkaisuja vuosittain. 2010-luvulla on julkaistu keskimäärin noin 120-130 julkaisua vuosittain. (Pelkonen, ym., 2016, 15)

Kyberturvallisuustutkimuksen osalta raportti ”Kyberalan tutkimus ja koulutus Suomessa 2019” kuvaa alan tutkimustarpeita yleisellä tasolla korkeakoulujen näkökulmasta. Raportissa todetaan, että kyberturvallisuuden tutkimukselle on keskeistä monitieteellinen lähestymistapa. Raportissa mainitaan matemaattiset mallit kehitettäessä anomalioiden havaitsemista, laskennallisen tieteen menetelmät hyödynnettäessä erilaisten kompleksisten järjestelmien mallinnuksessa ja yhteiskunnan monimutkaisten turvallisuusongelmien ratkaisemisessa. Kognitiotieteellinen lähestymistapa puolestaan mahdollistaa kybermaailman toimintaympäristön tutkimisen ongelmalähtöisesti eri tieteidenvälisten kysymysten ratkaisemiseksi. Tällöin tutkimuksessa voidaan erityisesti keskittyä luotettavan ja validin mallien kehittämiseen ihmisen toiminnalle digitaalisessa toimintaympäristössä. Tietojenkäsittelytiede tieteenalana tutkii tietotekniikkaan ja sen käyttöön liittyviä ongelmia. Kyberturvallisuus on koko tätä tieteenalaa läpileikkaava tekijä, joka pitää sisällään laajaan skaalaan teknologioita ja prosesseja suojattaessa verkkoja, tietokoneita, ohjelmia, dataa ja sovelluksia kyberhyökkäyksiltä ja

niissä vahingoittumisilta. Tutkimus- ja osaamistarpeet liittyvät tällöin tietojärjestelmätieteeseen, informaatioteknologiaan ja tietojenkäsittelytieteeseen. (Lehto & Niemelä, 2019, 15, 16)

Edellä on todettu, että kyberturvallisuuden tutkimusalue on nykyään tutkimusalana hyvin laaja. Asiaa on selvitetty myös tutkimuksessa ”Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen”. Selvityksen raprotissa tilanteesta todetaan seuraavaa: (Pelkonen, ym., 2016)

> ”Tutkimus osoittaa, edellytykset kyberturvallisuusosaamisen ja -alan kehittämiselle ovat Suomessa hyvät. Suomessa on korkeatasoista kyberturvallisuuteen liittyvää tutkimus-, kehitys- ja innovaatiotoimintaa ja -osaamista. Vahvuuksia on sekä yrityskentällä että korkeakouluissa ja tutkimuslaitoksissa. Alan osaamispohja on kuitenkin varsin kapea ja kärkiosaaminen keskittyy varsin harvoille toimijoille. Osaaminen myös hajaantuu laajaan joukkoon organisaatioita ja toimijoiden välinen yhteistyö on vasta kehittymässä. Selkeitä osaamisen kapeikkoja ja puutteita on muutamalla osaamisalueella. Viime vuosina alan kansainvälinen kilpailu on myös kiristynyt ja Suomessa tarvitaan määrätietoisia toimenpiteitä kyberturvallisuusosaamisen edelleen kehittämiseksi.”

Raprotissa todetaan myös, että kyberturvallisuustutkimus osa Suomen tutkimuskentässä käynnissä olevaa laajempaa muutosta, jossa Suomen tiede on monimuotoistunut. Perinteisten tutkimusalojen oheen on kehittymässä uusi kansainvälisesti merkittävä tutkimusalue informaatioteknologian ja yhteiskunta- ja kauppatieteiden tutkimuksista, jossa kyberturvallisuuden tutkimuksella on osansa. Nykyisen tilannekuvan mukaan kyberturvallisuuteen liittyvä tutkimus on Suomessa teknologisesti orientoitunutta ja tekniikkaan painottunutta. Alan tutkijoista kaksi kolmasosaan on ICT-alan tutkijoita. Muista tutkimusaloista on edustettuina tutkijoita muun muassa matematiikan tutkimuksesta, politiikan tutkimuksesta, sotatieteistä ja kognitiotieteistä. Alan julkaisutoiminnassa näkyy teknologinen suuntautuminen ICT-alueelle, kytkeytyen pääosin tietojärjestelmiin, ohjelmistoihin ja tietoverkkoihin. Kyberturvallisuuden kansallisen tutkimuksen kasvun voidaan katsoa alkaneen noin kaksikymmentä vuotta sitten. Tutkimuksessa on ollut myös supistumisen ajanjakso, mutta vuodesta 2013 lukien kasvu on ollut jatkuvaa. Kyberturvallisuusalan tutkimuskenttä on Suomessa edelleen pienehkö ja hajanainen ja Suomen tieteen kentässä volyymiltään varsin marginaalinen. Suppeasta tutkimusalueesta riippumatta alan tutkimus on korkeatasoista, jossa on kapeita kärkiosaamisalueita. Tällaisia ovat esimerkiksi kryptologia, haavoittuvuustutkimus, tietoturvan hallinta ja mobiililaitteiden tietoturva. Näin ollen alaa leimaa kuva, jossa kyberturvallisuus mielletään ensisijaisesti ja lähes pelkästään teknologiseksi erityisosaamiseksi. (Pelkonen, ym., 2016, 16-19)

### 3.6.2 Kriittisen infrastruktuurin tutkimuksia

Kriittinen infrastruktuuriin liittyvät käsitteet, joita kutsutaan kriittisen infrastruktuurin suojaamiseksi (Critical Infrastructure Protection, CIP) sekä kriittisen tietoteknisen infrastruktuurin suojaamiseksi (Critical Information Infrastructure Protection, CIIP). Kriittinen infrastruktuuri voidaan jakaa fyysiseen ja digitaaliseen osaan. Kyberfyysisillä järjestelmillä voidaan vaikuttaa digitaalisen osan

kautta fyysiseen osaan. Toisin sanoen digitaalisen osan sisältämillä ohjelmistoilla voidaan ohjata fyysisen osan toimintoja kokonaisuuteen liittyvien käyttäjien toimesta. Näin ollen kyberturvallisuuden käsitteen näkökulmasta tutkimuskokonaisuus voidaan liittää kriittisen infrastruktuurin suojaamiseen. Kriittisen infrastruktuurin organisaatioon kohdistuvat kyberturvallisuuden kehittämistoimenpiteet ovat siten osa sen suojaamista. Tutkimus pitää sisällään myös tietoteknisen osuuden.

Viimeisten noin kahdenkymmenen viimevuoden aikana ihmisten ja ICT-teknologian väliset keskinäisvaikutukset ovat muodostaneet Internetin välityksellä ihmisistä, paikoista ja asioista yhtenäisen kompleksisen systeemin. Tämä moderni systeemi liityntöineen merkitsee riskien lisääntymistä kansallisessa kriittisessä infrastruktuurissa, sen keskeisissä resursseissa ja järjestelmissä. Kompleksisuus lisää myös riskejä häiriötilanteiden laajenemisesta kriittisen infrastruktuurin sisällä. (Lewis, 2015)

Kriittisen infrastruktuurin suojaus (Critical Infrastructure Protection, CIP) on käsite, joka liittyy valmiuteen ja reagointiin vakaviin häiriötapahtumiin jonkin alueen tai maan kriittinen infrastruktuurin osalta. Yhdysvalloissa asia nousi esille 1990-luvun puolivälissä. Vuosikymmenen lopulla asiassa laadittiin ensimmäiset normit, kun presidentin antamalla direktiivillä (PDD-63/1998) perustettiin kansallinen ohjelma kriittisen infrastruktuurin suojaamiseksi. Vuonna 1999 perustettiin kansallinen neuvosto julkisen ja yksityisen sektorin yhteistyöhön (National Infrastructure Assurance Council, NIAC). Vuonna 2013 infrastruktuurin resilienssin vahvistamiseksi julkaistiin presidentin Executive Order 13636 (EO), ”Kriittisen infrastruktuurin kyberturvallisuuden parantaminen”. Vuonna 2014 julkaistiin ensimmäinen versio NIST-standardista ”Framework for Improving Critical Infrastructure Cybersecurity”. (Lewis, 2015)

Vastaavassa eurooppalaisessa kriittisen infrastruktuurin suojaamisohjelmassa (European Programme for Critical Infrastructure Protection, EPCIP) vuodelta 2006 viitataan erityisohjelmiin, jotka on luotu Euroopan komission tiedonannon ”Elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta”, EU KOM (2006) 786, seurauksena. Siinä näkökulmana on kriittisen infrastruktuurin suojelu terrorismilta. Jäsenvaltiot ovat velvollisia hyväksymään vuoden 2006 tiedonannon toimenpiteet kansalliseen säännöstöönsä. Kansallisten elintärkeiden infrastruktuurien tunnistaminen ja nimeäminen tapahtuu jäsenvaltiossa ennalta määriteltyjen kansallisten perusteiden mukaisesti. Tiedonannon mukaan jäsenvaltion tulee ottaen huomioon vähintään laadulliset ja määrälliset tiedot tietyn tärkeän infrastruktuurin häiriintymisen tai tuhoutumisen seurannaisvaikutuksia arvioitaessa. Tiedonannon soveltamisalaa käsiteltäessä tulisi infrastruktuurin vahingoittumisen tai tuhoutumisen laajuutta käsitellä määrittelemällä maantieteellinen alue, johon infrastruktuurin menetyksen seuraukset vaikuttaisivat. Tietyn infrastruktuurin vahingoittumisen tai tuhoutumisen aiheuttamien seurausten vakavuutta olisi arvioitava vaikutuksena väestöön, talouteen, ympäristöön sekä huomioimalla poliittiset, psykologiset ja kansanterveydelliset vaikutukset. (Euroopan yhteisöjen komissio, 2006)

Kriittisen infrastruktuurin kyberturvallisuudesta on kirjoitettu tieteellisiä artikkeleja kohtuullisen vähän, vaikka siihen, ja yleensä laajasti koko kybertoimintaympäristöön, kohdistuvia riskejä on alettu pitämään merkittävimpinä yhteiskunnan palvelujen toiminnan luotettavuutta koettelevina tekijöinä. Ne ovat toteutumisen todennäköisyyden ja vaikuttavuuden perustella maailman laajuisesti arvioituina kymmenen merkittävimmän riskin joukossa (World Economic Forum, 2019, 8).

Eräs huomiota herättävin viimeaikaisista kriittisen infrastruktuurin organisaatioiden kohdistuva kyberuhkista on ollut Stuxnet-haittaohjelma. Se on teollisuusautomaatiojärjestelmien SCADA valvonta- ja tiedonhankintajärjestelmään ( Supervisory Control and Data Acquisition, SCADA) liittyvä ja sen toimintaan vaikuttava haittaohjelma, jonka paljastuminen vuonna 2010 ja tuleminen laajalti yleiseen tietoisuuteen viimeistään vuonna 2014, merkitsi kriittiseen infrastruktuuriin kohdistuvien kyberhyökkäysten todellisuuden ja vaarallisuuden paljastumista. Stuxnet on esimerkki kehittyneestä kyberhyökkäyksestä, jossa teollisuusautomaatioon lukeutuvat ohjelmoitavat logiikkayksiköt voidaan saada toimimaan virheellisesti (CISA ICS-CERT, 2018).

Vuonna 2015 Ukrainan sähköverkkoon kohdistettu hyökkäys toteutettiin myös teollisuusautomaatiojärjestelmän ohjelmoitaviin logiikkayksiköihin kohdistuneena hyökkäyksenä. Ohittamalla SCADA valvonta- ja tiedonhankintajärjestelmä, hyökkäys poisti käytöstä sähköasemien etäkäytön ja sen jälkeen ne voitiin irrottaa muusta sähköverkosta ja katkaista sähköaseman alueelta sähköt. Pian tämän jälkeen myös muita SCADA-hyökkäyksiä tapahtui ympäri Eurooppaa (Carter, 2017).

Teollisuusautomaation valvonta- ja tiedonhankintajärjestelmään, SCADA:an liittyvistä kyberturvallisuuden haasteista on kirjoitettu tieteellisisiä dokumentteja. Asiaan on alettu kiinnittämään yhä laajemmin huomiota. Tutkimustulokset ovat teknillisestä näkökulmasta kirjoitettuja.

Esimerkiksi IEEE:n (Institute of Electrical and Electronics Engineers, IEEE) asiantuntijat ovat jo vuonna 2010 kiinnittäneet artikkelissa huomiota SCADA-järjestelmän suojaustarpeeseen. Artikkelissa todetaan, että vaatimus täyttää toiminnan turvallisuus- ja laatuvaatimukset on haastava asia verkottuneessa toimintaympäristössä. (Gao, ym., 2010)

Pohjois-Amerikka Electric luotettavuusyhtiö (North American Electric Reliability Corporation, NERC) perusti kyberturvallisuusstandardin, joka edellyttää, että automaatiojärjestelmän ohjelmistot noudattavat kyberturvallisuusmenettelyjä niiden kriittisissä ohjausjärjestelmissä. Artikkelissa on SCADA-järjestelmien kyberturvallisuuden hallintaa ehdotettu kehystä, joka pitää sisällään neljä pääkomponenttia: 1) järjestelmä reaaliaikainen seuranta, 2) toiminnan poikkeamien havaitseminen, 3) poikkeamien vaikutusanalyysi ja 4) poikkeamien lieventämisstrategiat. Tutkimustulokset ovat teknillisesti painottuneita. (Ten, ym., 2010)

SCADA-järjestelmien kyberturvallisuuden merkitystä kansallisen kriittisen infrastruktuurin suojaamisessa kuvastaa Yhdysvaltain liittovaltion julkaisu ”US

Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure" (2019) pyrkimyksistä yhdistää julkinen ja yksityinen sektori toimenpiteitä puolustauduttaessa kyberturvallisuuden uhkilta, jotka kohdistuvat teollisuuden automaatiojärjestelmiin (Industrial Control System, ICS) ja niiden valvonta- ja tiedonhankintajärjestelmiin (SCADA). Julkaisu kuvastaa huolta, joka liittyy ICS- ja SCADA-järjestelmien kyberturvallisuuden merkitykseen osana kriittistä kansallista infrastruktuuria. Julkaisu painottaa poliittisia ja sosiaalisia haasteita paremman kyberturvallisuuden saavuttamiseksi, samoin kuin prosesseja, joiden avulla voidaan toimia yhteisyössä julkisen sektorin ja yksityisen sektorin toimijoiden kesken kyberturvallisuuden edistämiseksi. Mukana on eri osapuolia ja toimialoja, jotka saattavat kohdata teollisuuden automaatiojärjestelmiin (ICS) tai niiden valvonta- ja tiedonhankintajärjestelmiin (SCADA) kohdistettavia kyberhyökkäyksiä. (Weed, 2019)

Kriittisen infrastruktuurin organisaatioihin kohdistuu jatkuvasti edellä mainittujen tapausten lisäksi huomattava määrä muulla tavoin toteutettuja hyökkäyksiä. Hyökkäysten määrä on ollut kasvussa viime vuosina. Teollisuusautomaatiojärjestelmien ja erilaisten älylaittien lisääntynyt käyttö kriittisen infrastruktuurin järjestelmissä on laajentanut hyökkäysmahdollisuuksia tietoverkkorikollisuudelle. IBM.n aluetta käsittelevän raportin mukaan noin seitsemänkymmentä prosenttia alan turvallisuustoimijoista maailmanlaajuisesti pitää uhka-arviota korkeana tai vakavana. Uhkat kohdistuvat organisaatioon sen ulkopuolelta ja sisäpuolelta. (IBM, 2019a).

Vastaavasti IBM:n terveydenhuollon kyberturvallisuutta käsittelevässä raportissa todetaan, että erityisesti terveystiedoista on tullut arvokkaita kohteita tietoverkkorikollisuudelle. Ne sisältävät haavoittuvuuksia, joita rikolliset käyttävät hyväksi. Uhkat kohdistuvat organisaatioon sekä ulkopuolelta että sisäpuolelta. (IBM, 2019b).

Kriittisen infrastruktuuriin ja sen organisaatioiden kyberturvallisuuteen kohdistuvia kansallisia tutkimuksia ovat Cyber Trust-tutkimushanke, KyberTeo ja Huoltovarmuuskeskuksen Kyber2020-hankekokonaisuus.

Cyber Trust –tutkimushankeen (2015-2017) tavoitteena oli kehittämää suomalaista kyberturvallisuusosaamista, alan yhteistyötä myötävaikuttamaa kansainvälisen näkyvyyden luomisessa sekä parantaa tutkimuksen avulla kansallista kyberturvallisuutta ja -luottamusta yhteistyössä tiedeyhteisöjen ja yritysmaailman toimijoiden kanssa (DIMECC, 2017). Yksi tutkimushankeen työpaketeista ole kriittisen infrastruktuurin sietokyvyn ja suojaamisen parantamiseen tähtäävä työpaketti (Critical Infrastructure Resiliency and Protection, CIRP). Jyväskylä yliopiston CIRP-työpaketin yhteydessä syntyneitä hankeraportteja ja julkaisuja on hyödynnetty väitöstyössä taulukoissa 1 ja 2 mainituilta osilta.

KyberTeo-tutkimushanke on kansallinen hankekokonaisuus vuosilta 2014-2016. Hankekokonaisuus on nimeltään "Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen". Se oli jatkoa seuraavalle teollisuuden tietoturvaan kohdistuneelle tutkimusprojektikokonaisuudelle: (Ahonen, 2017)

- TITAN "Tietoturvaa teollisuusautomaatioon", 2009-2010
- TITAN, 2011-2012

- TEO-TT ”Teollisuuden tietoturvan kansallinen kehittäminen teematyöpajoissa”, 2011-2012
- COREQ-VE ”Yhteinen tietoturvavaatimuskanta teollisuudelle”, 2012-2013
- COREQ-ACT ”Tietoturvan aktiiviset teollisuuscaset”, 2014-2016

KyberTeo-projektin pääasiakkaan on ollut Huoltovarmuuskeskus. Muina asiakkaina on ollut kymmenen hankkeeseen osallistunutta teollisuus- ja palveluyritystä kunakin projektivuonna. Projektin lopputuloksista on tiivistelmässä todettu muun muassa seuraavaa: (Ahonen, 2017)

> ”Kyberturvallisuuden kehittäminen edellyttää lähes aina tietoisuuden perustasoa, jolloin yrityksen päättäjät ja käytännön toimijat ymmärtävät riittävästi kyberuhkien todellisia vaikutuksia ja kohdistumisesta omaan toimintaansa. Vasta tämän jälkeen yritykseen voi syntyä tarvittava vastuiden määrittely ja resursointi mm. tuotantoon soveltuvien kyberturvallisuusuhkien havaitsemiseen, torjuntaan ja ennakkovarautumiseen.”

> ”Teollisuusautomaation kyberturvallisuuden kehittäminen Suomessa vaatii kaikkien toimijoiden osallistamista. Tämä johtuu mm. siitä, että kyberturvallisuuden tason toteuman ratkaisee lopulta ”arvoketjun heikoin toimija” tai ”järjestelmän huomaamaton haavoittuvuus”. Turvallisen toiminnan vastuuta ei voi ulkoistaa, sillä viimekädessä tuotanto vastaa itse kaikkien tarvittavien turvamenettelyjen käyttöönotosta, käytön valvonnasta ja kehittämisestä.”

> ”KYBER-TEO projekteissa vuosina 2014 - 2016 kehitettiin yritysten yhteistyötä ja edellytyksiä parantaa monia erilaisia automaation kyberturvallisuuteen vaikuttavia asioita, erityisesti: Alan edelläkävijäyrityksissä kehitettiin ja testattiin automaation kyberturvallisuuden kehittämisen palveluja, parhaita käytäntöjä ja ratkaisuja. Määriteltiin kyberturvallisuuden työnjako ja tehtävät automaation elinkaaressa. Parannettiin ammattilaisten kyberturvallisuustietoisuutta julkisten tulosten esittelytilaisuuksissa kertomalla uhkista ja seurauksista, sekä varautumiseen kehitetyistä käytännöistä ja koetelluista ratkaisuista. Kehitettiin ja koestettiin automaation kyberturvatestauksen ympäristöjä. Kehitettiin ja koestettiin automaation kyberturvaharjoittelun ympäristöjä. Kehitettiin ja koestettiin automaatioverkkojen kyberturvamonitoroinnin konsepteja ja menetelmiä. Kehitettiin ja pilotoitiin automaation kyberturvallisuuden sähköistä yhteistyöfoorumia.”

Energia-alan kyberturvallisuuden KYBER-ENE-hanke on osa Huoltovarmuuskeskuksen kyberturvallisuuden kehittämiseen tähtäävää Kyber2020-ohjelmaa. Hankkeen raportissa todetaan, että ”kyberturvallisuuden ylläpito ja kehitys on saatava osaksi päivittäistä rutiinityötä”. Rapotin mukaan energia-alan PK-yritysten kyberturvallisuudessa voidaan päästä varsin hyvälle toiminnan tasolle keskittymällä perusasioiden kehittämiseen. Perusosaamisen ja tietoisuuden kehittäminen tukevat myös kehittyneiden kyberhyökkäysten tunnistamista. Mikäli kaikki yrityksen sidosryhmät osaavat omassa työssään toimia tietoturvallisella tavalla ja tunnistavat kyberturvallisuuden merkityksen toiminnassa paranevat oman liiketoiminnan jatkuvuuden edellytykset. Raportissa luetellaan kehityksen vauhdittamiseksi seuraavia toimenpiteitä järjestyksessä: (Huoltovarmuuskeskus, 2019)

> ”1) Johdon tietoisuus kuntoon, 2) nykytilan kartoitus, 3) kehityskohteiden tunnistaminen ja keskustelu, 4) kehitysryhmän perustaminen, 5) vuosisuunnitelma, kehityshankkeiden määrittely, 6) kehittämisen budjetointi, tehtävien ja vastuunjako ja 7) tilannekuvan seuranta johdossa.”

Väitöstyössä useasti referoidut Valtioneuvoston kanslialle tehdyt kaksi tukimusta; ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” (2017) ja ”Kyberturvallisuuden strateginen johtaminen Suomessa” (2018) liittyvät myös kansalliseen tutkimusalueeseen.

### 3.6.3 Muita alan tutkimuksia; tutkimusaukon kuvaaminen

Kansallisessa kyberturvallisuuden tilaa käsittelevässä tutkimuksessa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” todetaan, että ”ala on kehittynyt viime vuosina kyberturvallisuusstrategian strategisten linjausten ja laaditun toimeenpanosuunnitelman perusteella”. Tutkimus painottaa kuitenkin tilannetietoisuuden ja havaintokyvyn parantamista, elintärkeiden toimintojen turvaamisen edistämistä, tutkimuksen ja yleisen tietoisuuden vahvistamista sekä kyberturvallisuuden kehittämistä osana kokonaisturvallisuutta. Toimenpiteillä voidaan vahvistaa kybertuvallisuutta kansallisena kilpailuetuna. (Lehto, ym., 2017, 2)

Hakuyhdistelmällä, kansallinen kriittinen infrastruktuuri ja sen julkisen ja yksityisen sektorin organisaatioiden kyberturvallisuus, on viimeisten viiden vuoden tarkastelujakson aikana käsitelty alan akateemisissa konferensseissa (European Conference on Cyber Warfare and Security ja International Conference on Cyber Warfare and Security) vasta viime aikoina.

George Drivas, Leandros Maglaras, Helge Janicke ja Sotiris Ioannidis ovat laatineet vuoden 2019 konferenssiin ” The 18th European Conference on Cyber Warfare and Security”artikkelin ”Cybersecurity Assessment of the Public Sector in Greece”. Artikkelin mukaan Kreikan kansallinen kyberturvallisuusviranominen (NCSA) on käynnistänyt 2018 auditointityön koko julkiselle sektorille tavoitteena kehittää digitaalisia taitoja ja vahvistaa julkisen ja yksityisen sektorin toimintatapoja hyödyntäen akateemisen yhteisön sekä julkisen ja yksityisen sektorin toimijoiden potentiaalia. Kehittämisessä aiotaan käyttää lähestymistapana PDCA-kehitysmenetelmää ja sidosryhmien tiivistä yhteistyötä kansallisen kriittisen infrastruktuurin turvaamiseksi kybertoimintaympäristössä. Artikkelin mukaan tavoitteen saavuttamiseksi tarkasteluun tarvitaan kokoelma prosesseja, tekniikoita ja ihmisiä. Ensimmäisessä vaiheessa on aloitettu selvitystyö valtionhallinnon kyberturvallisuustilanteesta keskeisistä ICT-infrastruktuureista. Alustavan esiauditoinnin avulla on pyritty arvioimaan organisaatioiden kyberturvallisuuden nykytilaa, toimintapolitiikkoja, kyberturvallisuuden menettelyjä sekä teknillisiä, että käyttäjien toimenpiteitä. Aineiston perusteella on tarkoitus suunnitella kehitystyön seuraavia vaiheita. Artikkelissa todetaan, että NIS-direktiivin mukaisten yhteiskunnan keskeisten palveluiden tarjoajien sekä digitaalisten palvelujen tarjoajien on otettava käyttöön asianmukaiset turvatoimet pyrkiessään saavuttamaan kyberturvallisuuden perustason. Käynnistetyt toimenpiteet ovat

tärkeitä tekijöitä tämän tavoitteen saavuttamisessa. (Drivas, Maglaras, Janicke & Ioannidi, 2019)

Eduardo Izycki ja Rodrigo Colli vuoden 2019 konferenssin ”The 18th European Conference on Cyber Warfare and Security”artikkelissa “Protection of Critical Infrastructure in National Cyber Security” on selvitetty kahdeksankymmenenkuuden maan kansallisten kyberturvallisuusstrategioiden yhtäläisyyksiä kriittisen infrastruktuurin suojaustoimenpiteissä. Kansalliset kyberturvallisuusstrategiat ovat olleet huomion kohteena noin viisitoista vuotta, mutta niitä on laadittu pääsoin vasta viimeisten kymmenen viimevuoden aikana. Tarkastelussa olleista strategioista on laadittu 2010-luvulla yhteensä seitsemänkymmentä seitsemän. Artikkelissa tunnistetut strategioiden yhteiset lähentymistavat liittyvät kriittisen infrastruktuurin määrittelyyn ja niihin luettaviin palveluihin (kts. oheinen Taulukko 5), kansallisen kriittisen infrastruktuurin suojausohjelman olemassaoloon, julkisiin ja yksityisiin sidosryhmiin ja tarpeeseen saada aikaan resilienssiä kriittisen infrastruktuurin järjestelmiin. Päätelmässä tunnistetaan myös tarve kansainväliseen yhteistyöhön kriittisen infrastruktuurien suojaamiseksi. Yhteistyöalueet voisivat löytyä koulutuksesta sekä uhkiin ja kriiseihin liittyvästä tiedonvaihdosta. Päätelmissä mainitaan myös, että keskipitkän aikavälin yhteistyöstä voitaisiin saada aikaan säätelyä kyberaseiden käytön rajoituksista kriittistä infrastruktuuria vastaan. Oheisessa taulukossa on esitetty tutkimuksen kansallisissa strategioissa esille tulleet kriittisen infrastruktuurin palvelut, ja ne huomioivat maat lukumäärinä ilmaistuna. (Izycki & Colli, 2019)

TAULUKKO 5 Kriittisen infrastruktuurin palvelut maiden lukumäärän mukaan

| **Palvelut** | **Maiden lukumäärät** |
|---|---|
| Sähköenergia | 27 |
| Tietoliikenne | 26 |
| Kuljetukset | 25 |
| Rahoitus | 21 |
| Vesi / viemäri | 19 |
| Terveydenhuolto | 19 |
| Tietotekniikka | 10 |
| Hätäpalvelut | 8 |
| Julkiset palvelut | 8 |
| Ruokahuolto | 8 |
| Puolustusvoimat | 7 |
| Jakelu ja logistiikka | 4 |
| Maakaasu ja öljy | 3 |
| Kemianteollisuus / Ydinvoima | 2 |
| Kaupankäynti | 1 |

Pierre Jacobs, Sebastiaan von Solms, Marthie Grobler ja Brett van Niekerk ovat vuoden 2019 konferenssin ”The 18th European Conference on Cyber Warfare

and Security" artikkelissa "Towards a Framework for the Selection and Prioritisation of National Cybersecurity Functions" tarkastelleet kansallisen kyberturvallisuuden kehittämiseen liittyvän toimintamallin tarpeellisuutta. He ovat todenneet, että toimintamalli voisi toimia perustana kehitettäessä kansallisen kyberturvallisuuden mallia hallintotehtävien tunnistamiseksi sekä niiden edellyttämien toimintojen valintaan, priorisointiin ja toteutukseen. Artikkelissa on lueteltu kolmetoista yleistä kansallista kyberturvallisuustoimintoa, joista kansallisvaltiot voivat käyttää tarkoituksenmukaisimmat valitsemalla tärkeimmät toiminnot kansallista toteutusta varten. Toiminnot ovat: (Jacobs, von Solms & Grobler, 2019)

- Sotilaallinen kyberturvallisuus / cyber Warfare
- Tietoverkkorikollisuus / Tutkimukset / Digitaalinen rikostekniikka
- Tutkimus- ja kehitystoiminta, koulutus ja tietoisuus
- Kriittisen tietoinfrastruktuurin suojaus (Critical Information Infrastructure Protection, CIIP)
- Salaus
- E-identiteetti
- Tapahtumien käsittely
- Seuranta ja arviointi
- Sisäinen toimenpiteiden koordinointi
- Ulkoinen sidosryhmien sitoutuminen
- Kansallisen politiikan ja strategian kehittäminen
- Kansallinen strateginen riskien ja uhkien arviointi
- Kansallisten määräysten kehittäminen

Valittujen toimintojen priorisoimiseksi artikkelissa ehdotetaan käytettäväksi kansallista kyberturvallisuusriskien hallintakehystä, joka on artikkelissa muodostettu yhdistämällä standardit ISO/IEC 27005 ja NIST SP 800-39, ja korvaamalla ISO/IEC 27005 -kontekstinmääritysprosessi NIST SP 800- 39 riskienhallintaprosessilla. (Jacobs, von Solms & Grobler, 2019).

Piere Jacobs, SH (Basie) von Solms ja Marthie Grobler ovat konferenssin "International Conference on Business and Cyber Security (ICBCS)" artikkelissaan "Towards a framework for the development of business cybersecurity capabilities" (2016) tarkastelleet organisaatioiden käyttämiä standardeja, menettelyjä ja parhaita käytänteitä suojatessaan ICT-varantojaan ja ylläpitääkseen mainettaan. Artikkelin mukaan suurin osa tutkituista asiakirjoista kuvaa ominaisuuksia, joilla voidaan kehittää liiketoimintaprosesseja kybertoimintaympäristössä. Ne ovat useimmiten kuitenkin toimialakohtaisia ja käsittelevät tyypillisesti teknillisiä, hallinnollisia ja fyysisen valvonnan menettelyjä. Kyvykkyyksillä, jotka muodostuvat ihmisistä, prosesseista ja tekniikasta, voidaan saavuttaa tuloksia tai vaikuttavuutta kyberturvallisuuden toiminta-alueella. Artikkelin perustella edellä mainittuja kyvykkyyksiä sisältävää organisaation kehittämisen kyberturvallisuuskehystä ei ole määritelty ja sille on olemassa tarvetta. Artikkeli pitää sisällään heidän kehittämänsä kehyksen kuvauksen, joka on nimeltään Bu-

siness Cybersecurity Capability Development Frameworki (BCCapDev Framework). Kehysajattelu on kehitetty siten, että se on modulaarinen, uudelleen käytettävä ja riippumaton muutoksista standardeissa, kehyksissä tai parhaita käytäntöjä. Kehys on myös kehitetty riittävän joustavaksi, jotta se olisi toimialaneutraali. Kehys muodostuu kuudesta tasosta, jotka ovat: (Jacobs, von Solms & Grobler, 2016)

- Taso 0, joka pitää sisällään tiedot organisaatiossa tarvittavista normeista ja ohjaavista asiakirjoista, kuten lakiasiat, toimintastrategia ja -politiikka sekä käyttöön hyväksytyt standardit.
- Taso 1, joka pitää sisällään yleisen hallinnon, kuten toiminnan johtamisen sekä suunnittelu- ja toteutusvastuut.
- Taso 2, joka kuvaa kehyksessä organisaation liiketoimintaa ja toimintaprosesseja.
- Taso 3, jossa määritetään toimenpiteet, joita kehitetään. Kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi NIST-standardi ”Framework for Improving Critical Infrastructure Cybersecurity” käyttää tarkoitukseen seuraavia kyberturvallisuusluokkia; identifioi, suojaa, tunnista, vastaa ja palauta.
- Taso 4, joka kuvaa tarvittavat rakenteet toimenpiteiden tukemiseksi. Kyseeseen tulevat toiminnot, kuten Operations Center system (SOC) ja Computer Security Incident Response Team (CSIRT) tai näiden yhdistelmä.
- Taso 5, joka kuvaa organisaation sisäisiä politiikkoja, prosesseja ja teknologiakohtaisia menettelyjä, jotka ohjaavat rakenteen toimintajaksoa.

Artikkelissa ehdotetun kehysajattelun tarkoituksena on antaa organisaatiolle joustavuutta ja ketteryyttä kehittäessä kyberturvallisuuteen liittyviä kyvykkyyksiä nopeasti muuttuvassa toimintaympäristössä. Sen tarkoituksena on myös varmistaa, että kaikki näkökohdat otetaan huomioon mahdollisimman hyvin kyvykkyyksien kehittämisen osalta. (Jacobs, von Solms & Grobler, 2016)

Tutkimusalueen piiriin voidaan lukea myös Jyväskylän yliopiston IT-tiedekunnassa tarkistettu organisaation tietohallinnon johtamiseen liittyvä Jouko Selkälän väitöstyö ”CIO decision making: Issues and a process view” (2016). Se käsittelee tietohallintojohtajan vastuita ja hallintomallia sekä päätöksentekoprosessia. Väitöstyön yhteenvedossa todetaan, että kriittinen kysymys on, kuinka organisaatiossa tietotekniikkaa voidaan käyttää tukemaan liiketoiminnan hyötyjä tai tavoitteita. Yleensä CIO, (Chief Information Officer, CIO) on tästä näkökulmasta tarkasteltuna yksi tärkeimmistä henkilöistä organisaatiossa. CIO ei ole vain vastuussa keskeytymättömästä suorituskyvystä ICT-toimintojen suhteen, vaan vastuut ulottuvat myös yhteydenpitoon sisäisiin ja ulkoisiin sidosryhmiin sekä sidosryhmien välillä. Huolimatta siitä, että väitöstutkimus on lisänneet ymmärrystä CIO: n keskeisistä tehtävistä ja vastuista, tutkimuksessa todetaan, että tutkija ei ole löytänyt aikaisempaa tutkimustietoa, joka olisi käsitellyt CIO: n koko päätöksentekoprosessia. Mikään aiempi tutkimus ei ole jäsentänyt ICT-päätöksentekorakennetta kolmitasolla jaolla: strateginen, taktinen ja operatiivinen.

Tulosta pidetään yllättävänä erityisesti ottaen huomioon CIO: n vastuiden suuren määrän organisaatiossa muun muassa ICT-hallintoon, ICT-arvon luomiseen, päätöksentekoon liittyen. (Selkälä, 2016, 109,115)

Kriittisen infrastruktuurin kyberturvallisuuden tutkimukset tuovat esille kansallisista strategioista johdetut tarpeet saada aikaan resilienssiä kriittisen infrastruktuurin järjestelmiin. Artikkeleissa "Towards a framework for the development of business cybersecurity capabilities" (2016), joka käsittelee organisaatioiden käyttämiä standardeja, menettelyjä ja parhaita käytänteitä suojatessaan ICT-varantojaan ja ylläpitääkseen mainettaan, todetaan, että suurin osa tutkituista asiakirjoista kuvaa ominaisuuksia, joilla voidaan kehittää liiketoimintaprosesseja kybertoimintaympäristössä. Siinä todetaan myös, että ne ovat useimmiten kuitenkin toimialakohtaisia ja käsittelevät tyypillisesti teknillisiä, hallinnollisia ja fyysisen valvonnan menettelyjä. Artikkelin mukaan kyvykkyyksillä, jotka muodostuvat ihmisistä, prosesseista ja tekniikasta, voidaan saavuttaa tuloksia tai vaikuttavuutta kyberturvallisuuden toiminta-alueella. Kyvykkyyksiä sisältävää organisaation kyberturvallisuuskehystä ei ole määritelty ja sille on olemassa tarvetta. Kehysajattelun tarkoituksena on antaa organisaatiolle joustavuutta ja ketteryyttä kehittäessä kyberturvallisuuteen liittyviä kyvykkyyksiä nopeasti muuttuvassa toimintaympäristössä. (Jacobs, von Solms & Grobler, 2016)

Edellä mainittua kuvaa kyberturvallisuuden tutkimusten toimialakohtaisuutta ja painottumisesta tyypillisesti teknillisiin, hallinnollisiin ja fyysisen valvonnan menettelyihin vahvistavat myös Antti Pelkosen (ym., 2016) sekä Robert Willison ja Mikko Siponen (2007) selvitykset kyberturvallisuuden ja tietoturvan tutkimuksista.

Kasallisissa kyberturvallisuuden hankkeiden loppuraporteissa (RR5 ja RR6) korostetaan kybertoimenpiteiden edellyttävän organisaatioilta tietoisuuden hyvää perustasoa, jolloin päättäjät ja muut käytännön toimijat ymmärtävät riittävästi kyberuhkien todellisia vaikutuksia toimintaansa. Kriittisen infrastruktuurin toimijoihin kohdistuvat kyberturvallisuuden häiriötekijät ovat merkittävä osa kybertoimintaympäristön haasteista, niin yhteiskunnan palvelujen, kuin kansalaisten omien tarpeiden osalta. Jatkuvasti tiedotusvälineissä raportoitavat uhkat kertovat myös koko alueen laajuudesta, jossa perinteisellä tietoturvallisuudella on edelleen merkittävä rooli digitaalisten tietojemme saatavuuden, luotettavuuden ja käytettävyyden turvaamisessa. ICT-järjestelmien ja -laitteiden verkottuminen globaaliksi kyberavaruudeksi edellyttää tietoturvaratkaisujen ohella kyberturvallisuuteen systeemitason turvallisuustutkimusta.

Väitöstyö kohdistuu organisaation kyberturvallisuuden johtamiseen ja kehittämiseen toimintaympäristössä, joka pitää sisällään ihmisistä, prosessista ja tekniikoista muodostuvia kokonaisuuksia. Niiden toiminnan jatkuvuuden varmistamiseen liittyvät niin suojaamistarpeiden tunnistaminen kuin riskienhallinta ja uhkiin varautuminen. Organisaation toimintaa kybertoimintaympäristössä on tarkasteltu aiempia tutkimuksia täydentävällä johtamista ja ICT-päätöksentekorakennetta korostavalla kolmitasoisella jaolla: strateginen, operatiivinen ja teknillinen/taktinen. Tuloksena on muun muassa edellä mainittua jakoa orga-

nisaation kyberrakennetta hyväksi käyttävä kyberturvallisuuden systeemikuvaus ja siihen liittyviä kyvykkyyksiä kehittävän turvallisuuskehyksen määrittely arkkitehtuurisena rakenteena, joka pitää sisällään konkreettisia toimenpiteitä. Tutkimustuloksista muodostettuja kehittämisehdotuksia voidaan pitää organisaation geneerisinä toiminnan jatkuvan parantamisen tavoitteina, ja siten ne täydentävät edellä mainittua toimialakohtaisuutta.

## 3.7 Kyberturvallisuuden normeja

> Mitä standardeja, ohjeita ja suosituksia voidaan hyödyntää organisaation kyberturvallisuuden hallinnan kehittämisessä?
>
> RR1. Pöyhönen J. (2018). Standardit, ohjeet ja suositukset osana teollisuusyrityksen kyberturvallisuuden hallintaa. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 55/2018.

### 3.7.1 Standardit ja ohjeet

Standardi on organisaation esittämä määritelmä siitä, miten jokin asia tulisi tehdä. Standardeja, ohjeita ja normeja käyttävät niin eri toimialojen laitevalmistajat ja palveluntarjoajat kuin julkisen sektorin toimijat ja tutkimuslaitokset omista lähtökohdistaan ja globaalissa toimintaympäristössä toimiessaan. Niitä on vuosikymmenien aikana laadittu useisiin eri tarkoituksiin huomattava määrä. Alan merkittävimmät kansainväliset kattojärjestöt ovat yleinen kansainvälinen standardisointiorganisaatio ISO (International Organization for Standardization, ISO), sähkötekniikkaan ja elektroniikkaan erikoistunut IEC (International Electrotechnical Commission, IEC) ja televiestinnän ITU (International Telecommunication Union, ITU). Tietotekniikan alalla ISO ja IEC ovat muodostaneet yhteisen komitean alan standardien kehittämiseksi. Kansalliset standardointijärjestöt saattavat käyttöön kansallisia standardeja ja osallistuvat kansainvälisten standardien laadintaan. Suomen kansallinen toimija on Suomen standardisoimisliitto ry (SFS). Suomessa on hajautettu standardisointijärjestelmä, jossa SFS toimii keskusjärjestönä ja laatii standardit yhdessä toimialayhteisöjensä kanssa.

SFS toteaa standardien tarkoituksesta seuraavaa: (Suomen Standardisoimisliitto SFS ry. Standardi tutuksi.)

> ”Standardisointi on yhteisten toimintatapojen laatimista. Sen tarkoitus on helpottaa viranomaisten, elinkeinoelämän ja kuluttajien elämää. Standardisoinnin ansioista tuotteet, palvelut ja menetelmät sopivat siihen käyttöön ja niihin olosuhteisiin, joihin ne on tarkoitettu. Se varmistaa, että tuotteet ja järjestelmät sopivat toisiinsa ja toimivat yhdessä.”

Usein standardeihin viitataan Euroopan unionin säädöksissä, jotka ovat asetuksia, direktiivejä tai päätöksiä. Asetukset tulevat sellaisenaan voimaan kaikissa EU-maissa, kun direktiivit voidaan puolestaan saattaa voimaan kussakin jäsenmaassa parhaaksi katsomallaan tavalla. Päätökset koskevat niitä organisaatioita

tai jäsenmaita, joille ne on osoitettu. Lisäksi standardit on mainittu myös lukuisissa EU:n asiakirjoissa, kuten esimerkiksi tiedonannoissa ja päätöslauselmissa. Ne eivät ole kuitenkaan juridisesti sitovia asiakirjoja. EU:n uuden lähestymistavan (New Approach) mukaisesti laadittavat direktiivit sisältävät vain tuotteiden olennaisesti terveyttä, turvallisuutta, kuluttajansuojelua ja ympäristöä koskevia vaatimuksia sekä vaatimustenmukaisuuden osoittamisen vaihtoehtoja. Tämän takia tekniset yksityiskohdat eli spesifikaatiot, joita tarvitaan tuotettaessa ja markkinoitaessa direktiivien mukaisia tuotteita, esitetään Euroopassa niin sanotuissa yhdenmukaistetuissa standardeissa yksittäisten standardien sijaan. Ne ovat eurooppalaisia standardeja, jotka on laadittu Euroopan komission toimeksiannosta. Niiden viitetiedot on julkaistu EU:n virallisessa lehdessä. Vanhoissa direktiiveissä ja kansallisissa säädöksissä sen sijaan viitataan edelleen lukuisiin yksittäisiin eurooppalaisiin standardeihin. Viittauksella standardi voidaan tehdä pakolliseksi tai sitä voidaan pitää esimerkkinä säädöksen vaatimukset täyttävästä ratkaisusta. (Suomen Standardisoimisliitto SFS ry. Standardit direktiivit ja ce-merkintä.)

Suomen Standardisoimisliitto toteaa standardien ja direktiivien suhteesta seuraavasti: ”Tekniset spesifikaatiot eivät ole pakollisia, vaan niillä on vapaaehtoisen standardin status. Kansallisten viranomaisten on kuitenkin tunnustettava, että tuotteet, jotka on valmistettu yhdenmukaistettujen standardien mukaisesti, täyttävät direktiiveissä olevat turvallisuusvaatimukset”. Tällaiset tuotteet saavat siten liikkua yli kansallisten rajojen. Myös kansallisissa säädöksissä voidaan viitata standardeihin. Tuotteet, joita uuden lähestymistavan direktiivit koskevat, varustetaan CE-merkinnällä. CE-merkintä on käytössä sähkölaitteissa ja muissa koneissa, lääkinnällisissä laitteissa, leluissa, painelaitteissa, henkilönsuojaimissa sekä radio- ja telepäätelaitteissa. (Suomen Standardisoimisliitto SFS ry. Standardit direktiivit ja ce-merkintä.)

Yhdysvalloissa National Institute of Standards and Technology (NIST) on kasallinen Yhdysvaltojen kauppaministeriön virasto, jonka tehtävänä on edistää innovaatioita ja teollisuuden kilpailukykyä. NIST:n standardit ja erilaiset ohjeet ja suositukset ovat usein maksuttomia. NIST: n toimintaan liittyy yhteisten toimintatapojen laatiminen organisaatioiden käyttöön. Ne kattavat laajan kirjon kyberturvallisuuden alalle soveltuvia ohjeita. (National Institute of Standards and Technology)

Liitteessä 2 on kuvattu tiivistetysti väitöstyön alueeseen lukeutuvia ja sen yhteydessä sovellettuja standardeja.

### 3.7.2 EU:n verkko- ja tietoturvadirektiivi, NIS-direktiivi

Euroopan neuvosto hyväksyi 17. toukokuuta 2016 virallisesti uudet säännöt verkko- ja tietojärjestelmien turvallisuuden parantamiseksi koko EU:ssa. Verkko- ja tietoturvadirektiivi (NIS-direktiivi) lisää jäsenvaltioiden välistä yhteistyötä kyberturvallisuuden tärkeällä alalla. Direktiivin tavoitteissa todetaan, että ”siinä asetetaan turvallisuuteen liittyviä velvoitteita keskeisten palvelujen tarjoajille (kriittiset toimialat kuten energia, liikenne, terveys ja rahoitus) ja digitaalisten

palvelujen tarjoajille (verkossa toimivat markkinapaikat, hakukoneet ja pilvipalvelut)". EU-maiden on lisäksi nimettävä yksi tai useampi kansallinen vastuuviranomainen sekä laadittava strategia kyberuhkien varalta. (Eurooppa-neuvosto, 2016)

Kyseinen Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148 on annettu 6 päivänä heinäkuuta 2016. Direktiivin toimenpiteiden tuli olla kansallisella tasolla käynnissä 9. toukokuuta 2018 lukien. Direktiivin kohteesta ja soveltamisalasta on todettu seuraavaa:

> "1.Tässä direktiivissä säädetään toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden saavuttamiseksi unionissa sisämarkkinoiden toiminnan parantamiseksi.
>
> 2.Tätä varten tässä direktiivissä
>
> a) säädetään kaikkien jäsenvaltioiden velvollisuuksista hyväksyä verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia;
>
> b) luodaan yhteistyöryhmä tukemaan ja helpottamaan strategista yhteistyötä ja tiedonvaihtoa jäsenvaltioiden kesken sekä kehittämään luottamusta ja luotettavuutta niiden keskuudessa;
>
> c) luodaan tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (computer security incident response teams) verkosto, jäljempänä 'CSIRT-verkosto', edistämään luottamuksen ja luotettavuuden kehittämistä jäsenvaltioiden välillä sekä edistämään ripeää ja tehokasta operatiivista yhteistyötä;
>
> d) otetaan käyttöön keskeisten palvelujen tarjoajia sekä digitaalisen palvelun tarjoajia koskevat turvallisuus- ja ilmoitusvaatimukset;
>
> e) säädetään jäsenvaltioiden velvollisuuksista nimetä kansalliset toimivaltaiset viranomaiset, keskitetyt yhteyspisteet ja CSIRT-toimijat, joiden tehtävät liittyvät verkko- ja tietojärjestelmien turvallisuuteen."

Direktiivi velvoittaa jäsenvaltiot määrittämään direktiivin soveltamisalan mukaisilla toimialoilla ja niiden osa-alueilla keskeiset palvelujen tarjoajat. Direktiivin 5. artiklassa on määritelty kriteerit keskeisten palvelujen tarjoajien määrittämiseksi seuraavasti: "Direktiivin mukaan tällöin on tarjottava palvelua, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi. Tämän palvelun on oltava riippuvainen verkko- ja tietojärjestelmistä. Lisäksi palveluun kohdistuvalla poikkeamalla tulisi olla direktiivin 6 artiklassa tarkoitettu merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen". Direktiivi jättääkin jäsenvaltioille päätösvaltaa keskeisten palveluiden määrittelemisessä.

Liikenne- ja viestintäministeriö lokakuussa 2016 asettama poikkihallinnollinen työryhmä valmisteli NIS-direktiivin kansallista täytäntöönpanoa. Loppuraportti on julkaistu 20.4.2017. Raportin mukaan yhteiskunnan toiminnan kannalta keskeisten palveluiden määrittäminen on kullakin direktiivin mukaisella toimialalla ja niiden osa-alueella riippuvaista toimialakohtaisista erityispiirteistä. Lisäksi todetaan, että "palveluiden keskeisyyteen vaikuttavat muun muassa palveluiden merkitys kansalaisille ja yrityksille, teollisuuden riippuvaisuus kysei-

sistä palveluista sekä se kuinka paljon erilaisia kilpailevia palveluita on markkinoilla saatavilla" ja, että "yhteiskunnan toiminnan kannalta keskeiset palvelut voivat olla huoltovarmuuskriittisiä tai kriittistä infrastruktuuria laajempi joukko toimijoita". NIS-direktiivin kansallista täytäntöönpanossa tullaan määrittämään keskeisten palveluiden tarjoajat lain tasolla. (Liikenne- ja viestintäministeriö, 2017, 29).

Palveluntarjoajien toimintaan liittyvät tietoturvariskien hallinta ja raportointivaatimuksen direktiivissä on asetettu seuraavasti: (Hallituksen esitys eduskunnalle, HE 192/2017 vp)

1. Energia/sähkön osa-alue:
- siirtopalvelu kantaverkossa ja järjestelmävastaavan kantaverkonhaltijan tarjoamat järjestelmäpalvelut
- sähkönjakelu jakeluverkossa, ei kuitenkaan sähkönjakelu suljetussa jakeluverkossa
- sähkönjakelu suurjännitteisessä jakeluverkossa, ei kuitenkaan sähkönjakelu suljetussa jakeluverkossa

2. Liikenne:
- lennonvarmistuspalvelu,
- rautatieliikenteen ohjauspalvelu,
- alusliikennepalvelu,
- lentoaseman hallinta,
- valtion rataverkon hallinta,
- sataman hallinta sekä
- ITS-direktiivin tarkoittaman ITS-järjestelmän ylläpito

3. Pankkiala ja finanssimarkkinoiden infrastruktuurit:
- luottolaitoslain mukainen luottolaitostoiminta
- sekä kaupankäynnistä rahoitusvälineillä annetun lain mukaisen pörssitoiminnan harjoittaminen.

4. Terveydenhuoltoala:
- terveydenhuollon asiakastietojen sähköinen käsittely sekä
- terveyden huollon laitteiden ylläpitäminen ja käyttäminen julkisten ja yksityisten sosiaalihuollon ja terveydenhuollon palvelujen tarjonnassa.

5. Juomaveden toimittaminen ja jakelu:
- vesihuoltolaitokset, jotka toimittavat vettä vähintään 5000 kuutiometriä vuorokaudessa sekä
- vesihuoltolaitokset, jotka toimittavat näille vettä.

6. Digitaalinen infrastruktuuri:
- aluetunnusrekisterin ylläpito. Tietoyhteiskuntakaareen sisältyy velvoitteet aluetunnusrekisterin ylläpitäjälle huolehtia tietoturvasta.

Viestintävirasto on lain mukaan fi-aluetunnusrekisteriä ylläpitävä viranomainen. Ahvenanmaan maakuntahallinto ylläpitää ax-aluetunnusrekisteriä.

7. Digitaalisten palvelujen tarjoajat:
- pilvi- ja hakukonepalvelua tarjoavat organisaatiot sekä
- verkossa toimiva markkinapaikka.
  Verkko- ja tietoturvadirektiivissä ei ole jätetty jäsenvaltioille vastaavaa palvelun keskeisyyttä koskevaa määritystehtävää koskien digitaalisten palveluiden tarjontaa, vaan direktiivin velvoitteet koskevat kaikkia direktiivin soveltamisalaan kuuluvia palveluntarjoajia.

## 3.8 Kyberturvallisuus ja tilannetietoisuus

### 3.8.1 Tilannetietoisuuden tarve

Organisaation päätöksenteko edellyttää kulloiseenkin käyttöön sopivaa ja tarkoituksenmukaista, reaaliaikaista, oikeisiin tietoihin ja arvioihin perustuva tilannetietoisuutta. Häiriötilanteissa päätöksentekijöiden on tiedettävä toimenpiteidensä perusta ja seuraukset sekä arvioitava muiden reagointi niihin ja arvioitava päätöksiin sisältyviä riskejä. Organisaation päätöksentekijöillä tuleekin olla kunkin toimintatason edellyttämä tilannetietoisuus ja -ymmärrys, joka mahdollistaa oikea-aikaisen päätöksenteon ja toiminnan. Tilannetietoisuuden ja -ymmärryksen muodostaminen edellyttää myös päätöksentekijöiden yhteistoimintaa ja osaamista, jolloin mahdollistuu kokonaisvaltainen toimintaympäristön seuranta, informaation analysointi, kokoaminen ja jakaminen. Tietojärjestelmillä on keskeinen rooli eri osapuolten yhteistoiminnassa ja tietolähteiden systemaattisessa käytössä sekä joustavassa tilannetietojen jakamisessa. (Turvallisuuskomitea, 2010, 54)

Yhteiskunnan turvallisuusstrategissa vuodelta 2010 tilannetietoisuudesta on todettu seuraavasti: (Turvallisuuskomitea, 2010, 54,55)

> ”Organisaatioiden ja päätöksentekijöiden tilannetietoisuuden muodostamista tuetaan tilannekuvajärjestelyillä. Yleisesti tilannekuva tarkoittaa asiantuntijoiden kokoamaa kuvausta vallitsevista olosuhteista ja eri toimijoiden toimintavalmiuksista, häiriötilanteen synnyttäneistä tapahtumista, sitä koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista. Tilannekuvaan saattaa liittyä tietojen analysointiin perustuvia toimintasuosituksia. Kokonaisuus muodostetaan verkostoitunutta toimintamallia hyväksikäyttäen ja kokoamalla tietoja eri lähteistä. Toiminnasta muodostuu tällöin prosessi informaation keräämistä, kokoamista, luokittelua ja analysointia varten. Prosessi palvelee myös analysoidun tiedon oikea-aikaisesta ja tehokkaasta jakamisesta sitä tarvitseville. Ympäröivä ”tietoavaruus” järjestetään siten, että tieto ymmärretään oikein ja toimijoilla on mahdollisuus saada oman toimintansa kannalta tärkeä tieto.”

Yhteiskuntaan ja sen organisaatioihin kohdistuvat laaja-alaiset häiriötilanteet ovat haasteellinen kybertoimintaympäristö tilannehallinnan edellyttämän kriit-

tisen reagointinopeuden osalta. Pitkälle kehittyneet ja perinteisille suojaustavoille vieraat kyberhyökkäykset (APT- eli Advanced Persistent Threat -hyökkäykset) voivat edetä tietoverkossa nopeasti, jolloin hyvä tilannetietoisuus ja tiedonvaihto ovat keskeisessä roolissa häiriötilanteen hallinnasta. Pahimmassa tapauksessa toiminnan vastuuttaminen pitäisi pystyä tekemään välittömästi ja siten käynnistämään suojaus- ja vastatoimet viivytyksettä sekä hyödyntämään käytössä olevat kyberturvallisuuden kyvykkyydet ja välineet. (Valtiontalouden tarkastusvirasto, 2017.)

Organisaatiot toimivat erittäin monimutkaisissa, toisiinsa liittyvissä kyberympäristöissä, joissa käytetään uusia tai jo pitkään käytössä olleita tietoteknisiä järjestelmäkokonaisuuksia tai näiden yhdistelmiä (system of systems). Organisaatiot ovat riippuvaisia näistä järjestelmistä ja niiden laitteista tehtäviensä suorittamiseksi. Johdon on tunnustettava, että selkeät, hyvin perustellut riskipohjaiset päätökset ovat välttämättömiä toiminnan jatkuvuuden näkökulmasta katsottuna. Riskienhallinta parhaimmillaan yhdistää organisaatioiden yksilöiden ja eri ryhmien parhaat kollektiiviset arviot riskeistä, jotka liittyvät strategiseen suunnitteluun sekä liiketoiminnan operatiivisen ja päivittäiseen johtamiseen. Riskin ymmärtäminen ja käsitteleminen ovat organisaation strategisia kyvykkyyksiä ja avaintehtäviä toimintojen organisoinnissa. Nämä edellyttävät organisaation laajuisesti muun muassa johdon eri tasoilla jatkuvaa turvallisuusriskien tunnustamista ja ymmärtämistä. Turvallisuusriskejä voi kohdistua organisaation oman toiminnan lisäksi yksilöille, muille organisaatioille ja koko yhteiskunnalle. (NIST 800-39, 1-2)

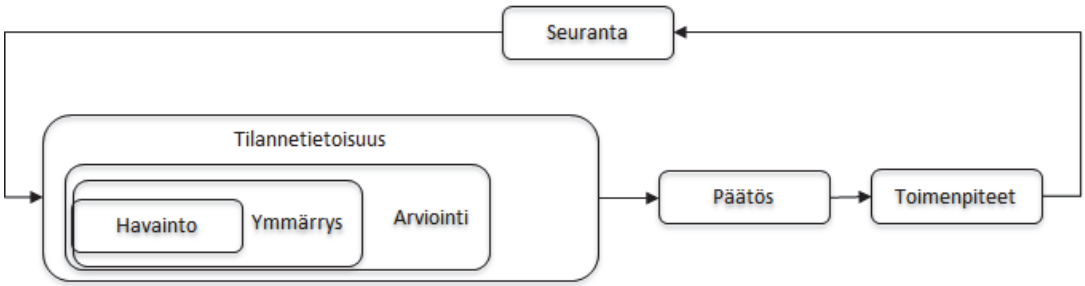
Managing Information Security Risk julkaisu suosittaa organisaatioiden kyberturvallisuuden riskienhallinnan toteuttamista kokonaisvaltaisena toimintana, jossa käsitellään riskejä strategiselta tasolta taktiselle tasolle. Siten varmistetaan, että riskipohjainen päätöksenteko on integroitu organisaation kaikkiin osiin. (NIST 800-39, 6)

Sama julkaistu painottaa riskien seurantatoimenpiteiden merkitystä jokaisella päätöksentekotasolla. Esimerkiksi taktisella tasolla seurantatoimet saattavat sisältää jatkuvia uhka-arviointeja siitä, miten alueen muutokset voivat vaikuttaa strategiselle ja operatiiviselle tasolle. Operatiivisen tason seurantatoimiin voi puolestaan sisältyä esimerkiksi uusien tai nykyisten tekniikoiden analysoinnit, jotta voidaan tunnistaa niistä aiheutuvat riskit liiketoiminnan jatkuvuudelle. Strategisen tason seurantatoimet voivat usein keskittyä organisaation tietojärjestelmäkokonaisuuksiin, toiminnan standardisointiin ja vaikka jatkuvaan turvallisuustoiminnan valvontaa. (NIST 800-39, 45)

Organisaation riskien seurantatoimenpiteiden tarpeellisuudesta voi vetää johtopäätöksen koko organisaation tilannetietoisuuden tarpeellisuuteen. Kuten edellä on kuvattu, organisaatioiden ja päätöksentekijöiden tilannetietoisuuden muodostamista tuetaan tilannekuvajärjestelyillä. Tarkoituksenmukainen tilannetietoisuus mahdollistaa tukea kyberturvallisuuden rikien hallintaa sekä myös laajemminkin organisaation koko kyberkyvykkyyden arviointia.

### 3.8.2 Tilannetietoisuuden teoria

Mica Endsley (1995) on kehittänyt tilannetietoisuuden mallia työskennellessään useissa eri tutkimustehtävissä Yhdysvaltojen ilmavoimien palveluksessa. Kuviossa 5 on esitetty mallin yleinen rakenne (Endsley 1995, muokattu). Tilannetietoisuuden ydin koostuu kolmesta peruselementistä, jotka ovat havaitseminen (Level 1), tilanteen ymmärtäminen (Level 2) ja sen vaikutuksen arviointi tulevaisuuteen nähden (Level 3). Näin muodostettava tilannetietoisuus antaa perusteet johtopäätöksiin ja niistä seuraavaan päätöksentekoon. Siihen vaikuttavat myös tilanteen mukaiset tehtävä- tai järjestelmäkohtaiset ominaisuudet sekä päätöksentekijän kokemukset ja arviointikyky. Päätöksenteko puolestaan ohjaa toimintaa, joka heijastuu takaisin havainnoitavaan toimintaympäristöön.




KUVIO 5 Tilannetietoisuus ja dynaaminen päätöksenteko.

Sid Faber pitää kirjoituksessaan ”Flow Analytics for Cyber Situational Awareness” (2015) toimia tilannetietoisuuden kehittämiseksi, niin julkisten kuin yksityisten organisaatioiden osalta, eräänä merkittävimmistä kyberturvallisuuden parantamiseen tähtäävistä lähiajan tavoitteista. Faber suosittaa Endsleyn kehittämän rakenteen soveltamista kybertoimintaympäristön seurantatarpeisiin. (Faber, 2015)

Tilannekuva on käsitteenä monitahoinen. Rauno Kuusiston Liikenne- ja viestintäministeriölle laatimassa raportissa ”Tilannekuvasta täsmäjohtamiseen. Johtamisen tietovirrat kriisin hallinnan verkostossa” (2005) on selvitetty tilannetietoisuuden rakentumista eri viranomaisten välillä. Tutkimusraportissa on selvitetty tilannekuvakäsitettä ja päädytty toteamaan tilanteesta ja tilannekuva seuraavasti: (Kuusisto, 2005)

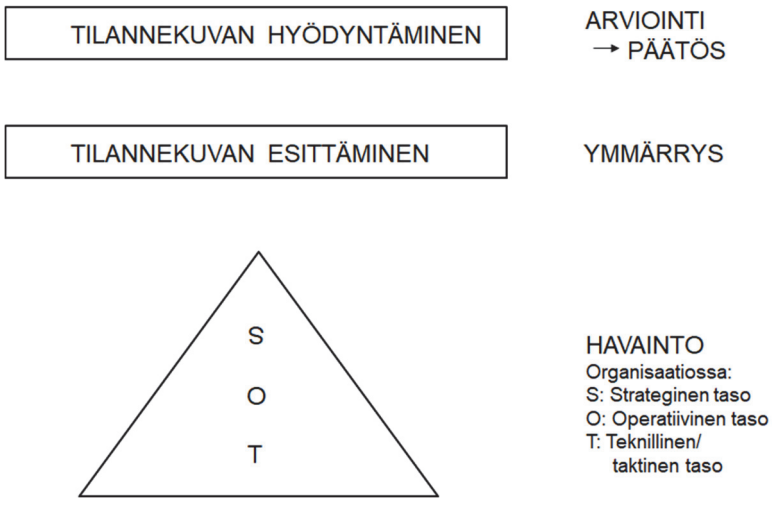
> ”Tilanne on käsite, joka kuvaa ajallisilla määreillä rajattavissa olevia toimijan omia tai sen ulkopuolelle olevien toimijoiden aikaansaamia tapahtumia.”

> ”Tilannekuva on tietystä tilanteesta saatu kuva tai käsitys. Koska tilannekuvalla on käsitteenä tavattoman erilaisia merkityksiä ja tulkintoja, on sen käyttö eksaktissa, yleisessä tekstissä hankalaa.”

Endsleyn kehittämän tilannetietoisuuden mallin yleistä rakennetta on sovellettu tässä tutkimuksessa. Väitöstyön tutkimusvaiheeseen muodostettu ja siinä käy-

tetty kriittisen infrastruktuurin ja organisaation tilannetietoisuuden muodostamisen viitekehys on esitetty kuviossa 6. Kuviossa tilannetietoisuus muodostuu havainnoista rakentuvien tilannekuvien eittämisen ja hyödyntämisen kautta.

Kuviossa 6 Endsleyn rakenteen havaintokohteita (Level 1) siinä edustavat strategisen (S), operatiivisen (O) ja teknillisen/taktisen (T) päätöksentekotasojen organisaatiokohtaiset havaintotarpeet. Tavoitteena on aikaansaada kutakin päätöksentekotasoa palveleva havaintokyky. Havainnoista muodostettavan tilannekuva, jonka esittäminen on puolestaan edellytys havaintojen ymmärtämiseen (Level 2). Tämän jälkeen muodostuvat edellytykset havaintojen vaikutusten analysoimiseksi ja arvioimiseksi tilannekuvaa hyödyntäen ja ymmärrystä hyväksi käyttäen (Level 3). Siinä analysointikyvykkyys on ratkaisevassa roolissa. Lopullisena tavoitteena on kullekin päätöksentekotasolle tarkoituksenmukaisten ja tilannekohtaisten oikeiden päätösten tekeminen ja päätösten mukaisten toimenpiteiden ohjaus. Organisaatiokohtaisella eri päätöksentekotasolle muodostuvan havaintotietojen luokittelulla mahdollistetaan tietojen siirto tasojen välillä ja siten kokonaiskuvan aikaansaaminen.




KUVIO 6 Tutkimuksen tilannetietoisuuden muodostamisen viitekehys.

Valtioneuvoston kanslian tilaamassa tutkimuksessa ”Kriittisen infrastruktuurin tilannetietoisuus” (2017) on tilannekuvallejärjestelmälle esitettyjä vaatimuksia. Tämän tutkimuksen kannalta katsoen tärkeimmät vaatimukset ovat: (Horsmanheimo, ym., 2017)

- ”Tilannekuva on sarja esityksiä, joiden muodolla ei ole väliä. Olennaista on, että joku hallinnoi sitä, tekee analyysiä ja päätöksiä.”
- ”Tilannekuvajärjestelmään tuotetaan tietoa yhteistyönä. Jokainen toimija vastaa itsenäisesti oman osaamisalueensa tiedon tuottamisesta ja oikeellisuudesta.”

- ”Tiedon on oltava prosessoitua, analysoitua ja ymmärrettävää. Sillä on oltava merkitys sekä itselle että muille vastaanottajille.”
- ”Tietojen pitäisi olla esitettyinä visuaalisesti ja selkeästi.”
- ”Tiedot on esitettävä ilman tarpeettomia teknisiä yksityiskohtia. Tiedon on oltava ymmärrettävää muiden alojen ihmisille.”
- ”Tilannekuvajärjestelmän pitäisi olla dynaaminen sekä käyttäjittäin tai toimialoittain räätälöity. Tiedoista pitäisi saada eritasoisia näkymiä.”
- ”Terminologian ja luokitusten pitäisi olla yhdenmukaista.”
- ”Tilannekuvajärjestelmän olisi oltava sisällytettävissä organisaatioiden prosesseihin siten, että tilannekuvajärjestelmän ylläpitämisestä ei tule ylimääräistä tehtävää suurhäiriötilanteisiin.”
- ”Eri toimijoiden pitäisi pystyä määrittelemään, mitä tietoa he tarvitsevat ja mitä tietoa he pystyvät järjestelmään syöttämään.”
- ”Tilannekuvajärjestelmällä pitäisi voida vaihtaa tietoja eri toimijoiden välillä eri organisaatiotasoilla. Tietoa pitäisi pystyä jakamaan myös valvoviin organisaatioihin.”
- ”Tilannekuvajärjestelmästä pitäisi saada ennusteita siitä, mitä tapahtuu 3, 6, 12 tunnin päästä.”
- ”Tilannekuvajärjestelmässä pitäisi pystyä esittämään ajallinen dimensio, miten asiat ovat kehittyneet - ollaanko menossa huonompaan suuntaan vai parempaan.”

### 3.8.3 NIS-direktiivi ja tilannetietoisuus

Kyberturvallisuuden laajan tilannetietoisuuden luomisessa korostuvat niin teknillinen, verkostomainen kuin hallinnollinenkin tilannekuva. Suomessa osa organisaatioista on kehittänyt viime vuosien aikana kyberturvallisuuden tilannekuvaa eri toimijoiden keskinäisten tietojenvaihtomekanismien avulla. Kyse on niin kansallisesta kuin kansainvälisestäkin yhteistoiminnasta. Kehityksestä huolimatta kyberturvallisuudessa toimivien eri osapuolten tietojenvaihdossa sekä havaintokyvyssä on edelleen parannettavaa. (Lehto, ym., 2017, 69)

Edellä mainittu tarve kehittää kansallista tilannetietoisuutta pitää sisällään tietoisuuden siitä, että Suomessa viestintäpalveluita ja digitaalista infrastruktuuria koskeva sääntely sisältyy keskeisin osin lakiin sähköisen viestinnän palveluista. Laki sisältää viranomaisten laajan keinovalikoiman puuttua viestintäverkkojen ja -palvelujen häiriötilanteisiin normaalioloissa. Lisäksi laki sähköisen viestinnän palveluista muun muassa edellyttää, että teleyritys ja niin sanottu lisäarvopalvelun tarjoaja on velvollinen ilmoittamaan käyttäjille ja viranomaisille havaitsemistaan kyberturvallisuuden häiriöistä. Viestintävirasto valvoo säännösten noudattamista. (FINLEX, 2014, Luku 33)

NIS-direktiivi laajentaa edellä mainittua lakia sähköisten viestinnän palveluista. Se mukaisesti ”direktiivi asettaa listan velvoitteita, kuten ilmoitusvelvollisuus, niin jäsenmaille kuin valituille yksityisen ja julkisen sektorinkin toimijoille”.

Lisäksi se edellyttää jäsenmailta yhteistyötä verkkoturvallisuuden osalta ja vaatii sen alaisille toimijoille toimenpiteitä verkko- ja tietojärjestelmäturvallisuuden riskien vaikutusten minimoimiseksi. (Euroopan unionin verkko- ja tietoturvadirektiivi, 2016)

NIS-direktiivi edellyttää, että jäsenvaltioiden oli otettava sen velvoitteet osaksi kansallista lainsäädäntöä viimeistään 9. toukokuuta 2018. Direktiivillä jäsenvaltiot velvoitetaan laatimaan kansallinen verkko- ja tietojärjestelmien turvallisuutta koskeva strategia sekä määrittämään direktiivistä johtuvia viranomaistehtäviä tietoturvallisuuden varmistamiseksi ja riskien hallitsemiseksi eri toimialoilla. Jäsenvaltiot velvoitetaan myös osallistumaan keskinäiseen yhteistyöhön uusissa EU-tason yhteistyöryhmissä tietoturvaloukkauksia koskevien tietojen sekä parhaiden kansallisten käytäntöjen vaihtamiseksi. Lisäksi jäsenvaltioiden on määriteltävä niin kutsutut ”keskeisten palveluiden tarjoajat” sekä ”digitaalisen palvelun tarjoajat” direktiivin soveltamisalan mukaisilla toimialoilla sekä velvoitettava nämä huolehtimaan tietoturvallisuuteen liittyvästä riskienhallinnasta ja häiriöraportoinnista.

Hallituksen esityksessä eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta todetaan, että yhteiskunnan toiminnan kannalta keskeisten palvelujen tietoturvallisuuden parantamiseksi lisättäisiin säännökset palveluntarjoajien velvollisuuksista. Esityksessä todetaan säädöksien lisäämistä ja velvollisuuksista seuraavasti: (Eduskunta, 2017)

> ”Lisäyksiä edellytetään tietoyhteiskuntakaareen, ilmailulakiin, rautatielakiin, alusliikennepalvelulakiin, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin, liikenteen palveluista annettuun lakiin, sähkömarkkinalakiin, maakaasumarkkinalakiin sekä vesihuoltolakiin. ”

> ”Velvollisuuden edellyttävät, että palvelujen tarjoajat huolehtivat viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittavat merkittävästä tietoturvallisuuteen liittyvästä häiriöstä valvovalle viranomaiselle ja yleisölle. Tietoyhteiskuntakaaren velvoitteet koskevat verkossa toimivan markkinapaikan tarjoajaa, hakukonepalvelun tarjoajaa sekä pilvipalvelun tarjoajaa. Ilmailulain velvoitteet koskevat lennonvarmistuspalvelun tarjoajaa sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjää. Rautatielain velvoitteet koskevat valtion rataverkon haltijaa sekä liikenteenohjauspalveluita tarjoavaa yhtiötä. Alusliikennepalvelulain velvoitteet koskevat alusliikennepalvelun tarjoajaa. Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain velvoitteet koskevat yhteiskunnan toiminnan kannalta merkittävän sataman pitäjää. Liikenteen palveluista annetun lain velvoitteet koskevat älykkään liikennejärjestelmän ylläpitäjää. Sähkömarkkinalain velvoitteet koskevat verkonhaltijaa. Maakaasumarkkinalain velvoitteet koskevat siirtoverkonhaltijaa ja vesihuoltolain velvoitteet vesihuoltolaitosta, joka toimittaa vettä vähintään tai ottaa vastaan jätevettä 5000 kuutiometriä vuorokaudessa.”

> ”Toimivalta valvoa riskienhallinta- ja häiriöraportointivelvoitteita olisi sektorikohtaisilla valvontaviranomaisilla. Tämä tarkoittaisi Viestintävirastoa, Liikenteen turvallisuusvirastoa, Energiavirastoa, Finanssivalvontaa, sekä elinkeino-, liikenne- ja ympäristökeskusta. Viranomaisten välisen yhteistyön turvaamiseksi ehdotetaan viranomaisten toimivaltuuksia koskevan lainsäädännön yhteyteen lisättäväksi säännökset valvovien viranomaisten yhteistyöstä sekä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi tarvittavien salassa pidettävien tietojen vaihdosta.”

Viestintävirasto on nykyään osa 1. tammikuuta 2019 perustettua Liikenne- ja viestintävirasto Traficomia, joka on Liikenne- ja viestintäministeriön hallinnonalalla toimiva asiantuntijavirasto. Traficomin on organisoitu osaamisalueiksi, joita ovat muun muassa Digitaaliset yhteydet ja Kyberturvallisuuskeskus. Edellisen vastuualueet ovat Digitaalinen infra, Toimivat markkinat, Markkinatieto, Luvat ja tunnukset sekä Taajuudet ja media. Kyberturvallisuuskeskuksen vastuualueet ovat puolestaan Viestintäverkkojen ja -palveluiden toimintavarmuus, Turvallisuuden kehittäminen ja valvonta sekä Kyberturvallisuuden tilannekuvan tuottaminen. (Traficom, 2020)

Kansallisen kyberturvallisuuden tilannekuvan muodostamisen, analysoinnin ja häiriötilanteiden hallinnan osalta Kyberturvallisuuskeskus (KTK) muodostaa keskisimmän osan. Kyberturvallisuuskeskuksen tehtäväalueita ovat: (Kyberturvallisuuskeskus, 2020)

1. ”Kyberturvallisuuskeskus toimii kansallisena tietoliikenneturvallisuusviranomaisena (National Communications Security Authority, NCSA) ja vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Kyberturvallisuuskeskuksen NCSA-toiminto on osa Suomen turvallisuusviranomaisorganisaatiota.”

2. ”Kyberturvallisuuskeskuksen CERT-toiminto (Computer Emergency Response Team, CERT) huolehtii Tietoyhteiskuntakaaressa (917/2014) säädetyistä tietoturvaloukkausten ennaltaehkäisy-, selvitys- ja tiedotustehtävistä. Tarkemmin sanoen seuraavista tehtävistä ja tavoitteista:

    - Selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

    - Kerätä tietoa verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista.

    - Tiedottaa tietoturva-asioista.

    - Toiminnan tavoitteet liittyvät yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistamiseen sekä yhteiskunnan elintärkeiden toimintojen turvaamiseen.”

Kyberturvallisuuskeskus on kansallista tilannetietoisuutta kokoava ja muodostava viranomaistaho. Kyberturvallisuuskeskus tekee läheistä yhteistyö muiden viranomaisten ja julkisen sektorin organisaatioiden sekä yksityisen sektorin toimijoiden kanssa. NIS-direktiivin kansallinen implementointi laajentaa tätä yhteistyötä ja parantaa siten kokonaistilannetietoisuutta.

# 4 TUTKIMUSMENETELMÄ JA TIEDONHANKINTA

## 4.1 Tutkimusote

### 4.1.1 Pehmeä systeemimetodologia

Pehmeää systeemimetodologiaa, SSM (Soft Systems Methodology, SSM) perustuu Lancasterin yliopiston professori Peter Checkland 1970-luvun lopulta alkaen kehittämään työskentelytapaan. Nykyisen perusmuotonsa se sai vuonna 1981 hänen julkaisemassa teoksessa ”Systems Thinking, Systems Practice". Menetelmässä tarkasteltava kohde on kokonaisuus, joka voidaan ymmärtää ja kuvata systeeminä. Systeemille on tunnusomaista, että sen rajat voidaan määrittää tunnistettavasti. Lisäksi siitä voidaan erottaa tekijät ja toimijat sekä niiden väliset vuorovaikutukset. Tutkimuksessa käytettävä malli pitää sisällään seitsemän vaihetta, joissa kuvataan olemassa olevaa todellisuutta ja luonnostellaan mahdollista tulevaisuutta. Teoksessa vuodelta 1981 ”Systems Thinking, Systems Practice" Checkland toteaa, että

> ”Näin voidaan parhaassa tapauksessa saavuttaa sellainen ratkaisu, joka on sisällöl- lisesti enemmän kuin pelkkä tekninen, toimintaa kuvaava malli.”

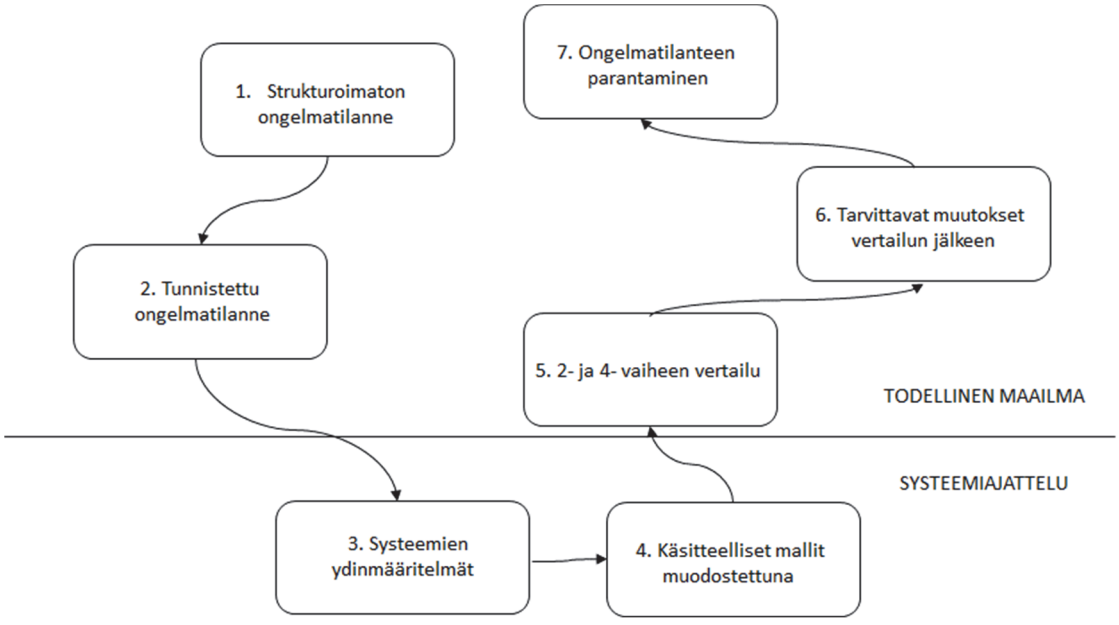
Pehmeää systeemimetodologia on menetelmällinen kokonaisuus, joka muodostaa kehikon inhimillisten systeemien käytännön tason ongelmaratkaisuun. Tällaiset systeemit (järjestelmät) kostuvat tyypillisesti yhdistelmistä, jotka pitävät sisällään ihmisyhteisöjä ja teknillisiä järjestelmiä. Menetelmää voidaan hyödyntää erityisesti sellaisessa tutkimuksissa, jossa systeemin (organisaation, yrityksen, kunnan, vuorovaikutusjärjestelmän tms.) toiminta edellyttää kehitystyötä esimerkiksi toimintaympäristössä tapahtuvan nopean muutoksen tai uuden oleellisesti toimintaan vaikuttavan informaation vuoksi. Menetelmää on myös käytetty tulevaisuudentutkimuksessa, jolloin organisaatioita ja sen kehitysvaihtoehtoja voidaan lähestyä systeemisestä näkökulmasta. Tällöin organisaatio ymmärre-

tään toiminnallisena ja vuorovaikutuksellisena kokonaisuutena. Kehitystoimenpiteillä voidaan vaikuttaa sen toimintaprosesseihin, teknisiin apuneuvoihin ja sisäisiin osajärjestelmiin sekä sisäisiin ja ulkoisiin sidosryhmiin. (Rubin, 2014, 1)

SSM:n avulla pystytään kehityskohteena oleva systeemi jäsentämään osa-alueisiin, selvittämään siihen liittyvät toimintamallit, käytännöt ja prosessit, joihin pyritään kehitystoimenpiteet kohdistamaan. SSM:n on siten koonnos periaatteita ja toimenpiteitä, joiden perusteella organisoitumista edellyttävä kokonaisuus voidaan hahmottaa systeeminä. Systeemikuvauksen kohdetta voidaan SSM:n periaatteiden ja toimenpiteiden avulla tutkia ja kehittää toiminnallisesti ja parantaa johtamisen toimintaedellytyksiä sen muodostamassa kokonaisuudessa. (Checklandin, 1985)

SSM:n perusmalli tutkimusprosessina sisältää seitsemän perättäistä vaihetta. Kahdessa ensimmäisessä vaiheessa tutustutaan tutkimuskohteeseen ja siitä muodostuvaan ongelma-asetteluun. Kaksi ensimmäistä vaihetta ovatkin nykytilanteesta johtuvan ongelmatilanteen määrittelyä ja ymmärtämistä. Kolmannessa vaiheessa tehdään ydinmääritelmät tutkimuskohteena olevan systeemin (organisaation) perustoiminnoista. Neljännessä vaiheessa laaditaan systeemiajattelun käsitteelliset mallit kehitystoimenpiteistä, joiden perusteella systeemin tulevia näkymiä voidaan tarkastella. Viidennessä vaiheessa vertaillaan systeemin (organisaation) nykytilannetta siihen, mitä kehitysmahdollisuuksia tulevaisuudessa toimintaan voisi todellisuudessa liittää. Vertailuvaiheen kautta saadun tiedon avulla määritellään tarvittavat ja toteuttamiskelpoiset muutokset. Vaiheessa seitsemän luodaan menettelyt muutoksen aikaansaamiseksi. Vaiheeseen liittyy myös systeemin (organisaation) jäsenten sitouttaminen toimenpiteiden implementointiin. (Checkland 1981; Checkland & Scholes 1999, A12-A13.)

Kuviossa 7 on esitetty SSM:n perusmalli seitsemän vaihetta (Checkland, 1981, 163).




KUVIO 7 Pehmeän systeemimetodologian perusmalli

### 4.1.2 Pehmeän systeemimetodologian käyttö tutkimuksessa

Checklandin mukaan systeemin perustekijät ovat emergenttisyys, hierarkia, kommunikaatio ja kontrolli. Näistä systeemin ominaisuuksista erityisesti emergenttisyys aiheuttaa muutosta systeemeissä. Se joko vähentää monimutkaisuutta tai synnyttää uutta monimutkaisuutta. Uusi tilanne voi kasvattaa epävarmuutta, koska systeemiin tulee ristiriitaisuutta ja kompleksisuutta. (Checkland 1981, 19)

Systeemissä esiintyä hierarkia ilmenee esimerkiksi teknillisesti siten, että sen elementeiksi voidaan tunnistaa komponentti, yksikkö, alajärjestelmä, ja itse järjestelmä. Infrastruktuuri on kokoelma järjestelmiä ja yleinen infrastruktuuri on toisiinsa kytkettyjen infrastruktuurien verkosto. (Rinaldi, ym., 2001, 13)

Systeemin kolmas elementti on kommunikaatio, jonka avulla välitämme informaatiota. Neljäs elementti on kontrolli tai menetelmä, jolla voidaan vaikuttaa systeemiin vuorovaikutuksen kautta. (Checkland, 1981, 19)

Pehmeässä systeemimetodologiassa on tavoitteena soveltaa tieteellistä menetelmää ihmisen kehittämiin erilaisiin toimintasysteemeihin. Siihen liittyvät tieteellinen päättely ja systeemiajattelu. Organisaation toimintaa voidaan tarkastella pehmeän systeemiajattelun näkökulmasta. Sen vuorovaikutusprosesseista saadaan menetelmän avulla uudenlaista tietoa sekä organisaation sisältä että sen suuntauksista ulospäin. Tällainen tieto auttaa ymmärtämään organisaation systeemejä ja niiden toimintaa. Lisäksi se auttaa myös muuttamaan ja kehittämään niitä. Pehmeä systeemiajattelu soveltuu vaikeasti määriteltäviä tai jäsentyviä kokonaisuuksia ja osa-alueita sisältävien laajojen sosiaalisten ympäristöjen ja niihin sisältyvien ongelma-alueiden tarkasteluun. Systeemimetodologian ja erityisesti pehmeän systeemimetodologian etuna voidaan pitää mahdollisuutta jäsentää ongelmatilanteita osakokonaisuuksiksi ja käsitellä niitä organisoidulla tavalla. Kirjassaan Systems Thinking, Systems Practice" (1981) Peter Checkland painottaa pehmeän systeemiajattelun vahvuutta tutkimuksissa, joissa ratkaisulta edellytetään teknillisen toimintamallin kuvaamista laajempaa tulosta. (Checkland, 1981)

Avoimessa systeemissä informaation lisääntyminen kasvu mahdollistaa monia vaihtoehtoisia polkuja tulevaisuuden muutoksille. Joka tapauksessa informaation lisääntymisen seurauksena tapahtuu muutoksia systeemin ohjausjärjestelmässä (johtamisessa), sisäisissä järjestelmissä, alasysteemeissä ja sitä kautta koko toimintaan ja sen muotoihin aiheutuu muutoksia. Esimerkiksi mahdollisuudet ylläpitää järjestystä, hallita tiedonkulkua tai johtaa systeemiä vanhoilla menetelmillä heikentyvät, kun olosuhteet systeemin sisällä muuttuvat. Kasvavan informaation käsittely edellyttää uutta energiaa, mistä saata seurata lisääntyneen informaation käsittelyyn haasteita. Tilan ennakoimattomuus, hämmennys ja epävarmuus lisääntyvät ja sitä kautta kaaoksen mahdollisuus systeemissä kasvaa. Kaaokseen voi sisältyä sekä uhkia että mahdollisuuksia – tilanne sisältää aihion molempiin. (Rubin, 2014)

## 4.2 Tutkimustietojen muodostaminen

### 4.2.1 Puolistrukturoitu teemahaastattelu ja SWOT-analyysi

RR4. Pöyhönen J. (2018). SWOT-analyysin soveltaminen yrityksen kyberturvallisuuden tilannekuvan muodostamiseen. Tutkimusmenetelmän kuvaus. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 58/2018.

Väitöstutkimuksen taustatutkimuksissa käytettiin teemahaastatteluja SWOT-analyysin rakennetta hyödyntämällä. SWOT-lyhenne tulee englannin kielisistä sanoista Strengths (vahvuudet), Weaknesses (heikkoudet), Opportunities (mahdollisuudet) ja Threats (uhat). SWOT-analyysi on väline analysoitaessa organisaation toimintakykyä ja sen toimintaympäristöä kokonaisuutena. Se on nelikenttämenetelmä, jota käytetään yleensä yrityksen strategian laatimisessa, sekä oppimisen tai ongelmien tunnistamisessa, arvioinnissa ja toimintaprosessien kehittämisessä. SWOT-analyysin kohteena voi olla jonkin yrityksen toiminto, organisaatio koko laajuudessaan tai jonkin tuotteen tai palvelun asema ja kilpailukyky tai esimerkiksi kilpailijan toiminta ja kilpailukyky. Analyysin toteutuksen vastuut ja ylläpito voidaan kuvata organisaation toimintakäsikirjaan kuhunkin tapaukseen tarkoituksenmukaisella tavalla.

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

SWOT-analyysin jaoteltu sisäisiin ja ulkoisiin tekijöihin voidaan toteuttaa kybertoimintaympäristössä esimerkiksi seuraavasti: (Melkman & Simmonds, 2016)

- Vahvuudet ja heikkoudet ovat sisäisiä tekijöitä. Organisaation vahvuus voi olla esimerkiksi hyvät toimintaedellytykset kybertoimintaympäristössä ja maine luotettavana toimijana toimintaympäristön haasteista huolimatta. Heikkous puolestaan voi olla organisaation kyvyttömyys tunnistaa toimintaansa osana yrityksen verkottunutta toimintaympäristöä tai puutteet toiminnan varmistamisessa toimintaympäristön asettamissa vaateissa.
- Mahdollisuudet ja uhat ovat ulkoisia tekijöitä. Mahdollisuus voi olla esimerkiksi yrityksen vaikutusmahdollisuus kyberluottamusta lisääviin toimenpiteisiin ulkopuolisia resursseja hyväksi käyttäen. Uhka voi puolestaan muodostua siitä, että yritys ei tunnista toimintaympäristönsä kyberturvallisuuden haasteita ja yrityksen ulkopuolelta uhkaavia tietomurtoja.

SWOT-analyysi on laadullisen eli kvalitatiivinen tutkimus, jossa pyritään ymmärtämään tutkittavaa ilmiötä. Eräs sovellus SWOT-analyysistä on tilannekuvan muodostaminen tutkimuskohteesta, jonka avulla voidaan kuvata siinä esiintyviä ilmiöitä. Ilmiöiden merkityksen tai tarkoituksen selvittämisen avulla puolestaan saadaan muodostettua kokonaisvaltainen ja syvällinen käsitys kohteesta. Teemahaastattelua voidaan pitää yhtenä laadullisen tutkimuksen aineistonhankinnan tapana. Teemahaastattelu on puolistrukturoiduksi haastattelu, koska se on rakenteeltaan avointa haastattelua ennalta tarkemmin määritelty kuin avoin haastattelu, mutta väljempi kuin strukturoitu haastattelu. Tutkimuksen aineiston hankinnassa sovellettiin puolistrukturoitua haastattelua ja SWOT-analyysiä.

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

> ”Teemahaastattelu sijoittuu formaaliudessaan lomakehaastattelun ja avoimen haastattelun väliin. Haastattelu ei etene tarkkojen, yksityiskohtaisten, valmiiksi muotoiltujen kysymysten kautta vaan väljemmin kohdentuen tiettyihin ennalta suunniteltuihin teemoihin. Teemahaastattelussa pyritään huomioimaan ihmisten tulkinnat ja heidän merkityksenantonsa. Ihmisten vapaalle puheelle annetaan tilaa, vaikka ennalta päätetyt teemat pyritään keskustelemaan kaikkien tutkittavien kanssa.”

> ”Teemahaastattelu on keskustelunomainen tilanne, jossa käydään läpi ennalta suunniteltuja teemoja. Teemojen puhumisjärjestys on vapaa, eikä kaikkien haastateltavien kanssa välttämättä puhuta kaikista asioista samassa laajuudessa. Tutkijalla on haastattelussa mukanaan mahdollisimman lyhyet muistiinpanot käsiteltävistä teemoista, jotta hän voisi keskittyä keskusteluun, ei papereiden tavaamiseen. Teemat voi listata esimerkiksi ranskalaisin viivoin ja lisäksi voi laatia joitakin apukysymyksiä tai avainsanoja keskustelun ruokkimista varten. Teemahaastattelun ei siis tulisi olla pikkutarkkojen kysymysten esittämistä tarkassa järjestyksessä paperilta lukien. Teemoista ja niiden alateemoista pyritään keskustelemaan varsin vapaasti. Teemahaastattelu on sopiva haastattelumuoto esimerkiksi silloin, kun halutaan tietoa vähemmän tunnetuista ilmiöistä ja asioista (vrt. puolistrukturoitu ja strukturoitu haastattelu).”

> ”Teemahaastattelu edellyttää huolellista aihepiiriin perehtymistä ja haastateltavien tilanteen tuntemista, jotta haastattelu voidaan kohdentaa juuri tiettyihin teemoihin. Sisältö- ja tilanneanalyysi on siis teemahaastattelussa tärkeää. Käsiteltävät teemat valitaan tutkittavaan aiheeseen perehtymisen pohjalta. Tutkimusaihe ja tutkimuskysymykset on muutettava tutkittavaan muotoon, operationalisoitava. Kysymysten harkitsemisen lisäksi myös haastateltavien valitsemiseen tulee suhtautua harkinnalla: Tutkimukseen osallistuvia ei tulisi valita satunnaisesti tarraten kehen tahansa kulkijaan.”

Kattava yrityksen kyberturvallisuuden analysointi voidaan toteuttaa siten, että tarkastelun näkökulmat ulotetaan organisaation strategiaan, operatiivisiin toimiin ja teknillisen/taktisen tason toimintaan.

Tämän tutkimusalueen osalta SWOT-analyysin teemat johdettiin Suomen kyberturvallisstrategian strategisten linjausten (2013) kohdan 3 yritystoimintaa käsittelevästä kokonaisuudesta. Lisäksi teemojen laadinnassa hyödynnettiin ISO/IEC 9000-laatustandardin seitsemää perusperiaatetta ja ISO/IEC 27000-informaatioturvallisuuden standardin keskeisimpiä pääkohtia.

Teemat yleistettiin otsikkotasolle niin, että niitä voitiin soveltaa puolistrukturoituna haastatteluna minkä tahansa organisaation kartoitukseen. Teemojen

organisaatiokohtaisia haastattelukysymyksiä johdateltiin myös tunnistetuista lähtötiedoista.
Yrityksen vahvuuksia ja heikkouksia arvioitaessa haastatteluteemat olivat:

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

Mahdollisuuksia ja uhkia arvioitaessa teemat olivat:

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

Tutkimuksen haastattelun johdanto-osiossa kohdeorganisaatiolla oli mahdollisuus sijoittaa toimintansa osaksi verkottunutta toimintaympäristöä. Toimintaympäristön yleisellä kuvauksella pyrittiin laajentamaan kohdeorganisaation haastatteluteemoja siten, että tutkimukseen saatiin kohteen sisäisen tutkimuksen lisäksi käsitys sen toiminnasta yhteiskunnan kriittisen infrastruktuurin osana.

Taulukossa 6 haastatteluteemat on sijoitettu väitöstutkimuksen viitekehyksen viidelle kybermaailman rakenteen kerrokselle (kognitiivinen kerros, palvelukerros, semanttinen kerros, syntaktinen kerros ja fyysinen kerros).

TAULUKKO 6 Tutkimuksen viitekehys ja haastatteluteemat ja näkökulmat.

| **Kyber-rakenne** | **Yritystason ICT-toiminto** | **ICS-toiminto** | **SWOT-teemat ja -näkökulmat** |
|---|---|---|---|
| Kognitiivinen kerros | Johtaminen, henkilöstö, sidosryhmät, toimintaverkosto | Johtaminen, henkilöstö, sidosryhmät, toimintaverkosto | Johtaminen, henkilöstön osaaminen, tilannetietoisuus, sidosryhmänäkemys, kyberturvallisuuden hallinta (riskit, toimintapolitiikka, jatkuvuus), toiminnan jatkuva parantaminen |
| Palvelu-kerros | Verkkoyhteydet, IT-palvelut | Verkkoyhteydet | Suojattavat prosessit, ohjausmekanismit, tuotteet ja palvelut |
| Semanttinen kerros | Käyttöliittymät, data | Valvomot, data | Suojattavat prosessit, ohjausmekanismit, tuotteet ja palvelut |
| Syntaktinen kerros | IT-järjestelmät (SW, verkkoliikenne) | Prosessiasemat (SW, verkkoliikenne) | Suojattavat järjestelmät, tuotteet ja palvelut |
| Fyysinen kerros | IT-laitteet | Kenttälaitteet, kaapeloinnit | Hallinta ja ohjausmekanismit |

### 4.2.2 Aineiston sisältölähtöinen analyysi

Sisällönanalyysissä aineistoa ja tutkimuskohdetta tarkastellaan eritellen, yhtäläisyyksiä ja eroja etsien ja asioita tiivistäen. Sisällönanalyysi voi olla tekstianalyysia, jossa tarkastellaan jo valmiiksi tekstimuotoisia tai sellaiseksi muutettuja aineistoja. Esimerkkejä tutkittavista teksteistä ovat kirjat, päiväkirjat, haastattelut, puheet ja keskustelut. Sisällönanalyysin avulla pyritään muodostamaan tutkittavasta ilmiöstä tiivistetty kuvaus, joka kytkee tulokset ilmiön laajempaan kontekstiin. (Saaranen-Kauppinen & Puusniekka, 2006)

Tässä tutkimuksessa aineistolähtöisestä sisällönanalyysiä on sovellettu teoreettiseen viitekehykseen liitettynä. Tarkoituksena on ollut tiedon hankinnan lisäksi saada tutkimukseen induktiivinen ote eli edetä yksittäisistä havainnoista yleisempiin johtopäätöksiin. Kyseessä ei ole kuitenkaan ollut teoreettisen viitekehyksen testaaminen. Aineistoina on käytetty tutkimusalueen kirjallisuutta, tieteellisiä julkaisuja, verkkojulkaisuja, blogeja, raportteja, työryhmä ja kokousaineistoja.

## 4.3 Tutkimusalueen kuvaus

Väitöstutkimuksen osalta kriittisen infrastruktuurin organisaatioiden kyberturvallisuuden strukturoimatonta kokonaistilannetta oli mahdollista selvittää kahden kansallisen kyberturvallisuuden selvitystutkimuksen kautta, joissa väitöstukija toimi tutkijana ja raportoijana.

Aluksi tilannetta kartoitettiin tutkimushankkeen ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” yhteydessä. Tutkimuksen toteutuksesta on todettu seuraavasti: (Lehto, ym., 2017, 10)

> ”Tutkimushankkeessa haastateltiin yhteensä 31 yksityisten yrityksien ja julkisten organisaatioiden tieto/kyberturvallisuudesta vastaavaa henkilöä. Yksityisten yritysten haastattelujen teemat käsittelivät yritysten kyberturvallisuuden vahvuuksia, heikkouksia, uhkia ja mahdollisuuksia. Lisäksi haastattelussa kartoitettiin laajemmin kunkin toimialan kyberturvallisuuden tilaa ja kehittämistarpeita. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina ja haastateltaville luvattiin täysi anonymiteetti.”

Toinen tutkimus, joka oli jatkoa edelliselle, mahdollisti syventää tutkimusalueen lähtötilannetta. Tutkimushanke oli ”Kyberturvallisuuden strateginen johtaminen Suomessa”. Tutkimuksen toteutuksesta on todettu seuraavasti: (Lehto, ym., 2018, 9)

> ”Tutkimushankkeessa kerättiin hyvin monipuolinen ja laaja-alainen aineisto. Keskeisimmät aineistokokonaisuudet olivat eri turvallisuuteen liittyvät strategiat ja ohjeet, olemassa oleva tutkimustieto sekä julkisen sektorin toimijoiden ja alan asiantuntijoiden haastattelut. Tutkimushankkeessa haastateltiin yhteensä 40 yksityisten ja julkisten organisaatioiden johtohenkilöitä ja tieto/kyberturvallisuudesta vastaavia henkilöitä. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina ja haastateltaville

> luvattiin täysi anonymiteetti. Haastatteluaineiston, asiakirja-analyysin sekä kansainvälisen vertailutiedon perusteella luotiin analysoitu tietoaineisto, johon tässä tutkimuksessa esitetyt havainnot, esitykset ja mallit perustuvat."

Molemmissa tutkimuksissa oli mukana laajasti organisaatioita merkittävimmistä yhteiskunnan kriittisen infrastruktuurin organisaatioista. Tutkimustuloksia on tuotu esille tutkimuskohteen yksi eli sähköyhtiön osalta luvussa 5. Samassa luvussa on esitetty myös tutkimuskohteen kaksi eli sairaalan tulokset, jotka perustuvat alueelta käytettävissä olevan tiedon sisältöanalyysiin.

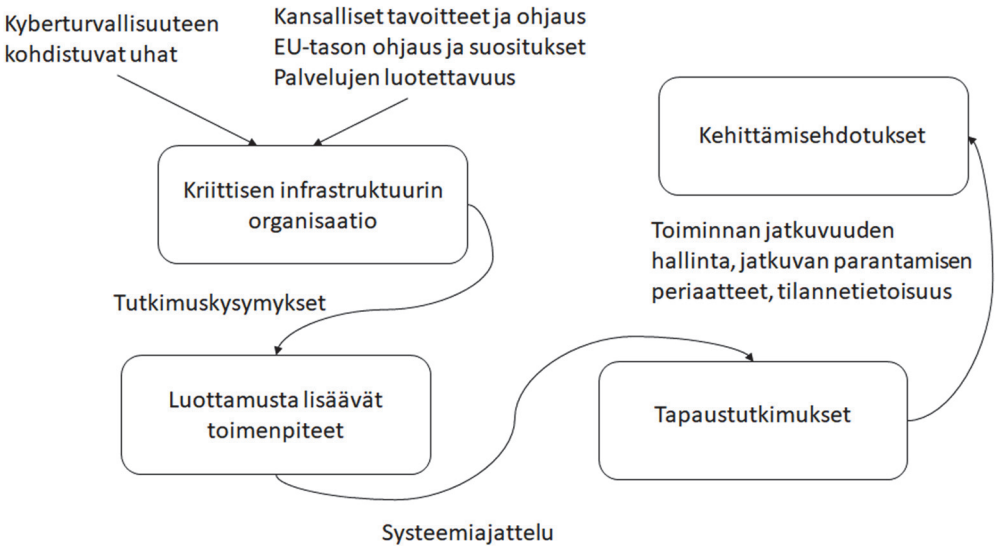
Tämän luvun alakohdissa on määritetty tiivistetysti tutkimusaluetta, SSM-tutkimusprosessin toimijoita sekä laadittu sosiaalisen ja poliittisen systeemin analyysit. Tutkimuksen aikana on laadittu myös CATWOE-analyysi organisaatiotason kyberturvallisuuden osatekijöiden havainnollistamiseksi. Se pitää sisällään määritelmät systeemitasolla asiakkuudesta, toimijoista, muutosprosessista, näkökulmista, omistajista ja toimintaympäristöstä. Tutkimusalueeseen liittyvät SSM-prosessin mukaiset määrittelyt ja analyysit ovat muodostettu tutkimuskohteista yleistetylle tasolle siksi, että niitä voitaisiin hyödyntää mahdollisimman laajasti erityisesti tutkimustulosten osilta kriittisen infrastruktuurin organisaatioissa. SSM-prosessin mukaisia muita menettelyjä on käytetty sähköyhtiön ja sairaalan tapaustutkimuksissa ja tulosten esille tuomisessa. Tutkimustuloksista johdetut organisaation kyberturvallisuuden kehittämisehdotukset ovat luvussa 6. Niiden implementointiin voidaan hyödyntää tämän luvun analyysitietoja. SSM-tutkimusmenetelmä ei pidä sisällään mitään erityistä kehitystoimenpiteiden implementointimenetelmää (kts. KUVIO 7). Väitöstyössä siihen tarkoitukseen esitetään käytettäväksi organisaatioiden toiminnan kehittämisen PDCA-menetelmää.

### 4.3.1 Perusanalyysi

Perusanalyysin (Problem Situation) tarkoituksen on laatia lyhyt ja tiivis määrittely tutkimuskohteesta. Perusanalyysiprosessissa voidaan piirtää peruskuva (Rich Picture) käsiteltävästä ongelma-alueesta havainnollistamaan tutkimuskysymysten taustoja. Kuvalla avulla on mahdollista selkeyttää tutkimustilannetta, johon yleensä liittyy monimutkaisuutta ja kompleksisuutta. Lisäksi kuvalla on tarkoitus täydentämään kirjoitettua testiä. Se myös mahdollistaa esittää vapaamuotoisesti tutkimuksen keskeisimmät entiteetit, rakenteet ja näkökulmat, käytössä olevat prosessit sekä tunnistetut ja potentiaaliset haasteet. (Checkland & Poulter, 2006, 24–26)

Tämän väitöstyön perusanalyysin kuvaus on muodostettu eri tutkimushankkeiden haastattelujen ja projektikokousten ja -tapaamisten tietojen pohjalta. Lisäksi kokonaiskuvan muodostamisessa on hyödynnetty viitelähteitä. Kuvauksessa keskeisimmän entiteetin muodostaa kriittisen infrastruktuurin organisaatiot, joihin kohdistuvat yhtäältä kyberturvallisuuden uhat ja toisaalta yhteiskunnan tavoitteet ja ohjausnormit palvelujen ylläpitämiseksi. Entiteetti koostu laajasta joukosta organisaatioita niin julkiselta kuin yksityiseltäkin sektorilta. Tunnistetut ja potentiaaliset haasteet liittyvät näiden organisaatioiden toiminnan

luotettavuuteen kybertoimintaympäristössä. Organisaation toimintaympäristöstä on johdettu tutkimuskysymykset johtamiseen ja toiminnan kehittämiseen tavoitteena määrittää merkittävimpiä luotettavuuteen vaikuttavia tekijöitä. Systeemitason tarkastelussa organisaatio ja sen tietojärjestelmät on kuvattu viisikerroksisella kyberrakenteella, joka on väitöstyön viitekehys. Tapaustutkimukset on suoritettu systeemitarkastelua hyväksi käyttäen. Perusanalyysin tavoitteena on hahmottaa edellä mainittujen seikkojen avulla tutkimuskokonaisuus. Tutkimuksessa huomio kiinnittyy erityisesti siihen, että millä menettelyillä organisaatioiden on mahdollista ylläpitää toimintaprosessejaan jatkuvasti kompleksisessa kybertoimintaympäristössä. Kyseessä on organisaation toiminnan jatkuvuuden hallinta ja siten palvelujen luotettavuus. Peruskuva (KUVIO 8) sitoo kaikki edellä mainitut seikat tutkimuskokonaisuudeksi, johon pehmeä systeemimetodologian mukainen tutkimusote kohdistuu.




KUVIO 8 Tutkimustilanteen määrittelykuvaus.

### 4.3.2 Interventioanalyysi

SSM-prosessissa on erilaisia toimijoita, joista tutkimusmenetelmän osalta voidaan nimetä asiakas, ongelman käsittelijä tai ratkaisija ja asian tai ongelman omistaja. Asiakas on henkilö tai jokin muu taho (organisaatio, tiimi), jota toiminnan kehittäminen eniten hyödyttää, tai muutoin tunnistaa järjestelmän nykytilan ongelmat ja haluaa kehitystyön avulla saada parannusta tilanteeseen. Ongelman käsittelijän tai ratkaisijan vastuulla on kehittämisprosessien johtaminen ja kehittämistulosten aikaansaaminen. Tämä taho voi myös olla myös asiakas. Kehitystä vaativan ongelman tai haasteen omistajalla tarkoitetaan niitä tahoja, joita tilanne eniten koskettaa. Nämä tahot voivat olla henkilöitä tai prosesseja organisaation sisällä tai ne voivat myös olla erilaisia tekijöitä organisaation ulkopuolella. (Checkland & Poulter, 2006, 27–29)

Kriittisen infrastruktuurin organisaation osalta toiminnan luotettavuutta ja toimintaprosessien jatkuvuuden hallintaa voidaan pitää tarkastelun lähtökohtana. Tällöin asiakkaiksi voidaan tunnistaa niin yrityksen johto kuin palveluja käyttävät organisaation sidosryhmät. Kyberturvallisuuteen liittyvien nykytilan ongelmien tunnistamisella ja kohdeorganisaation kehitystyöllä edistetään näiden tahojen asiakastyytyväisyyttä. Kehittämisprosessien johtaminen ja kehittämistulosten aikaansaaminen on kohdeorganisaation johdon vastuulla. Toisin sanoen organisaation johto on kehitystyössä ongelman käsittelijä tai ratkaisija. Koska tutkimusmetodin mukaan tämä taho voi myös olla asiakas, niin niiksi voidaan nimetä tämän väitöstutkimuksen osalta myös kriittisen infrastruktuurin toiminnasta vastaavat yhteiskunnan tahot. Tällöin kyseeseen tulevat ensisijaisesti NIS-direktiivin kansallisista toimenpiteistä vastaavat ministeriöt sekä huoltovarmuuden osalta Huoltovarmuuskeskus ja kyberturvallisuudesta vastaava Kyberturvallisuuskeskus. Näiden tahojen tuki kriittisen infrastruktuurin organisaation kehitystoimille voidaan järjestää muun muassa ohjeistuksena, tilannetietoisuutena, tukena Huoltovarmuuskeskuksen ICT-poolityön kautta tai tieteellisinä tutkimushankkeina. Kehitystä vaativan ongelman tai haasteen omistaja on kohdeorganisaation toimintaprosessit ja niiden johto.

### 4.3.3 Sosiaalisen systeemin analyysi

SSM on organisaation toiminnan kehittämiseen liittyvä tutkimuksellinen lähestymistapa. Kehittämistoimenpiteiden tulee olla helposti hyväksyttäviä ja lisäksi organisaatiokulttuurin kannalta toteuttamiskelpoista. Sosiaalisessa systeemissä asiaan vaikuttavat organisaation historia, tapa toimia ja toiminnan näkökulma. (Checkland & Poulter, 2006, 31–34)

Tutkimusalueen sosiaalinen systeemi muodostuu toimijoiden roolien, toiminnan normien ja arvojen välisestä vuorovaikutuksesta. Kriittisen infrastruktuurin organisaatiolla on omat tärkeä roolinsa koko alueen palvelujen toteuttamisessa. Roolit on mainittu kriittisen infrastruktuurin kuvauksessa. Tämän lisäksi organisaatiossa on myös niiden sisäiset omat roolinsa, jotka kuvaavat kunkin organisaation toimintakulttuuria. Normit eli standardit määrittävät yhteisiä toimintatapoja. Organisaatiot voivat soveltaa niitä yleensä parhaiten katsomallaan tavalla, mutta tutkimusalueelta löytyy myös velvoittavia normeja, kuten NIS-direktiivi. Organisaatiokohtaiset perusnormit määrittävät yleensä johtamista ja ohjaavat tehtävien suorittamista. Näitä ovat muun muassa organisaation työjärjestys, johtamis- tai toimintajärjestelmä sekä henkilöstön tehtävänkuvaukset. Kyberturvallisuuden normistoa voidaan käyttää apuna edellä mainituissa normeissa tai muussa toiminnan ohjaamisessa ja henkilöstön koulutuksessa. Niiden avulla voidaan myös edistää yhteisen käsityksen muodostamista organisaatioiden välisen toiminnan avuksi. Organisaation arvo ovat yleensä julistettu kohteen toiminnasta kertovassa tiedotteessa. Pohjimmiltaan ne ovat kuitenkin subjektiivisena käsityksiä tavoiteltavasta tai haluttavasta asiasta. Ne ovat siten myös henkilökohtaisia käsityksiä asioista. Koko tutkimusalueen osalta arvokkaim-

maksi arvoksi erottuu luottamus. Sillä on keskeinen merkitys kyberturvallisuudessa ja sitä kautta niin kriittisen infrastruktuurin palvelujen saatavuudessa kuin niiden tuottamisessakin eri organisaatioissa.

### 4.3.4 Poliittisen systeemin analyysi

Organisaatiot pitävät sisällään eri osapuolten väleillä valtapeliä, joka voi heijastua sen suorituskykyyn. Toimintaan voidaan vaikuttaa huomioimalla valtapeli, hallitsemalla sen vaikutuksia ja siihen sitoutunutta energiaa. (Checkland & Poulter, 2006, 35–37)

Poliittinen systeemi muodostuu organisaation eri toimijoiden intressien, valtasuhteiden ja toimintaprosessien hallinnan vuorovaikutuksessa. Se voi ilmetä erityisesti operatiivisessa tasolla organisaatioiden sisäisten toimintaprosessien (liiketoimintaprosessien) väleillä tai taktisella ja teknillisellä tasolla toteutettavissa toiminnoissa. Kysymys on siis organisaatiossa eri päätöksentekotasoilla ilmenevässä vallasta ja sen käytöstä. Systeemiajatuksen mukaan kaikilla toimijoilla on jonkinlainen suhde systeemissä toimimiseen. Organisaation kyberturvallisuuden kehittämisen osalta on tunnistettava valtaa käyttävät toimijat. Organisaation ylimmän johdon tuki kehittämistoimenpiteille on ensiarvoisen tärkeää, sillä operatiivisessa päätöksentekotasolla ja taktisella päätöksentekotasolla on haasteellista saavuttaa muutoin yhteisiä tavoitteita kehittämistoimenpiteille. Lisäksi ylimmän johdon tuki mahdollistaa tarvittavien resurssien ohjaamisen toimenpiteiden toteutukseen.

Kriittisen infrastruktuurin kyberturvallisuuden kehittämisessä on myös organisaatioita laajemmassa mielessä poliittisia systeemejä. Ne muodostuvat toimintaa tukevista ja ohjaavista tahoista. Toimenpiteillä on merkittävä rooli koko tutkimusalueen toiminnan kehittämisessä. Tätä aluetta tutkimuksessa on sivuttu kansallisista kyberturvallisuutta käsitelleistä tutkimushankkeista saatujen tietojen perusteella. Esille nousevat NIS-direktiivin toimenpiteistä vastaavat ministeriöt, Kyberturvallisuuskeskus ja kansallisesta huoltovarmuudesta vastaava Huoltovarmuuskeskus.

### 4.3.5 CATWOE-analyysi

Systeemin tarkempaan määrittelemiseen ja kuvaamiseen lukeutuu ydinmääritelmä (Root Definition). Ydinmääritelmä koostuu systeemin osatekijöistä. CATWOE-prosessi tarkoittaa systeemin jakamista osatekijöihin. (Checkland & Poulter, 2006, 38–43)

CATWOE tulee oheisista sanoista ja niiden merkityksestä kehittämisprosessissa: (Checkland & Scholes 1999, 35)

- Customer (asiakas: on prosessin tuotoksen vastaanottaja ja siten taho, jonka toimintaan prosessi vaikuttaa)
- Actors (toimijat: ovat osa prosessin toimintaa)
- Transformation process (muutosprosessi: ketju toiminoja, jotka saavat prosessiin tulevan syötteen muuttumaan tuotokseksi)

- World view (maailmankuva: näkökulma, joka ohjaa kehittämisprosessin toteutusta)
- Owners (omistajat: ovat prosessin toiminnasta, tuloksesta ja kehittämisestä vastuussa olevat toimijatahot)
- Environmental constraints (toimintaympäristön rajaus: prosessin ulkoiset ja sisäiset rajoitukset)

Seuraavissa kappaleissa kuvataan CATWOE:n avulla väitöstutkimuksen kehittämisprosessiin liittyvät osatekijät, joilla on keskeinen vaikutus koko systeemiin ja sen kehittämisen toteutukseen.

**Asiakas** (Customer):
Kriittisen infrastruktuurin organisaation asiakkuus voidaan jakaa pääasiallisesti kahteen ulkoiseen haaraan, jotka ovat palveluja tai tuotteita hyödyntävät kansalaiset ja toisaalta koko yhteiskunta kokonaisturvallisuuden näkökulmasta ajateltuna. Organisaation sisällä vaikuttavien ydin- ja tukiprosessien väleillä on myös asiakkuuksia, jotka mahdollistavat koko organisaation toiminnan. Organisaation verkottuneeseen toimintaan liittyy myös asiakkuutta verkoston sidosryhmien väleillä.

**Toimijat** (Actors):
Organisaation kyberturvallisuuden kehittämisen toimijat ovat johtajia ja esimiehiä, jotka saavat aikaan eri päätöksentekotasoilla tapahtuvat päätöksentekoprosessit. Toimijoihin lukeutuvat myös organisaatioiden koko henkilöstö. Lisäksi organisaation kyberturvallisuuden kehittämisen kannalta tärkeitä toimijoita ovat tutkimusorganisaatiot, joiden tutkimuspanoksia tarvitaan kehittämisratkaisuja valmisteltaessa, kehitettäessä ja valittaessa.

**Muutosprosessi** (Transformation process):
Kehitys- tai muutosprosessia voidaan yksinkertaisesti kuvata muutoskohteena olevaan prosessiin tulevan syötteen ja prosessin ulostulosta eli tuotoksesta saatavan suoritteen välisellä toiminnalla. Organisaatiossa kyberturvallisuuden jatkuvasti kasvavat vaatimukset ovat yleisellä tasolla prosessin syötteitä ja niihin vastaavat kehitystoimenpiteet muodostavat muutosprosessin, josta on tavoitteena suoritteet eli organisaation aiempaa parempi kyky tunnistaa kyberturvallisuuden uhkia, vastata niihin ja tarvittaessa sietää häiriötilannetta turvaamalla toimintaprosessien jatkuvuuden hallintaa. Muutosprosessin syötteinä voivat toimia myös organisaation ulkopuolelta tulevat tekijät, kuten kyberturvallisuusalan ohjaus kansallisten tai kansainvälisten suorituskykyvaatimusten täyttämiskeksi. Muita syötteitä voivat olla muun muassa teknillisten ICT-järjestelmien tai -laitteiden vanheneminen tai niiden käyttötavasta johtuvat muutostarpeet.

**Näkökulma** (World View):
Globaalin kybertoimintaympäristön muuttuminen uhkakuvineen edellyttää organisaatioilta oman toimintaympäristönsä tilannetietoisuuden ylläpitämistä. Kehittyvä organisaatio tunnistaa toiminnan jatkuvan parantamisen periaatteet. Organisaation toiminnan jatkuvan parantamisen johtamiseen voidaan liittää strateginen-, operatiivinen- tai taktinen näkökulma. Taktisen näkökulman prosesseihin liittyvät myös teknilliset ICT-järjestelmät, -laitteet, tiedonsiirtoverkot ja data.

Organisaation kybertuvallisuuden osalta taktiseen näkökulmaan liittyy siis myös teknillinen näkökulma. Väitöstutkimuksessa on käytetty tästä taktisen tason johtamisen ja teknillisen kokonaisuuden yhdistelmästä teknillistä/taktista käsitettä. Näkökulmat muodostavat organisaation vallankäyttötasot ja siten ratkaisevat kehitystoimenpiteiden suorittamisen mahdollisuudet. Organisaatioon liittyvien eri vallankäyttötasoille voi syntyä erilaisia näkökulmia ja odotuksia kehittämisen perusteista, toimintaan sitoutuvista resursseista, menetelmistä ja aikatauluista. Tilanteeseen voi liittyä kitkaa kehitystyön linjauksista ja toimenpiteistä päätettäessä. Tämän vuoksi väitöstyössä esitetään eräs yleisesti organisaatioiden kehitystoimintaan käytetty menettelymalli näkökulmien yhteiseksi pohjaksi. Kehitystoimenpiteiden toteutukseen voivat osallistua asiantuntijoina alan yliopistot, korkeakoulut ja tutkimuslaitokset, jotka tuovat tällöin omat näkökulmansa siihen. Kehittämismahdollisuuksia voidaan myös tarkastella teknologisesta näkökulmasta. Tästä lähtökohdasta käsin väitöstyössä on esitetty uusien tekniikoiden näkökulmia kyberturvallisuuden kehittämiseen. Kriittisen infrastruktuurin ohjaustahot muodostavat kansallisen kokonaisturvallisuuden ja EU-tason näkökulmat. Näihin näkökulmiin kytkeytyy kansallinen huoltovarmuus.

**Omistajat** (Owners):
Organisaation kyberturvallisuuden kehittämiseen liittyvien ongelmien omistajat sisältyvät strategiselle, operatiiviselle tai teknilliselle/taktiselle päätöksentekotasolle. Ensisijaiset omistajat ovat näiden päätöksentekotasoilla olevia johtajia ja esimiehiä. He voivat vaikuttaa muutoksen toteutukseen eniten. Myös organisaation henkilöstö kuuluu ongelman omistajiin. Henkilöstön kyberturvallisuuden kyvykkyys ratkaisee lopulta toimenpiteiden onnistumisen. Henkilöstön kyvykkyys on myös ratkaisevassa asemassa ongelmiin liittyvän tilannetietoisuuden rakentumisessa. Ongelman omistajina voivat ratkaisijan roolissa olla myös organisaation ulkopuoliset sidostyhmät. Näitä ovat toimintaverkoston kumppanit ja esimerkiksi käytössä oleva koulutus- ja tutkimusorganisaatiot tai tutkimushankkeita edistävät tahot. Kriittisen infrastruktuurin toimivuuteen liittyvät ohjaustahot voivat myös näkyä ongelman omistajina kansallisesta kokonaisturvallisuuden näkökulmasta tarkasteltuna.

**Toimintaympäristö** (Environment):
Organisaation ulkoinen kybertoimintaympäristö on jatkuvassa muutostilassa. Digitalisaatio tuo uusia ulottuvuuksia siihen muun muassa teknologian kehityksen myötä. Käynnissä on digitalisaation aikaansaamana muun muassa Teollisuus 4.0 kutsuttu kehitys, joka lisää erityisesti verkottuneiden laitteiden määrää toimintaympäristössä, muodostaa niistä uusia teknillisiä kokonaisuuksia ja uusia palveluja. Kaikki organisaatiot kohtaavat väistämättä ainakin jollakin aikavälillä tarpeet hyödyntää uusinta tekniikkaa ja sen mukanaan tuomia mahdollisuuksia. Väitöstyön taustatutkimuksien haastatteluissa on tullut myös esiin joidenkin organisaatioiden tarpeet laajentaa toimintaansa uusille liiketoiminta-alueille teknologian kehityksen vuoksi. Organisaatiolla ei kaikissa tilanteissa ole myöskään mahdollisuutta kehittää kyberturvallisuuttaan ja siihen liittyvää kyvykkyyttään täysin vapaasti ja vain omista lähtökohdistaan. Tässä mielessä erityisesti organi-

saation puolustuksellisten vastatoimien kyvykkyyden kehittäminen tulee toteuttaa harkitusti. Kehittämisen tulee aina perustua voimassa oleviin lakeihin ja asetuksiin. Myös hallinnonalankohtaiset normit ja ohjeet voivat asettaa vaatimuksia kehittämistoimenpiteisiin. Toimintaympäristössään organisaatio voi kohdata myös rajallisia resursseja niin teknologian kuin osaamisenkin osalta.

# 5 KRIITTISEN INFRASTRUKTUURIN ORGANISAATION KYBERTURVALLISUUS

Millaisia tekijöitä liittyy kriittisen infrastruktuurin organisaation kyberturvallisuuden muodostumiseen?

SSM-tutkimusprosessin vaiheen kaksi mukaista kriittisen infrastruktuurin organisaatioiden kyberturvallisuuden kokonaistilannetta on selvitetty tämän luvun alussa. Myöhemmin luvussa on organisaatioiden kyberturvallisuuden tilannetta syvennetty ja selvitetty kahden esimerkin kautta, jotka ovat energiasektorin sähköyhtiö (Tutkimuskohde 1) ja terveydenhuollon sairaala (Tutkimuskohde 2). Luvuissa on esimerkkiorganisaatioiden osalta laadittu myös SSM:n vaiheen neljä mukaisesti ydinmääritelmät tutkimuskohteiden tyypillisille tietoteknillisille järjestelmille ja niiden nykytilakuvaukset käsitteellisten kehittämistoimenpiteiden perustaksi. Luvussa 6 on kartoitettu tavoitetasolla organisaation kyberturvallisuuden kehittämisessä hyödynnettäviä menettelyjä. Tiedoista muodostuu SSM:n vaihe neljä. Luvussa 6 on myös esitetty kehittämistoimenpiteitä, joista muodostuu SSM-mallin kohta kuusi.

Organisaation globaali kybertoimintaympäristö on kehittynyt digitalisaation takia monikerroksiseksi informaatioverkostoksi, johon lukeutuvat niin julkisen hallinnon kuin yksityisen sektorin verkkoja ja teollisuusprosessien valvonta- ja ohjausjärjestelmiä. Internet kytkee ne maailmanlaajuiseksi verkostoksi. Verkottunut yhteiskunta on monimutkainen ja kompleksinen kokonaisuus, johonka kohdistuu uhkia, joihin on pystyttävä varautumaan entistä tehokkaammin. Hybridiuhkista ja kyberhyökkäyksistä on muodostunut osa kybertoimintaympäristöä ja sen haasteita, jolloin on mahdollista, että sisäinen turvallisuus heikkenee ja siten alentaa yhteiskunnan toimintakykyä ja kriisisietoisuutta.

Toisaalta digitaalinen tietoyhteiskunta on merkittävästi lisännyt yhteiskunnan hyvinvointia ja se on mahdollistanut uusien, ja mahdollistaa myös edelleen, tuotteiden ja palveluiden aikaansaamisen. Digitalisaation kehityksen myötä tavaroista ja palveluista tulee jatkuvasti älykkäämpiä. Yhdessä ne muodostavat toisiinsa liittyviä palvelualustoja teknologian avulla, jolloin organisaatiot voivat

luoda aiempaa syvällisempiä ja reaaliaikaisempia suhteita sidosryhmiinsä. Kehityksen kääntöpuolena on kasvanut riski erilaisista kybertoimintaympäristön uhkista. Toimintaympäristön kehitys vaikuttaa erityisesti Suomeen, joka on yksi kehittyneimmistä digitaalisista tietoyhteiskunnista. Erilaiset digitaaliset verkostot ja niiden palvelut ovat keskeinen osa yhteiskuntaa. Tietoteknisten laitteet ja järjestelmät muodostavat informaatioinfrastruktuurin, jonka toimintahäiriöistä voi aiheutua kielteisiä vaikutuksia koko yhteiskunnan toimintaan.

Edellä kuvattuun kehitykseen liittyen tässä väitöstutkimuksessa kansallisen kriittisen infrastruktuurin organisaatioiden kyberturvallisuuden nykytilan kuvausta on selvitetty pääosin kolmessa eri kansallisessa tutkimushankkeessa. Energiasektorin sähköyhtiöiden nykytilan tutkiminen toteutettiin CyberTrust-tukimushakkeessa, sen työpaketissa, joka käsitti kriittisen infrastruktuurin resiliensiä ja suojaamisesta (Critical Infrastructure Resiliency and Protection, CIRP) sekä tutkimushankkeessa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”. Terveydenhuoltoon liittyvän sairaalan nykytilan tutkimus toteutettiin Watson Health Cloud Finland tutkimushankkeessa. Nykytilakuvauksilla on pyritty saamaan kokonaiskuva kriittisen infrastruktuurin kyberturvallisuustilanteesta tarkoituksenmukaisten kehitystoimenpiteiden aikaansaamiseksi koko alueen organisaatioiden käyttöön.

## 5.1 Tutkimuskohde 1; sähköyhtiö

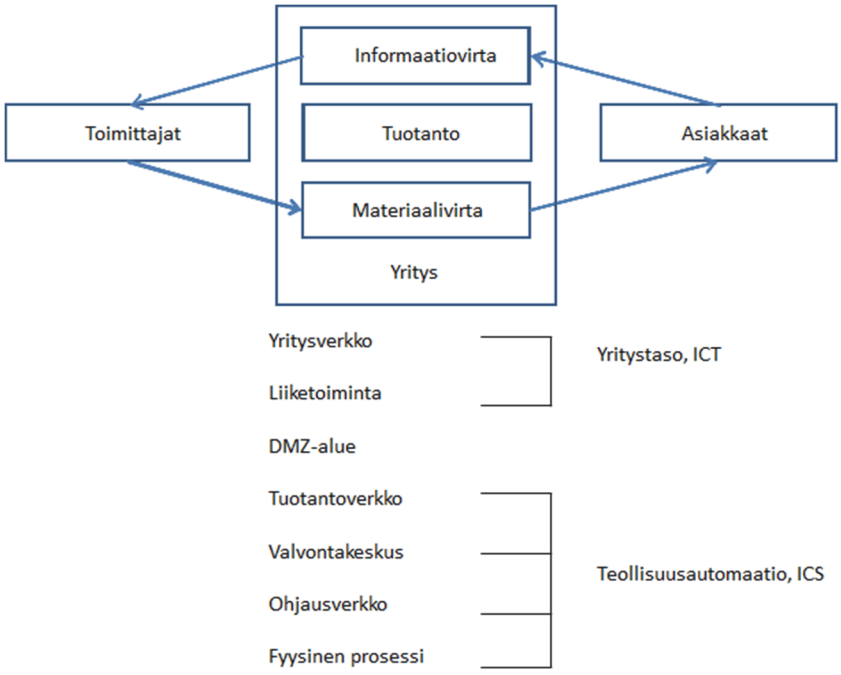
P1. Pöyhönen, J., Lehto, M. (2017). Cyber security creation as part of the management of an energy company. ECCWS 2017: Proceedings of the 16th European Conference on Cyber Warfare and Security (pp. 332-340). Published by Academic Conferences and Publishing International Limited. Reading. UK

RR2. Pöyhönen J. (2018). Cyber security in the management of an electricity company. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 56/2018.

RR3. Pöyhönen J. (2018). Kyberturvallisuuden hallintajärjestelmän luominen energiayhtiön lämpövoimalaitokseen. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 57/2018.

### 5.1.1 Teollisuusautomaatiojärjestelmät

Sähköyhtiön toimintaan liittyviä yleisiä verkostoja ja prosesseja voidaan havainnollistaa logistisella viitekehyksellä, joka pitää sisällään toimittajaverkoston, tuotantoprosessin, asiakasverkoston ja näitä yhdistävät informaatio- ja materiaalivirrat. ICT-prosessit lukeutuvat yrityksen infrastruktuuriin ja muodostavat siten merkittävän osan yrityksen ydinprosesseja tukevista toiminnoista. Yritystason ICT-prosessit liittyvät hallintoon ja verkoston informaatio- ja materiaalivirtojen hallintaa. Tuotantotasolla puolestaan ovat tuotannon automaatiojärjestelmät eli ICS-järjestelmät (Industrial Control System). Kuviossa 9 on esitetty yrityksen logistisen viitekehyksen rakenne ja yrityksen yleiset ICT-prosessit (Bowersox, ym.,1986 (muokattu); Knowlesa, ym., 2015).




KUVIO 9 Sähköyhtiön logistiikan viitekehys ja yleiset ICT- ja teollisuusautomaatiojärjestemät.

Teollisuusautomaatio-organisaation ICT-prosessien hierarkian ylimmillä tasoilla ovat hallinnon yleiset tietojärjestelmät ja toiminnanohjausjärjestelmä eli ERP-järjestelmä (Enterprise Resource Planning, ERP). Tyypillinen ERP-järjestelmä sisältää ylätasolla kokonaisprosessin ohjauksen muun muassa ohjaamalla tuotantovolyymiä sekä hoitaa raaka-aine täydennyksiä, varastointia, jakelutoimintoja, maksuliikennettä ja henkilöstöresursseja. ERP-ohjelmistojen ja valvomojen välissä voi tarvittaessa sijaita tuotannonohjausjärjestelmä eli MES-järjestelmä (Manufacturing Execution System, MES), joka mahdollistaa valvomosta saatavan tiedon välittämisen ERP-järjestelmään.

Tuotannon automaatiojärjestelmät puolestaan jakaantuvat omiin hierarkiakerroksiin, joista ylimpänä on valvomo, josta koko prosessin toiminta esitetään graafisessa muodossa ja hälytyksinä valvojille. Tiedon perusteella käsitellään prosessihälytykset sekä valvotaan ja ohjataan prosessin toimintaa. Seuraavan kerroksen muodostavat prosessiasemat, joissa ovat prosessin ohjaus-, mittaus- ja säätötoimenpiteitä suorittavat laitteet. Samalle kerrokselle kuuluvat myös laitteiden vika- ja häiriövalvontatoiminnot. Alin kerros muodostuu kenttälaitteista, joilla prosessin toimilaitteita ohjataan ja valvotaan sekä kerätään mittauslaitteista mittaustietoa.

Suomen Automaatioseura luokittelee teollisuusautomaatiojärjestelmät niiden ohjausjärjestelmien ja verkkorakenteen perusteella karkeasti seuraaviin ryhmiin: (Suomen Automaatioseura ry., 2010, 53)

> "Hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS)."

> "SCADA-käytönvalvontajärjestelmät (Supervisory Control and Data Acquisition Systems, SCADA)."

”Ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC).”

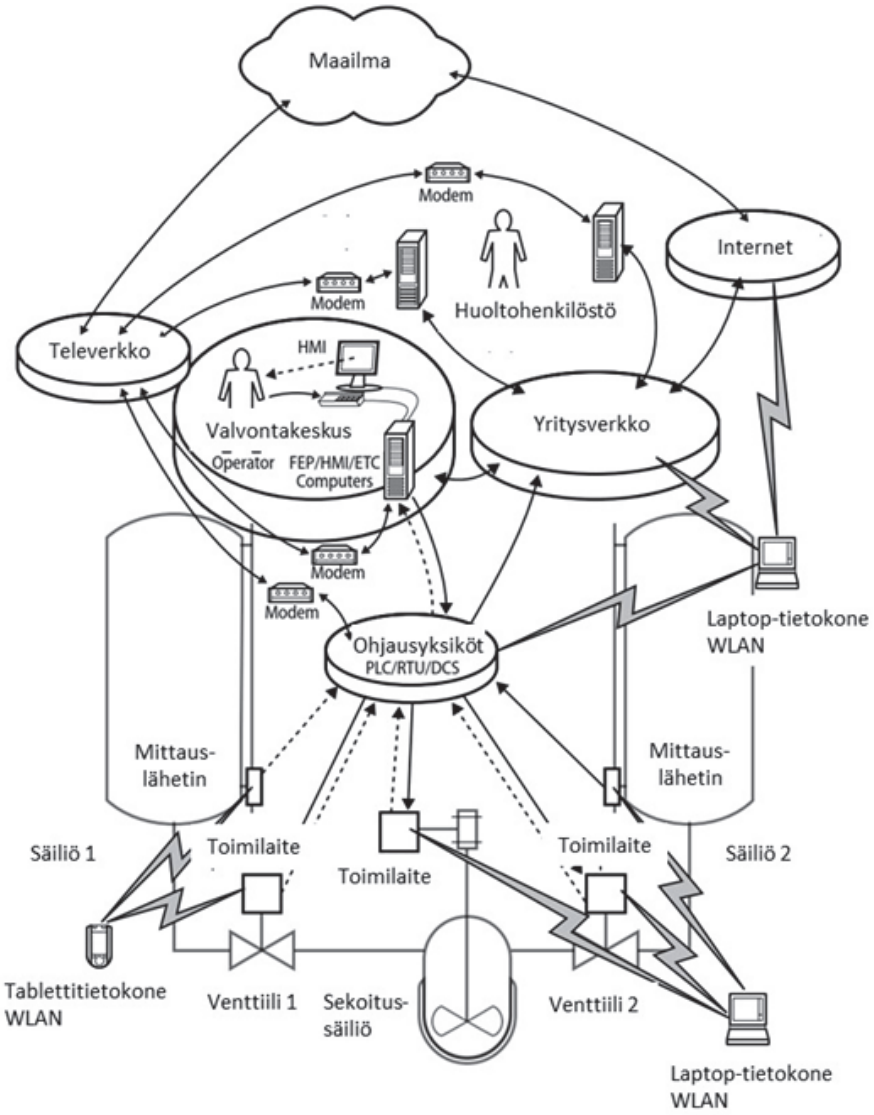
Hajautettuja järjestelmiä (DCS) käytetään ohjaamaan ja suojaamaan laajoja ja monimutkaisia prosesseja, kuten voimalaitoksia, kemianlaitoksia ja öljynjalostuslaitoksia sekä terästeollisuuden, elintarvikealan, panimoalan, lääketeollisuuden, sellu- ja paperiteollisuuden, metalliteollisuuden ja kaivosten laitoksia, jotka sijaitsevat tavallisesti yhdellä alueella. Hajautettu ohjausjärjestelmä käsittää prosessitason ohjaustoimet ja yhden tai useampia hajautettuja ohjausyksiköitä samassa tehdaslaitoksessa. Prosessin valvontayksikkö toimii ohjauspalvelimessa ja kommunikoi sen ala-asemissa oman erillisen aliverkon kautta. Ohjausyksikkö antaa prosessille asetusarvoja ja hankkii mittaustietoja hajautetuilta ohjausyksiköiltä. Hajautetut ohjausyksiköt ohjaavat ja suojaavat tuotantoprosessien toimintoja ohjausyksikön antamien käskyjen mukaisesti käyttämällä mittausanturien palautetieoja ja säätämällä tuotantoprosessiin sijoitettuja toimilaitteita. (Suomen Automaatioseura ry., 2010, 53)

SCADA-tyyppisiä järjestelmiä käytetään pääasiassa maantieteellisesti hajautettujen järjestelmien ohjaukseen, joista hankitaan keskitetysti tietoja eri yksiköistä ohjaustoimintoja varten. Tyypillisiä tällaisia hajautettuja toimintoja ovat infrastruktuurijärjestelmät, kuten energianjakeluverkot, kaasulinjat, vesijärjestelmät, jätevesijärjestelmät sekä muut vastaavat yleiset verkot ja teollisuusverkot. SCADA-järjestelmien tehtävänä on alajärjestelmien etäohjaus, mikä tapahtuu tavallisesti automaattisesti. Yritysten liiketoimintojen optimointia varten niistä voi olla pääsy tehtaan tietojärjestelmiin Internet-verkon kautta ja joskus myös laajan lähiverkon (Wide Area Network, WAN) kautta. Teollisuuslaitoksissa varsinainen prosessin ohjausjärjestelmä on yleensä erotetussa Internet-verkosta. Prosessitoimintoja voidaan kuitenkin ohjata huoltopalvelujen vuoksi paikallisverkon (Local Area Network, LAN) kautta. SCADA-tyyppisiin järjestelmiin kuuluvat keskusvalvontayksikkö (Central Monitoring System, CMS) sekä yksi tai useampia etäasemia (Remote Terminal Unit, RTU). Keskitetty ohjausjärjestelmä kerää ja tekee lokit tiedoista, joita saadaan etäasemista, ja tuottaa tarvittavat ohjaustoimenpiteet etäasemien tekemien havaintojen ja mittaustietojen perusteella. Etäasemaan kuuluu joko säätöasema ohjaus- ja toimilaitteineen tai ohjelmoitava logiikkayksikkö, joka ohjaa toimilaitteita ja valvoo antureita. (Suomen Automaatioseura ry., 2010, 54-56)

Ohjelmoitavia logiikoita (PLC) käytetään yleisemmin ohjaamaan erillisiä prosesseja, SCADA-järjestelmien alajärjestelmiä tai erillisiä turvatoimintoja. Prosessin ohjauksessa tyypillisiä esimerkkejä löytyy kappaletavarateollisuuden valmistusjärjestelmistä. Turvatoimintojen esimerkkejä löytyy koneautomaatiosta, joissa turvatoimintoja tarvitaan tyypillisesti jatkuvatoimisesti. (Suomen Automaatioseura ry., 2010, 56)

Yhdysvaltojen Air Force Research Institute on julkaissut tutkimuksen, jossa tarkastellaan liittovaltion pyrkimyksiä yhteistyöhön julkisen ja yksityisen sektorin kanssa puolustautuakseen kyberhyökkäyksiltä teollisuuden automaatiojärjestelmiin (ICS) ja valvonta- ja tiedonhankintajärjestelmiin (SCADA). Tutkimus käsittelee näiden järjestelmien merkitystä osana kansallista kriittistä infrastruktuuria. (Weed, 2019)

Kuviossa 10 on edellä mainitussa tutkimuksessa määritetty organisaation teollisuusautomaatiojärjestelmän perusrakenne. Kuviosta ilmenevät henkilöstöroolit, pelkistetty prosessikaavio, prosessin ohjaus-, säätö- ja valvontajärjestelmät laitteineen sekä tiedonsiirtoverkot rakenteen sisällä ja sieltä ulos. (Weed, 2019, 5)




KUVIO 10 Teollisuusautomaatiojärjestelmän perusrakenne.

Väitöstutkimuksen viitekehyksen kognitiiviselle kierrokselle kuviossa kohdistuvat käyttö-, valvonta- ja huoltohenkilöstön toimenpiteet. Kohteen palvelukerros pitää sisällään Internet-verkon kautta saatavat palvelut. Syntaktinen kerros pitää sisällään valvontaohjelmistoja ja tietovarantoja (SCADA). Semanttinen kerros sisältää tuotantoprosessin ohjauksen ohjelmistoja, tiedonsiirto-ohjelmistoja ja sanomarakenteita. Fyysisellä kerroksella ovat prosessin tiedonsiirtoverkkojen laitteet, valvonta- ja ohjauslaitteet ja toimilaitteet.

Arvioitaessa teollisuusautomaatiojärjestelmien sijoittumista kybermaailmaan ja niiden kyberturvallisuuteen vaikuttavia seikkoja, on ensiarvoisen tärkeää

tiedostaa järjestelmien keskeisimmät ominaisuudet. Esimerkiksi tuotantoprosessien ohjaamisessa käytössä olevia hajautettuja automaatiojärjestelmiä voidaan luonnehtia siten, että ne ovat toiminnaltaan hyvin vakiintuneita ja niiden elinkaaret ovat pitkiä verrattuna yrityksen muihin ICT-järjestelmiin. Automaatiojärjestelmien elinkaaret voivat olla perusjärjestelmän osalta jopa useiden vuosikymmenien mittaisia. Lisäksi perusjärjestelmien rakennetta muutetaan harvoin. Muutokset toteutetaan lähinnä suurempien kunnossapito- tai muutostöiden yhteydessä järjestelmien elinkaaripäivityksinä. Automaatiojärjestelmät ovat myös resursseiltaan rajoittuneita, jolloin niissä ei ole voitu käyttää tyypillisiä teknillisiä tietoturvaratkaisuja eikä salaustekniikoita Niiden käyttöorganisaatiot ovat hyvin koulutettuja tehtäviinsä ja tuntevat siten laitteet, laitteiden toimintaperiaatteet ja niiden toimintaympäristöt. Automaatiojärjestelmien tietovarastot sisältävät pääosin tuotantoprosessin tietoja eikä niinkään liiketoimintaprosessin tietoja. Suoraa yhteyttä Internet-verkkoon ei aina tarvita eikä tuotantoprosessin tietoteknisiä laitteita käytetä muihin tarkoituksiin. Ne ovat hajautettuina valmistusprosessiin, sen valvonta-, mittaus- ja ohjaustehtäviin sekä turvatoimintoihin. Järjestelmiin tapahtuva pääsyn hallinta on useimmiten tarkasti järjestetty. Automaatiojärjestelmien toimintojen ja henkilöstön valvonta on hallittua muun muassa prosessin toiminnan käytettävyys- ja turvallisuusvaatimusten takia. (Suomen Automaatioseura ry., 2010)

### 5.1.2 Sähköyhtiön kyberturvallisuuden merkitys

Modernin yhteiskunnan toiminnan kriittisten infrastruktuurien eri osien yhteistoiminta ja palvelut riippuvat peruslähtökohdiltaan luotettavasta kansallisesta sähköjärjestelmästä. Tämän lisäksi luotettavuus muodostuu siinä toimivien organisaatioiden toimintatavoista, niiden välisistä toimivista tiedonsiirtoverkostoista sekä palvelutason järjestelmien tiedon käytettävyydestä, luotettavuudesta ja eheydestä kybertoimintaympäristössä.

Fingrid Oyj on kansallinen julkinen osakeyhtiö, jonka tehtävänä on vastata sähkön siirrosta Suomen kantaverkossa. Fingrid Oyj on määritellyt Suomen sähköjärjestelmän seuraavasti: (Fingrid Oyj., 2020)

> "Sähköjärjestelmä koostuu voimalaitoksista, kantaverkosta, suurjännitteisistä jakeluverkoista, jakeluverkoista sekä sähkön kuluttajista. Kansallinen järjestelmämme on osa yhteispohjoismaista sähköjärjestelmää yhdessä Ruotsin, Norjan ja Itä-Tanskan järjestelmien kanssa. Sitä täydentävät tasasähköyhteydet Venäjältä ja Virosta, joilla pohjoismainen järjestelmä on yhdistetty Venäjän ja Baltian voimajärjestelmään."

Sähköä tuotetaan Suomen voimalaitoksissa monipuolisesti usealla eri energianlähteellä ja tuotantomuodolla. Tärkeimmät sähkön tuotannon energialähteet ovat ydinvoima, vesivoima, kivihiili, maakaasu, biomassa, tuulivoima sekä turve. Energialähteiden lisäksi jaottelu voidaan suorittaa myös sähkön tuotantomuodon mukaan. Suomessa on noin 120 sähköä tuottavaa yritystä ja noin 400 voimalaitosta, joista yli puolet on vesivoimalaitoksia. Sähköstä lähes kolmannes tuotetaan yhteistuotantona lämmöntuotannon yhteydessä. Sähköntuotantomme on siten varsin hajautettua. Sähkön tuotannon monipuolisuus ja hajautettu tuotantorakenne lisäävät sähkön kansallista toimitusvarmuutta. (Energiateollisuus, 2019)

Sähköjärjestelmän kansallinen merkitys on hyvin samankaltainen valtiosta riippumatta. Vertailukohtana ja esimerkkinä tästä yhteydessä voidaan käyttää sähköjärjestelmää Yhdysvalloissa. Myös siellä sitä pidetään kriittisenä infrastruktuurina ja avainresurssina koko yhteiskunnan toimivuuden näkökulmasta katsottuna. Sen osat ovat perusrakenteiltaan samanlaiset kuin Suomen sähköjärjestelmän osat, mutta Yhdysvalloissa verkon kuormituksen tasehallinta poikkeaa sekä rakenteelliselta että teknilliseltä toteutukseltaan merkittävästi Suomen vastaavasta järjestelytä. Yhdysvalloissa nähdään, että sähköverkko edustaa teknillisesti huippuunsa vietyä järjestelmäkokonaisuutta, jonka ratkaisut edellyttävät vaativuusasteeltaan jopa kaikista edistyneimpiä tekniikoiden käyttöä. Kyberturvallisuustarkastelussa verkon tekniikka ja ohjausjärjestelyt muodostavat merkittävimmät tarkastelualueet. (Lewis, 2015)

Sähköjärjestelmän kriittisyys ilmenee Huoltovarmuuskeskuksen toimitusjohtajan pitämästä esitelmästä sähkön käyttövarmuuspäivillä otsikolla ”Sähköjärjestelmä yhteiskunnan toimivuuden perustana”. Oheinen taulukko 7 on ote esitelmästä (Kananen, 2013). Se kuvaa sähkökatkoksen vaikutuksia yhteiskunnan toimintoihin katkoksen pituuden funktiona. Kyberturvallisuuden vaarantuminen on ollut tarkastelussa yhtenä kaikista merkittävimpänä uhkana energiahuollon ja energiaverkkojen toiminnan osalta. (Kananen, 2013)

TAULUKKO 7 Sähkökatkoksen vaikutuksia yhteiskunnan toimintoihin.

| **Keskeytysaika** | **Vaikutus** |
|---|---|
| 1 sekunti | Teollisuuden herkkiä prosesseja voi pysähtyä. Tietojärjestelmien tietoja voi kadota. |
| 1 minuutti | Teollisuuden ja sairaaloiden prosesseja pysähtyy. |
| 15 minuuttia | Kauppojen toiminta keskeytyy. Katkos voi haitata ihmisten jokapäiväistä toimintaa. Liikenteessä tapahtuu viivästymisiä. |
| 2 - 3 tuntia | Teollisuusprosesseille voi syntyä mittavia vahinkoja. Matkapuhelinliikenteen toimivuudessa on ongelmia. Kotieläintuotannossa on häiriöitä. |
| 12 - 24 tuntia | Veden tulo koteihin ja toimistoihin lakkaa. Rakennukset alkavat jäähtyä pakkasilla. Pakasteet alkavat sulaa. |
| Useita vuorokausia | Yhteiskunnan toiminta häiriintyy vakavasti. Teollisuus ja palvelut eivät toimi. Työpaikat ja koulut suljetaan. Rakennuksiin muodostuu jäätymisvaurioita. |

### 5.1.3 Sähköyhtiön kyberturvallisuuden uhkatekijät

ICT- ja teollisuusautomaatiojärjestelmät ovat osa yleistä kybermaailmaa, jonka päällimmäiset riskit liittyvät rahan, sensitiivisen tiedon ja maineen menettämiseen sekä liiketoiminnan estymiseen. Turvallisuusratkaisut muodostavat tällöin riskien hallinnan keskeisimmät tekijät. Riskien taustalla olevia haavoittuvuuksia voidaan puolestaan arvioida teknologian puutteena suhteessa hyökkäysteknologiaan, puutteina henkilöstön osaamisissa tai toimintatavoissa, puutteina organisaation johtamisessa sekä puutteina toimintaprosesseissa tai niiden tekniikoissa. Haitantekijöiden yleisimmät motiivit liittyvät tuhovaikutusten aikaansaamiseen prosesseissa, prosessihaavoittuvuuksien tiedusteluun, anarkismiin tai egoismiin. Toimijat voi olla jopa valtiollisia toimijoita tai ehkä yleisimmin järjestäytyneitä aktivisteja tai hakkereita tai sitten yksittäisiä itsenäisiä toimijoita. (Lehto, 2015)

Haitalliset toimenpiteet voivat kohdistua organisaation järjestelmiin henkilöstöä hyväksi käyttäen haittaohjelmien saattamiseksi järjestelmiin tai kybervakoiluna (tietoverkkovakoiluna). Ne voivat myös kohdistua langattomien yhteyksien tai Internet-yhteyksien kautta tapahtuvina tunkeutumisina tai verkkohyökkäyksinä järjestelmiä kohtaan. Haitantekijöiden tavoitteet voivat liittyä verkon palvelujen estämiseen, koko toiminnan lamauttamiseen, tietovarkauksiin tai niiden vääristämiseen tai vakoiluohjelmien perille saattamiseen. Myös niin sanotuilla takaporteilla saastutetut komponentit tai komponenttien tarkoituksellinen ohjelmointi hyökkääjän tarpeisiin ovat yhä enemmän esillä tämän päivän kybermaailmassa. (Lehto, 2015)

Yhdysvalloissa sähköjärjestelmään kohdistuvat turvallisuusuhat liittyvät voimalaitosten logistiikkaan häiritsemällä ja vahingoittamalla raaka-ainetoimitusten toimitusreittejä, siirto ja jakeluverkkojen tai niiden välisten muuntamo- ja kytkinasemien vahingoittamiseen fyysisellä vaikutuksella tai tekemällä kyberhyökkäyksiä sähköjärjestelmän ohjaus- ja säätöjärjestelmiin. (Lewis, 2015)

Sähköyhtiö ICT- ja teollisuusautomaatiojärjestelmät muodostavat monimutkaisen digitaalisen kokonaisuuden, jonka suojaustoimenpiteet edellyttävät kyberuhkien laaja-alaista analysointia ja niistä mahdollisesti aiheutuvien vaikutusten riskiarvioita koko teknologia-alueella. Suojausratkaisuja suunniteltaessa joudutaankin huomiota kohdistamaan sekä organisaatiotason ICT-järjestelmiin että teollisuusautomaatiojärjestelmiin ja lopulta myös niiden keskinäisten vaikutusten huomioimiseen. Tarvittavien toimenpiteiden kartoittaminen johtaa tarpeeseen systeemiajattelun kautta rakentuvien ratkaisujen etsintään, kyberuhkien perusteella laadittaviin riskiarviointeihin ja toimintaa varmistavaan valmiussuunnitteluun. Toimenpiteiden tavoitteena on varmistaa toimintaprosessien jatkuvuuden hallinta. Käytettävyyden merkitys on keskeinen liiketoiminnan tuloksen muodostuksen ja toiminnan luotettavuuden näkökulmista tarkasteltuna. Lisäksi prosessien sisältämien ja käyttämien tietojen luotettavuus ja sisällöllinen eheys ovat myös keskeisiä tavoitteita.

### 5.1.4 Sähköyhtiön kyberturvallisuuden nykytila

Alan organisaatioita koskevan nykytilakartoituksen haastatteluista on tehty taulukon 8 ja taulukon 9 mukaiset tiivistetyt yhteenvedot. Taulukoissa SWOT-analyysin tulokset ovat ryhmiteltyinä haastatteluteemojen mukaisesti.

TAULUKKO 8 SWOT-analyysi; vahvuudet ja heikkoudet.

| | **VAHVUUDET**<br>**Positiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** | **HEIKKOUDET**<br>**Negatiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** |
|---|---|---|
| SISÄISET | Johtaminen:<br>• kyberturvallisuus huomioitu strategisena tavoitteena, politiikka usein julkaistu<br>• riskiperusteinen johtaminen, osana kokonaisturvallisuutta ja liiketoimintaa<br>• toimenpiteitä priorisoitu<br><br>Tilannekuva:<br>• uhkakuvat usein toimintaverkostosta ja kumppaneilta suoraan<br>• Kyberturvallisuuskeskuksen tiedotteet<br><br>Henkilöstön osaaminen:<br>• ICT-henkilöstöllä hyvä<br>• muulle henkilöstölle e-learn-koulutusta<br>• osaamisen todentaminen<br><br>Tuotteet ja palvelut:<br>• parhaat tuotteet käytössä<br>• palveluissa hyvä osaaminen<br>• ulkoistettuna ostopalveluna<br>• osin hajautettu riskiperusteisesti<br>• työasemat usein omana palveluna<br>• sopivat ”tavanomaisiin” uhkiin<br>• puhtaat verkot<br><br>Sidosryhmät:<br>• ulkoistuksissa parhaat kumppanit<br>• toimialayhteistyö<br>• PPP-yhteistyö, mm. HVK<br>• kansainvälinen yhteistyö | Johtaminen:<br>• politiikan jalkautus läpi organisaation usein haastavaa<br>• haasteena vaativien uhkien tunnistaminen<br>• toiminta usein reaktiivista<br>• kyberturvallisuuden johtoryhmäedustus puuttuu<br><br>Tilannekuva:<br>• yleistilanne muodostettava hajallaan olevista tiedoista<br>• toimintaverkoston tilannekuvan muodostaminen vaikeaa<br>• teknillisen/taktisen tason reaaliaikaisen tilannekuvan luominen IT-varannoista ja teollisuusautomaatiosta (ICS) haastavaa<br><br>Henkilöstön osaaminen:<br>• koko henkilöstön kouluttaminen haastavaa isoissa organisaatioissa<br>• syvä osaaminen harvojen kansallisesti käsissä, laajat häiriöt haastavia hoitaa<br>• ICT/ICS-kokonaisuuden osaamishaaste<br><br>Tuotteet ja palvelut:<br>• kumppanuusverkoston toiminnan arviointi haastavaa<br>• puutteellinen näkymä palvelujen suojaukseen (mm. pilvipalvelut)<br>• kattavassa tunnistautumisessa kehitettävää |

| **VAHVUUDET**<br>**Positiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** | **HEIKKOUDET**<br>**Negatiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** |
|---|---|
| • usein hyvä maine sidosryhmien silmissä<br><br>Jatkuvuuden varmistaminen:<br><br>• harjoitustoimintaa, suunnitteluharjoituksia<br>• varautumissuunnitelmia laadittu<br><br>Asiantuntijapalvelut:<br><br>• erilaiset auditoinnit<br>• ongelmatilanteiden selvittäminen<br>• parhaat käytänteet<br>• kansalliset tutkimusohjelmat, osa yrityksistä mukana | Sidosryhmät:<br><br>• yrityksen liiketoiminnan ja kasallisen huoltovarmuuden välinen ristiriita (resursointi)<br><br>Asiantuntijapalvelut:<br><br>• auditoinnin kattavuus läpi koko toiminnan ja ohjelmistojen toimintaan/palveluun<br>• yritysten omaehtoista tutkimustoimintaa on vähennetty |

TAULUKKO 9 SWOT-analyysi; mahdollisuudet ja uhkat.

| | **MAHDOLLISUUDET**<br>**Lista mahdollisuuksista, jotka lisäävät kyberluottamusta** | **UHKAT**<br>**Lista uhkatekijöistä, jotka vaikuttavat kyberluottamukseen** |
|---|---|---|
| ULKOISET | Edistyksellisen tekniikan hankinta:<br><br>• mahdollisuus investoida uuteen tekniikkaan; erityisesti isot yritykset<br><br>Uudet yhteistyötahot:<br><br>• PPP-toiminnasta kilpailuetua<br>• yhtenäisen tilannekuvan muodostaminen<br><br>Uudet kehitysmahdollisuudet:<br><br>• kansallinen tiedustelulaki ja sen muodostama viranomaistuki<br>• nykyistä laajempi benchmarking-toiminta<br>• auditointitoiminnan kehittäminen | Toimintaympäristön analysointi:<br><br>• tuntemattomat uhkatekijät ja tietomurrot<br>• uudet liiketoimintamallit; edellyttävät uusien tekniikoiden käyttöönottoa (esim. IOT, robotiikka), joiden mukanaan tuomaa uhkakuvaa ei tunneta riittävästi<br><br>Kyberuhkien analysointi:<br><br>• haasteena teollisuusvakoilu ja valtiollisten toimijoiden kyvykkyys<br>• terrorismi; kyberfyysinen vaikuttaminen sähköverkkoon<br>• henkilöstöriskit<br>• avainhenkilöstöön kohdistuvat uhat<br><br>Toimintaverkoston analysointi:<br><br>• ei riittävää näkymää toimintaverkostoon ja sen riippuvuussuhteisiin<br>• osaamisen katoaminen ulkoistetuissa palveluissa; ylikansallinen yhtiö, saneeraukset taloudellisista syistä, joista seuraa osaamisen katoaminen |

#### 5.1.4.1 Yleistä tuloksista

Tutkimuskohteissa yleisten haittaohjelmien aiheuttamien uhkien osalta suojaustoimenpiteet ovat hallinnollisesti ja teknillisesti koko tutkimusalueella kohtalaisen hyvällä tasolla. Sähköjärjestelmän teollisuusautomaation toimintaa valvotaan jatkuvalla seurannalla ja tiedonsiirtoverkkojen puhtauteen luotetaan. Näiltä osin myös teknilliset suojaustoimenpiteet ovat hyvällä tasolla. Yleisesti tunnistetaan, että kansallinen sähköjärjestelmä toimii perustana koko kriittiselle infrastruktuurille ja sen palveluille.

Tutkimuskohteiden kyberturvallisuuden erityisosaaminen on hyvällä tasolla. Organisaatiot ovat ulkoistaneet ICT-toimintojaan hyödyntääkseen parhaita saatavilla olevia tuotteita ja palveluja sekä varmistaakseen niiden käytettävyyden. Tutkimuksessa tuli esille, että kansallista ja kansainvälistä yhteistoimintaa kybertuvallisuuden tilannetietoisuuden muodostamisessa pidetään ehdottomana edellytyksenä ennakoivalle toiminnalle. Suomea pidetään edelläkävijänä viranomaisten ja yritysten välisessä yhteistoiminnassa (Public, Private, Partnership, PPP-toiminta). Se parantaa merkittävästi tilannetietoisuutta ja koko yhteiskunnan resilienssiä toimintaympäristössä. Toisaalta edistyksellisten haittaohjelmien (APT) aiheuttamiin kyberuhkien osilta yritysten tilannekuva on muista haittaohjelmista saatavaa uhkakuvaa haastavampi. Erityisesti ATP-uhkien osalta toiminta edellyttää erityisen tiivistä viranomaisten ja yritysten välistä yhteistyötä.

Tutkimuksen perusteella voidaan todeta, että kohdeorganisaatioiden kyberturvallisuustoiminnassa esiintyy edelleen häiriötilannekohtaista reaktiivisuutta, mutta merkittäviä edistysaskelia kohti proaktiivista toimintaa on otettu kaikilla päätöksentekotasoilla. Kyberturvallisuuden johtamiseen on muodostunut strategia- ja riskiperusteisia näkökulmia. Kyberturvallisuus huomioidaan jo melko usein yritysten toimintapolitiikoissa. Toiminnan vakavien häiriötilanteiden huomioimiseksi osassa yrityksiä on laadittu varautumissuunnitelmia ja niiden toteuttamista on myös harjoiteltu. Riskitarkastelua ja varautumissuunnittelua ollaan liittämässä aikaisempaa useimmin liiketoimintaprosesseihin.

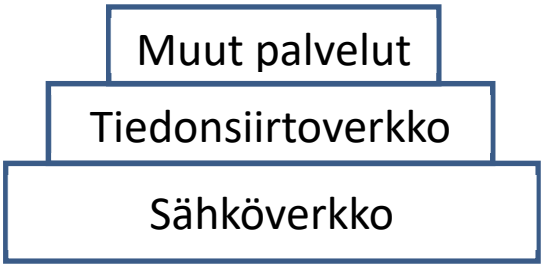
Kansallisen tutkimustoiminnan ylläpitämistä pidetään tärkeänä ja organisaatiot ovatkin omalta osaltaan sitoutuneita osallistumaan kansalliseen tutkimustoimintaan. Huoltovarmuuskeskuksen johdolla toteutettavaa harjoittelutoimintaa pidetään tärkeänä ja hyvänä toiminnan kehittämismahdollisuutena.

Tutkimuksessa tunnistettiin kattavasti organisaatioissa toteutettuja strategisia linjauksia sekä operatiivista ja teknillistä/taktista toimintaa edistäviä toimenpiteitä. Niitä ovat muun muassa riskiperusteinen johtaminen, henkilöstön koulutusohjelmat, parhaiten saatavilla olevien tuotteiden ja palvelujen käyttö suojaustoimenpiteinä, yhteistyöverkostot, asiantuntijapalvelut, kuten auditointipalvelut ja harjoittelu. Lisäksi joillakin organisaatioilla on käytössään hälytysmenettelyt nopean vasteen aikaan saamiseksi häiriötapahtumiin.

Lisäksi tutkimuksessa ”Kyberturvallisuuden strateginen johtaminen Suomessa” tuli esiin nopean vasteen osalta menettely, jossa organisaatioiden tietoturvapalveluita laajennetaan tulevaisuudessa paremman tilannekuvan saa-

miseksi hyödyntämällä tietoturvapalveluihin kuuluvaa tietoturvavalvomotoimintaa, SOC-toimintaa (Security Operations Centre, SOC). Näin tietoturvauhkia ja -poikkeamia havaitaan paremmin ja nopeammin, jolloin niiden vaikutusten ennakointi tehostuu. SOC-järjestelmäkokonaisuus luo automaattisesti hälytyksiä havaitessaan mahdollisesti poikkeavaa tai haitallista liikennettä. Tietoturvavalvomo kokoaa hälytykset ja pystyy yhdessä muun keräämänsä tiedon sekä yhteystyötahojen toimittamien uhkatietojen avulla reagoimaan tietoturvapoikkeamiin. Uhkatilanteet pyritään ratkaisemaan yhteistyössä lähituen sekä verkkoa ylläpitävän tahon kanssa. Tietoturvavalvomo analysoi uhkia ja koordinoi korjaavien toimenpiteiden toteutuksen. (Lehto, ym., 2018, 46).

Tutkimuskokonaisuuden tulosten perusteella kansallisen kriittisen infrastruktuurin käsitettä voidaan pelkistää kuvion 11 mukaiseksi rakenteeksi. Sen perusteella sähköyhtiö voi asemoida oman strategisen asemansa ja tunnistaa toimintansa osana kokonaisuutta, jonka muiden osin toiminta perustuu luotettavasti toimivaan sähköverkkoon. Rakenne edesauttaa myös eri kerroksissa toimivien organisaatioiden keskinäisten kyberriippuvuuksien havainnoinnissa sekä tehokkaiden ja tarkoituksenmukaisten toimenpiteiden kohdistamisessa rakenteeseen toiminnan jatkuvuuden varmistamiseksi.




KUVIO 11 Kriittisen infrastruktuurin pelkistetty rakenne.

Tutkimustulosten perusteella sähköyritysten kybertoimintaedellytyksiä edistävät seuraavat vahvuuksia ja mahdollisuuksia hyödyntävät, heikkouksia ja uhkia torjuvat toimenpiteet:

- Osallistutaan aktiivisesti kansalliseen viranomaisten ja yritysten väliseen yhteistyöhön (PPP-yhteistyö) kaikilla tasoilla. Näin parannetaan yleistä kyberturvallisuuden tilannetietoisuutta sekä edistetään toimenpiteitä erityisesti edistyneimpien haittaohjelmien tiedostamisessa ja torjunnassa. Vahvistetaan edelleen toimialakohtaista verkostoitumista ja muuta verkottumista yritysmaailman kanssa. Pidetään yllä vahvaa kansainvälistä yhteistyötä eri foorumeilla. Kehitetään yrityskohtaisesti reaaliaikaisen taktisen tason tilannekuvajärjestelmän käyttöä ja hyödynnetään kumppaneiden parhaiksi todettuja tuotteita ja palveluja.

- Kehitetään toimintaa kybertoimintaympäristössä aiempaa proaktiivisempaan johtamiseen. Kehitetään toimenpiteitä kaikilla päätöksentekotasoilla ja panostetaan kyberturvallisuutta edistävään kyvykkyyden vahvistamiseen yrityksen koko kyberrakenne huomioiden. Yrityksen toiminnan vahvuus kybertoimintaympäristössä muodostuu seuraavista elementeistä: strategia, työkalut (politiikka, verkostot tuotteet ja palvelut, varautumissuunnitelmat), koulutus ja vakuuttaminen.
- Kehitetään yrityskohteista kyberturvallisuuden systeemiajattelua, jossa prosessit ovat verkostossa ja tieto on keskeisessä roolissa. Varmistetaan, että verkoston kaikki osat huolehtivat omasta suojautumisestaan ja, että verkoston solmut pitävät itsensä jatkuvasti verkoston toimivina osina. Verkoston jäsenten toiminnan motivaatio muodostuu yhteisestä kyberturvallisuuden intressistä ja resilienssin saavuttamisesta ydinalueille. Toiminnan avainasia on jatkuva ja tiivis informaation vaihto.
- Kehitetään yrityksen jatkuvan parantamisen menettelyjä kehittämällä auditointitoimintaa aiempaa kattavammaksi periaatteella, joka huomio koko toiminnan, tuotteet ja palvelut.

#### 5.1.4.2 Kyberturvallisuuden merkittävimmät haasteet

Tutkimustietojen perusteella voidaan todeta, että isojen yritysten osalta kyberturvallisuuden valmiudet ovat kehittyneet myönteiseen suuntaan. Monet sähköyhtiöille palveluja tuottavat pienetkin yritykset voivat olla merkittävässä roolissa isompien yritysten toimintaverkostoissa. Huomion arvoista on, että tutkimusten mukaan muissa yrityskokoluokissa perinteistä tietoturvaa kattavammat suojaustoimenpiteet ovat vasta käynnistymässä ja toimenpiteiden resursoinneissa on eroja (Helsingin seudun kauppakamari, 2019). Ketjutetut palvelut koetaan haasteellisiksi osassa sähköyhtiöitä, vaikka omat toimenpiteet voivatkin olla jo melko hyvin kehittyneet. Näkyvyyttä ketjun eri osiin ei ole helposti saatavilla, jolloin herää kysymys osien kyberturvallisuuden kyvykkyydestä. Yritysten kyberturvallisuuteen liittyviä kyvykkyyseroja on todennettu Helsingin seudun kauppakamarin tutkimuksissa 20015 – 2019. Ensimmäisessä tutkimuksessa vuodelta 2015 todetaan asiasta ja yritysten kyvystä tunnistaa kyberturvallisuuden häiriöitä seuraavasti: (Helsingin seudun kauppakamari, 2015)

> ”Vastauksista kävi ilmi selvä ero suurten yritysten ja muiden valmiuksien välillä. Suurilla yrityksillä on vastauksien mukaan selvästi korkeampi omaa kyky tunnistaa tunkeutumiset itse. Tämä kyky on hyvin keskeinen tekijä suojautumisessa.”

Kahdessa myöhemmässä vastaavassa tutkimuksessa edellä mainittu tilanne ei ollut oleellisesti muuttunut. (Helsingin seudun kauppakamari, 2016: Helsingin seudun kauppakamari, 2019).

Digitalisaatiosta on tullut yhä tärkeämpi osa energiayhtiöiden ja niiden asiakkaiden välistä toimintaa. Digitalisuuteen pohjautuvat palvelut ovat osa tätä kehitystä. Erilaiset sovellukset ja palvelut ovat siten aiempaa enemmän Internet- ja pilvipalveluina, josta on ollut seurauksena se, että yritykset ovat luoneet reaaliaikaisia digitaalisia yhteyksiä kumppaneihinsa, asiakkaisiin, palvelu- ja tavaratoimittajiin sekä julkishallintoon. Nämä menettelyt kybertoimintaympäristössä ovat tehostaneet toimintakokonaisuutta, mutta samalla niistä on ollut seurauksena erilaisten haavoittuvuuksien lisääntyminen. Tästä johtuva uhkakuvien laajentuminen edellyttää erityisen huomion kiinnittämistä yritystoiminnan tilannetietoisuuteen, riskitarkasteluun ja varautumiseen.

Osana edellä kuvattua kehitystä useat keskeiset kriittisen infrastruktuurin sähköyhtiöt ovat ulkoistaneet myös tietoliikennettään, IT-toimintojaan ja -palvelujaan. Se on samalla merkinnyt myös osan oman kyberturvallisuuden hallinnan ulkoistamista. Ulkoistetuissa verkostoissa ja palveluissa on sekä kotimaisia että ulkomaalaisia yrityksiä. Tutkimuksessa on todettu verkostossa toimivien tietoturvayritysten osaamisen olevan korkealla tasolla, mutta samalla esitettiin epäilyjä resurssien riittävyydestä, mikäli kohdataan laajoja selvitystä vaativia häiriötapauksia.

Sähköyhtiön toimintaprosessien merkittävimmät kyberympäristöön liittyvät riskit edellyttävät luottamuksen kasvattamista ja ylläpitämistä kaikilla yritystoiminnan tasoilla. Yrityksen kattavat kyberluottamusta lisäävät toimenpiteet yhdessä toiminnan kyvykkyyksien kehittämisen kanssa parantavat myös kilpailukykyä. Yrityksen tai jonkin sen organisaatio-osan toiminnan kehittämisen onnistumien riippuu viimekädessä johdon sitoutumisesta toimintaan ja toimenpiteiden resursoinnista. Usein joudutaankin turvautumaan yrityksen ulkopuolisiin kehittäjiin jo pelkästään siksi, että oma henkilöstö sitoutuu lähes kokonaisuudessaan päivittäiseen operatiiviseen toimintaan. Yrityksen ulkopuolisen kehitysresurssin käyttö kasvattaa organisaation kyvykkyyttä myös tietotaidon hankinnan näkökulmasta katsottuna.

## 5.2 Tutkimuskohde 2; sairaala

RR8. Pöyhönen J., Lehto M., Lehto M. (2019). Kyberturvallisuus sairaalajärjestelmissä, toiminnan kehittäminen University of Jyväskylä, Faculty of Information Technology, research paper, 75/2019.

RR9. Lehto M., Pöyhönen J., Lehto M. (2019). Kyberturvallisuus sosiaali- ja terveydenhuollossa. Loppuvaportti Vol 2. VFH- ja WHC-hankekokonaisuus. Jyväskylä yliopisto, IT-tiedekunta. Jyväskylä yliopisto, Informaatioteknologian tiedekunta.

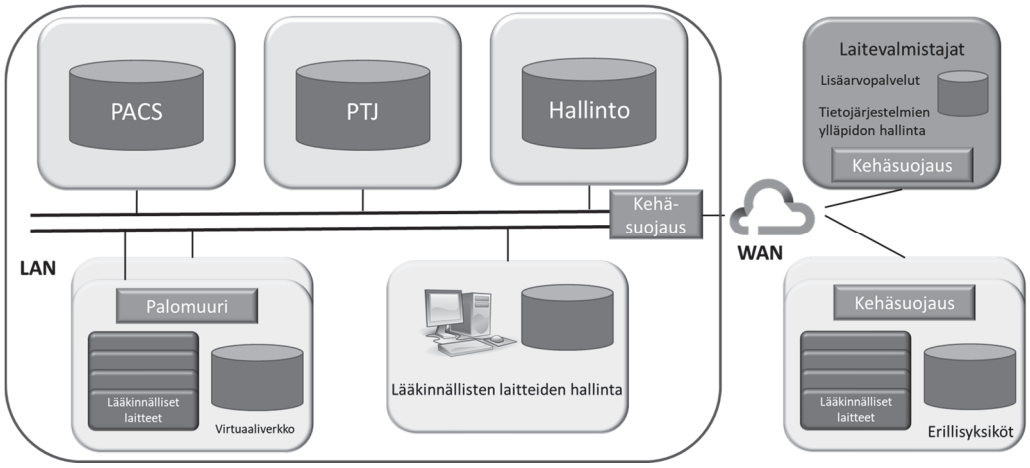
### 5.2.1 Sairaalan tietojärjestelmät

Terveydenhuollon tietojärjestelmäkokonaisuudessa on useita satoja erilaisia järjestelemiä ja laitteita sekä niiden välisiä yhteyksiä. Käyttäjiä koko toimialalla on noin 180 000 (Terveyden ja hyvinvoinnin laitos, 2014).

Sairaaloiden järjestelmät ovet eräänlaisia automaatiojärjestelmiä, joilla potilaiden tilaa mitataan ja seurataan. Niiden laitteet keräävät tietoja potilaista ja tarvittaessa voivat lähettää hoitohenkilökunnalle esimerkiksi hälytyksiä huomiota vaativista tilanteista tietoverkon yli. Lääkepumput voivat ottaa vastaan tietoja potilaille annettavista lääkemääristä ja muuttaa toimintaansa saamiensa ohjaustietojen perustella. Lisäksi sairaaloissa on verkottuneita kiinteistöautomaatio- ja turvajärjestelmiä. Automaatiojärjestelmien yhteinen piirre on, että ne koostuvat herkistä laitteista, jotka digitaalisen tiedon varassa vaikuttavat fyysiseen maailmaan. Ne muuttavat myös fyysisestä maailmasta tekemiään havaintoja digitaaliseksi tiedoksi päätöksentekoa varten. Laitteiden edellytetään usein toimivan reaaliaikaisesti. (Viestintävirasto, 2016)

Sairaalaympäristön toimivuus edellyttää useiden erilaisten tietojärjestelmäja automaatiojärjestelmäkokonaisuuksien hyödyntämistä. Merkittävimpiä niistä ovat sairaalan ydinprosesseihin kuuluva tietojärjestelmäkokonaisuus sekä kiinteistön automaatio- ja turvajärjestelmät (kulunvalvonta).

Tutkimuskohde 2 käsittää edellä mainituista sairaalan tietojärjestelmäkokonaisuuden. Kuviossa 12 on esitetty sen geneerinen rakenne (Integrating the Healthcare Enterprise, 2015, 21).




KUVIO 12 Geneerinen sairaalan tietojärjestelmäkokonaisuus.

Kuviossa 12 on esitetty sairaalan tietojärjestelmäkokonaisuudesta keskeisimmät osat kuten hallinnon tietojärjestelmä, potilastietojärjestelmä eli PTJ, digitaalisen kuvan arkistointijärjestelmät (Picture Archiving Communications Systems, PACS) sekä lääkinnälliset laitteet kokonaisuutena. Kuvioon on myös hahmoteltu niiden väliset tietoverkkorakenteet. Verkkorakenne ulottuu myös laitetoimittajiin ja terveydenhuollon erillisyksiköihin ja siten niiden lääkinnällisiin laitteisiin. Kokonaisuudesta muodostuu käytännössä laaja verkottunut tietojärjestelmien muodostama toimintaympäristö.

Terveydenhuollon tietojärjestelmien keskiössä ovat potilastietojärjestelmät (PTJ). Potilastietojärjestelmien ydinjärjestelmiä käytetään sairaaloissa laajasti. Ydinjärjestelmiä ovat muun muassa potilaiden lähetteiden käsittely- ja ajanva-

rausjärjestelmät sekä hoitotietojen kirjausjärjestelmät. Potilastietojärjestelmät pitää sisällään potilaan historiatiedot sairaalakäynneistä ja toimenpiteitä. Niistä tuotetaan myös tarvittavat hallinnolliset raportit, tilastot, kustannus- ja laskutustiedot. Potilastietojärjestelmät voidaan jakaa lähes kaikissa yksiköissä käytettäviin edellä kuvattuihin operatiivisiin ydinjärjestelmiin sekä niitä täydentäviin yksikkökohtaisiin erillisjärjestelmiin. (Integrating the Healthcare Enterprise, 2015, 11)

Sairaalajärjestelmien sisältämien lääkinnällisten laitteiden tyyppikirjossa on tekniikan kehityksen myötä tapahtunut huomattavaa kasvua, joka on osa yleisestä älykkäiden laitteiden kehityksestä ja käytön lisääntymistä. Niihin lukeutuvat myös muun muassa matkapuhelimet, tablettitietokoneet ja henkilökohtaiset laitteet, jotka pitävät sisällään lääkinnällisiä sovelluksia/ohjelmistoja.

Lääkinnällisten laitteiden geneerinen arkkitehtuurimalli koostuu tietokonelaitteistosta, sen laiteohjelmistosta, käyttöjärjestelmästä, hallinta- ja valvontaosiosta sekä tiedonsiirtoverkosta. Lisäksi laitetasolta on käytössä yleisiä liityntäportteja mittaussensoreille, käyttäjäliittymiä ja standardiliittymiä, kuten liityntämahdollisuus esimerkiksi USB-laitteille (Universal Serial Bus, UBS). Laitteissa käyttöjärjestelmät perustuvat usein kaupallisiin arkkitehtuureihin ja käytössä on myös niihin liittyvä kaupallisia laitteistoalusta (Commercial off-the-shelf, COTS). Käyttöjärjestelmä voi käyttää kaupallisia laitteistokomponentteja (emolevy, tietokone) ja myös käyttäjälle räätälöityjä alustoja. Hallinta- ja valvontaosio pitää sisällään testaus-, kalibrointi-, monitorointiominaisuuksia, laitteen logitietoja, laitteen turvamekanismien hallintaominaisuuksia, laitteen konfiguraatio- ja ohjelmiston versionhallintatietoja. Tiedonsiirtoverkossa siirretään kliinistä-, hallinnollista- ja teknillistä dataa. Arkkitehtuuri pitää sisällään kyberturvallisuuden näkökulmasta tarkasteltuna keksisiä toiminnallisia komponentteja. (Integrating the Healthcare Enterprise, 2015, 16)

Sairaalaympäristössä käytettäviä yleisiä laitteita yhdistävät verkkoyhteystyypit voidaan kuvata käyttötarkoituksineen seuraavasti: (Grimes, 2016, 11)

- Langallisen tai langattoman verkon kautta yhteys elektronisiin potilastietoihin.
- Yhteys kuva-/tallennusvarastoon (esim. Picture Archiving and Communication Systems, PACS - kuvantumisjärjestelmä).
- Etäyhteys tietoihin/kuviin (esim. lääkäri).
- Etäpalvelu (esim. valmistajan päivitykset, vianetsintä, korjaus).
- Etähallinta (esim. kliiniset päivityksiä kuten lääkekirjastot infuusiopumpuille).
- Etäohjaus (esim. muuttaa hälytyksiä, asetuksia, hoidon määrää)
- Lääkinnällisten laitteiden välinen sisäinen viestintä (esim. diagnoosilaite "informoi" terapeuttisia laitteita ja valvoo lääkkeiden annostelua).

Sairaalan verkottuneissa tietojärjestelmissä kertyy reaaliajassa tietoa eri lähteistä. Osa sairaalan datasta on pirstaloitunut erillisiin järjestelmiin, mikä luo haasteita sen keskitettyyn jakamiseen tai analysointiin. Toisaalta osa tietolähteistä, kuten

potilas-, ja perimätietojärjestelmät muodostavat jo lähtökohdiltaan yhtenäisen data-alustan. Tulevaisuudessa tietojärjestelmäkehityksen on mahdollistettava sekä palvelujen ja rakenteiden että teknisten ratkaisujen uudistaminen, jolloin edellytyksenä on yhteistyöhön nojautuva ja verkostomainen ratkaisujen kehittämistapa. Parhaimmillaan ratkaisuja levitetään koko terveydenhuollossa tehokkaasti laajamittaiseen käyttöön ja niiden pohjalta kehitetään myös uusia palveluita ja tuotteita. Toimintaan kytkeytyvät myös kyberturvallisuuden kyvykkyydet, ihmiset, prosessit ja teknologiat, ja niiden toiminnan kehittäminen osana sairaalan turvallista toimintaa.

### 5.2.2 Sairaalan kyberturvallisuuden merkitys

Sairaalatoiminnot ja laajasti koko terveydenhuolto ovat merkittävä osa kansallista kriittisestä infrastruktuurista ja siten niiden kyberturvallisuuteen kohdistuukin aivan erityisiä vaatimuksia. Sairaalan järjestelmien tietojen luotettavuus, eheys ja saatavuus (käytettävyys) ovat äärimmäisen tärkeitä potilaiden turvalliselle hoidolle ja koko sairaalan toimivuudelle. Tietojen luottamuksellisuutta on suojattava paitsi yksityisyyden suojan takaamiseksi, myös henkilötietojen rikollisen käytön estämiseksi. Kyberturvallisuuden osalta tarkasteluun on otettava kattavasti toimintaprosessien Internet-verkkoon kytkeytyvä digitaalinen järjestelmä- ja laiteympäristö. Näiden järjestelmien ohella myös sairaalarakennusten kiinteistöautomaatio ja turvajärjestelmät asetuvat kyberturvallisuuden tarkastelun osalta tärkeään asemaan.

Huomattavaa on, että terveydenhuolto on ollut viime vuosina yhä lisääntyvässä määrin kyberhyökkäysten kohteena. Tilanneteen laajuutta kuvaa esimerkiksi tapahtumat Yhdysvallissa, jossa sataa miljoonaan terveydenhuollon rekisteritietoa oli hyökkäyksen kohteena yhden vuoden aikana. (IBM, 2019 b).

Terveydenhuollossa tapahtuva digitalisaation nopea kehittyminen merkittävää tarkasteltaessa toimialaa myös kyberturvallisuuden näkökulmasta. Teknillinen kehitys mahdollistaa muun muassa sairaalapalveluja jatkokehittämisen erityisesti uusia laitteita ja tietoverkkoja hyödyntämällä. Siinä voidaan hyödyntää esimerkiksi laitteita, jotka ovat osa esineiden internetin eli IoT:n (Internet of Things, IoT) jatkuvaa laajentumista. Verkkojen ja niihin kytkeytyvien älykkäiden laitteiden muodostama kokonaisuus tietovarantoineen aiheuttaa toisaalta myös yleistä huolta toiminnan luotettavuudesta. Kyberturvallisuutta haastavat tekniikat, joissa esiintyy erityisesti haavoittuvia laitteita ja ohjelmistosovelluksia osana hoitotyötä. Usein ne ovat osana niin sanottuja kyberfyysisiä järjestelmiä. Haavoittuvuudet voivat johtaa siten vaaratilanteisiin, joilla on suora potentiaalinen vaikutus kliiniseen hoitoon ja potilasturvallisuuteen. Yleisesti voidaan todeta, että jo nykyisessä tilanteessa verkottunut toimintaympäristöä muodostaa haavoittuvuuksista riskejä laajalti sairaalajärjestelmiin. Toimintaprosesseissa tapahtuva uusien tietoteknillisten järjestelmien ja laitteiden lisääntyminen kasvattaa näitä riskejä edelleen. Näin ollen onkin oleellista huomioida kyberturvallisuuden edistämisessä teknillisten ratkaisujen hyödyntäminen erillisten toiminnallisten alueiden aikaansaamiseksi toimintaprosesseittain ja kehittää tarkoituksenmukai-

sia suojaustoimenpiteitä niissä. Myös ennakoivaa varautumista riskien tarkastelun lisäksi on tarpeen kehittää. Tilanne koskettaa laajasti terveydenhuollon alueella eri toimijoita ja sidosryhmiä.

Sairaalaa kohtaan tapahtuvilla kyberhyökkäyksillä on onnistuessaan merkittäviä vaikutuksia koko terveydenhuollossa, koska alan toiminta vaatii reaaliaikaisen pääsyn toiminnan edellyttämiin palveluihin kuten potilastietojärjestelmiin tai sähköisiin resepteihin. Näissä toimintaprosesseissa keskeytyksiä aiheuttavat haittaohjelmahyökkäykset voidaan havaita nopeasti, mutta palveluiden palauttaminen normaalitilaan voi kestää useita päiviä riippuen suojausjärjestelyjen toteutuksesta, järjestelmän koosta, tartunnan laajuudesta ja varmuuskopiojärjestelyistä. On myös mahdollista, että osassa monimutkaisia järjestelmiä haitalliset tapahtumat huomataan vasta kuukausien kulutta, jolloin niiden tutkinta on haastavaa ja toisaalta isoja tietomääriä on jo voinut päätyä ulkopuolisten hallintaan tai rikollisten käyttöön. Sairaalan kyberturvallisuudella on merkittävä vaikutus terveydenhuollon toimintaprosessien jatkuvuuden hallintaan ja koko kriittisen infrastruktuurin toiminnan luotettavuuteen.

### 5.2.3 Sairaalan kyberturvallisuuden uhkatekijät

Terveydenhuolto on toimialana kiinnostava kohde kyberhyökkäyksiä tekeville yksittäisille haitantekijöille tai rikollisorganisaatioille muun muassa toimialan sensitiivisen tietosisällön vuoksi. Terveydenhuollon kyberturvallisuuden jatkuva parantaminen ja toimintaympäristön uhkatietoisuuden kehittäminen palvelevat kaikkien kansalaisten etuja. Se edellyttää vahvaa ymmärrystä terveydenhuollon tietoturvasta ja toimintatavoista. Terveydenhuollon suurimmat kyberuhat liittyvät sairaalan lääkinnällisten laitteiden käyttöturvallisuuteen. Sairaalaympäristössä muita merkittäviä uhkia muodostavat muun muassa haittaohjelmat, jotka hyödyntävät järjestelmien ja laitteiden ohjelmistojen haavoittuvuuksia, laitteiden käyttötavat ja salasanakäytänteet, etähallittavat laitteet ja mobiililaitteet. Lisäksi sairaalaympäristössä uhkana ovat haittaohjelmat, jotka leviävät tyypillisesti murrettujen verkkosivustojen ja verkkomainosten, sähköpostin ja sosiaalisen median välityksellä. Henkilökunnan käyttäessä näitä palveluja uhkana on, että vierailukäynti voi johtaa sivustolle, josta haittaohjelma pääsee vierailijan tietokoneelle ja sitä kautta se voi levitä edelleen muualle organisaation verkkoon. (Halonen, 2016, 7, 26.)

Väitöstyön taustatutkimuksena toimivan sairaalan kyberturvallisuustutkimuksen (RR8) tausta-aineistoksi analysoitiin pääosin vuosien 2013-2018 aikana tapahtunutta yli kuuttakymmentä (65 kpl) hyökkäystä terveydenhuoltoa vastaan. Tarkasteluun löydettiin tapauksia Suomesta, muualta Euroopasta ja Pohjois-Amerikasta raportoituja kyberhyökkäyksiä. Menetelminä niissä korostuvat tietojen kalastelumenetelmät, kiristysohjelmat, palveluestohyökkäykset, hakkeroinnit, virushaittaohjelmat ja laiteiden sekä tallenteiden varkaudet tai katoamiset. Tapahtumat sijoittuvat organisaation kyberrakenteen eri kerroksille. Haitalliset tapahtumat voivat levitä rakenteessa laajalle organisaatioon eri tietoverkko-

jen välityksellä. Verkkojen kautta on mahdollista löytää väyliä teknillisiin järjestelmiin tai laitteisiin tunkeutumiselle, joista on suora yhteys esimerkiksi kyberfyysiseen vaikutukseen sairaalan toimintaprosesseissa.

Vastaavasti Yhdysvaltain Office for Civil Rights (OCR) organisaatiolle vuonna 2015 ilmoitetusta terveydenhuoltoa kohtaa kohdistetun noin 300:n kyberhyökkäyksen jakauma oli seuraava: (Snell, 2016.)

- Hakkerointi ja tietomuro, 220
- Tietokoneen (vast.) varkaus, 58
- Tietokoneen (vast.) häviäminen, 16
- Tietojen vääränlaisesta hävittämisestä, 7

Järjestelmien ja laitteiden ohjelmistossa voi olla virheitä, jotka altistavat koko laitteen tai sen sisältämän tiedon tietoturvaloukkauksille. Virheisä aiheutuva haavoittuvuustyyppi mahdollistaa haittaohjelmien levityksen ja pääsyn käsiksi salassa pidettäviin tietoihin tai vaikkapa estää laiteohjelmiston toiminnan. Ohjelmistohaavoittuvuuden hyväksikäyttö voi toimia myös haittaohjelman levittämis- tai aktivoitumismekanismina alemman tason käyttöoikeuksilla varustettuihin laitteisiin. Alemman tason käyttöoikeuksilla aktivoitunut haittaohjelma voi hyödyntää kohteen ohjelmistohaavoittuvuutta ja siten saada haltuunsa korkeamman tason käyttöoikeuksia. Haittaohjelman levitysmekanismi ketjuuntuu ja on siten vaikeasti jäljitettävä. Haittaohjelmien tyypillinen levittämistapa on sähköpostin liitetiedoston kautta tapahtuva leviäminen. Sähköpostiohjelmistojen tai selainten haavoittuvuudet voivat mahdollistaa myös haittaohjelman aktivoitumisen ilman liitetiedoston avaamista jo sähköpostin esikatselutilassa. Sähköpostin liitetiedostoina leviävät virukset voivat hyödyntää myös liitetiedoston käsittelyyn käytettyjen sovellusohjelmistojen haavoittuvuuksia. Tällöin olennaista on pyrkiä tunnistamaan haavoittuvuuksista aiheutuvat uhkat ja hallitsemaan niiden vaikutuksia. Organisaation onkin huolehdittava järjestelmien ja laitteiden ohjelmistojen aktiivisesta päivittämisestä sekä ohjeistettava välittömät toimenpiteet häiriötilanteiden varalle. (Valtiovarainministeriö, 2009.)

Organisaatioissa henkilökunnan IT-järjestelmien käyttötavoista ja salasanakäytänteistä voi muodostua merkittäviä uhkia kyberturvallisuuteen, mikäli toimitaan ohjeiden ja kyberturvallisuuspolitiikan vastaisesti. Esimerkkeinä toimivat tapaukset, joissa asetetaan yhteiskäyttöisiä salasanoja tai estetään vaikkapa aikalukituksen päälle menoa laitteessa. Organisaation toiminnassa tuleekin muistaa, että henkilökunta on helpoin kohde tietojen kalasteluun rikollisiin tarkoituksiin. (Siwicki, 2016.)

Terveydenhuolto ja erityisesti sairaalat ovat kyberrikollisille kiinnostavia kohteita muun muassa potilastietojärjestelmien sisältämien tietojen takia. Tyypillinen potilastieto voi sisältää luottokorttinumeroita, sähköpostiosoitteita, sairasvakuutusnumeroita, työnantajatietoja sekä sairaushistoriatietoja. Rikolliset hyötyvät tiedoista myymällä niitä pimeillä markkinoilla. Tiedot ovat yleensä voimassa vuosia, jolloin kyberrikolliset käyttävät tietoja myös tietojenkalasteluhyökkäyksissä, petoksissa sekä identiteettivarkauksissa (Lehto, ym., 2017, 18).

Kyberrikolliset ovat siirtäneet aiempaa enemmän huomiotaan terveydenhuoltoon, ja uhkista on tullut yhä monimutkaisempia (IBM, 2019 b). Rikolliset voivat myydä hakkeroinnin avulla saatuja potilastietoja, jotka ovat arvokkaita niiden tiedon määrän ja laadun vuoksi. Kiristyshaittaohjelmahyökkäykset ovat myös laajentuneet sairaaloihin kohdistuen niiden potilastietojärjestelmiin. Näissä hyökkäyksessä järjestelmien tietojen käytettävyys on estetty. Toiminnan luonteeseen kuuluu, että tietojen käytettävyyden palautuksista vaaditaan lunnaita.

Sairaaloissa lääketieteelliset laitteet ovat nykyään lähes poikkeuksetta verkkoon yhdistettäviä laitteita, jolloin tietoa voidaan hyödyntää koko organisaatiossa. Kyberturvallisuuden uhkat kohdistuvat siten koko organisaatioon. Lisäksi erilaisia mobiililaitteita käytetään yhä useammin myös sairaaloissa ja laajasti koko terveydenhuollossa. Laitteiden käyttö ei rajoitu paikkaa ja siten ne eivät ole välttämättä rakenteellisesti suojatussa tilassa. Laite voi myös jäädä ajoittain ilman valvontaa, jolloin riski sen joutumisesta varastetuksi kasvaa. Mobiililaitteiden kyberturvallisuuteen liittyy haasteita perinteisiä paikallisesti käytettäviä tietojärjestelmiä enemmän. Mobiililaitteiden käytön riskit kriittisissä toiminnoissa tulevat myös siitä, että niiden tiedonsiirto tapahtuu sairaalajärjestelmien ulkopuolisessa verkoista.

Digitalisaation muodostama kehitys on kasvattanut teknologiamarkkinoita, joka mahdollistaa sen, että yksilöt keräävät ja säilyttävät omia terveystietojaan. Tämä on johtanut siihen, että kun aiemmin terveystiedot olivat keskitetysti saatavilla vain terveydenhuollon ammattilaisille, niin nyt tietoja tallennetaan useisiin eri paikkoihin. Tiedot ovat siten hajautuneet. Esimerkkeinä toimivat henkilökohtaiset kannettavat laitteet, älypuhelimet, kannettavat tietokoneet ja pilvipalvelut. Yksilöillä on aiempaa helpompi pääsy tietoihinsa, mutta se on tuonut esiin uusia yksityisyyden suojaa koskevia tietosuojakysymyksiä ja osaltaan myös laajempia kyberturvallisuusriskejä. Terveydenhuollon palveluja ollaan lisäämässä koteihin aiempaa enemmän. Kokonaislaitekanta lisääntyy ja se asettaa haasteita laitteiden, ohjelmistojen ja verkon toimivuudelle ja käytölle sekä siten myös koko alueen kyberturvallisuudelle.

Sairaaloiden ICT-järjestelmien ja -laitteiden lukumäärä on huomattavan laaja verrattuna moneen muuhun kriittisen infrastruktuurin organisaatioon. Se merkitsee väistämättä myös ikärakenteeltaan kirjavaa laitekantaa. Erillishankinnat, jotka on toteutettu ohi tietohallinto-organisaation lisäävät erityisesti laitteisiin liittyvän tilannetietoisuuden haasteita. Tietohallinto-organisaatiossa on myös paras tieto kyberturvallisuudesta ja organisaation kyberturvallisuuspolitiikan ylläpitämisestä. Lääkinnällisten laitteiden turvallisuutta koskeva määräys on vuodelta 2004 (Lääkelaitoksen julkaisusarja 1/2004). Siinä todetaan, että alan järjestelmien kokonaisturvallisuuden kehittämisessä avainasemassa ovat laitteen elinkaaren hallinta, ohjelmistojen turvallisuus, riskienhallinta ja tietoturvallisuus (Fimea, 2004, 4). Lisäksi todetaan, että uusi tekniikka edellyttää valmistajan kannalta merkittäviä tuotekehityspanostuksia tietoturvaominaisuuksiin ja, että kehitys monimutkaistaa järjestelmärakenteita ja käyttäjäorganisaation tulee huomioida tämä asia (Fimea, 2004, 41,42). Etäkäytettävien ja -hallittavien laitteiden

markkinoiden nykyinen laajuus ei ole ollut tuolloin vielä määräystä laadittaessa näköpiirissä. Siinä on kuitenkin nähty kehityskulku ja huomioitu järjestelmien monimutkaistuminen sekä eri osapuolten välinen yhteistyön tarve niitä kehitettäessä. Lisäksi laitteiden ohjelmistoja päivitetään lähes poikkeuksetta etänä. Tämä kokonaisuus tarkoittaa sitä, että myös laitteistotoimittajat kytkeytyvät terveydenhuollon kyberturvallisuuteen. Uhkatekijät korostuvat, mikäli yhteistyötä ja organisaation toimintaprosesseja ei noudateta.

Koko terveydenhuolto ja erityisesti sen sairaalaorganisaatiot ovat kiinnostavia kohteita kyberhyökkäyksille. Onnistuessaan niiden vaikutukset ovat laajaalaisia ja merkittäviä ulottuen potilasturvallisuuteen, potilaiden ja työntekijöiden tietojen yksityisyyteen ja lopulta sairaalan maineeseen sekä talouteen.

### 5.2.4 Sairaalan kyberturvallisuuden nykytila

Tietotekniikkaa on käytetty laajalti lääketieteessä viimeisten kahden vuosikymmenen aikana. Sähköisiä terveystietojen, biolääketieteen tietokantojen ja kansan terveyttä koskevia tietojen saatavuutta ja jäljitettävyyttä on kehitetty. Tietojen taloudellinen arvo on tunnistettu. Terveydenhuoltoon liittyvät tiedot ovat erittäin luottamuksellisia. Tietojenkäsittelyyn ja tallennukseen liittyvää tilannetta voidaan kuvata seuraavasti: (Zhang, ym., 2017, 88.)

- Datan kasvu: Digitalisaatio ja erityisesti sairaalatietojärjestelmien kehitys on lisännyt lääketieteellisen datan määrää. Kannettavien terveys/hyvinvointilaitteiden käytön lisääntyminen on kasvattanut myös koko terveydenhuollon dataa.
- Tiedonkäsittelyn nopeus: Useimmat lääketieteelliset laitteet, erityisesti kannettavat/puettavat laitteet, keräävät jatkuvasti tietoja. Nopeasti tuotetut tiedot on käsiteltävä välittömästi, jotta toimenpiteiden vasteaika saadaan minimoiduksi.
- Erilaiset tietorakenteet: Sairaalan tietojärjestelmät ja laitteet tuottavat monimutkaisia ja heterogeenisiä tietorakenteita (esim. tekstiä, kuvaa, ääntä tai videota).
- Arvonlisäys: Tietojen tehokas käyttö tuottaa lisäarvoa. Sähköisten potilastietojen (Electronic Health Record, EHR) ja sähköisten terveystietojen (Electronic Medical Record, EMR) yhdistämisen avulla voidaan tehostaa sairaalan ja koko terveydenhuollon tietojen arvonlisäystä.

Digitalisaatio on mahdollistanut sairaalapalvelujen edelleen kehittämisen muun muassa tietoverkkoja hyödyntämällä. Kehitykseen liittyvät jo tällä hetkellä myös älykkäät laitteet, IoT-laitteet ja kehittyneet sensorilaitteet keskinäisine tiedonsiirtokykyineen.

Sairaalan tietoverkkojen laajuus, niihin kytkeytyvien yksittäisten järjestelmien ja laitteiden määrät, laitteiden älykkyyden kehittyminen, sekä niissä olevat tietovarannot muodostavat sairaalasta järjestelmien järjestelmä. Tähän monimut-

kaiseen ja toiminnaltaan kompleksiseen kokonaisuuteen sisältyy myös toiminnan luotettavuuden haasteita. Kyberturvallisuuden osalta siitä esimerkkeinä toimivat ohjelmistohaavoittuvuuksia sisältävät järjestelmät ja laitteet ja niiden käyttötilanteet osana tietoteknillisesti moninaisesti verkottunutta toimintaympäristöä ja siten myös osana merkittävää määrää kyberfyysisiä järjestelmiä. Terveydenhuollossa haavoittuvuudet voivat johtaa vaaratilanteisiin, joilla on vaikutus kliiniseen hoitoon ja potilasturvallisuuteen. Tilanne koskettaa laajasti terveydenhuollon alueella eri organisaatioita ja niiden sidosryhmiä.

Sairaaloiden organisaatioiden tuleekin kiinnittää jatkossa entistä enemmän huomiota kyberturvallisuuteen. Laajat järjestelmäkokonaisuudet, joissa on myös vanhoja osajärjestelmiä ja laitteita, ovat haavoittuvia ilman mahdollisuutta jatkuvaan ohjelmisto- ja laitepäivitykseen. Kasvava määrä kehittyneitä kyberhyökkäyksiä on kohdistettu sairaaloihin ja potilastietojärjestelmiin.

Kaikilta hyökkäyksiltä ei ole mahdollista suojautua, mutta käytössä olevia kyberturvallisuuden perusratkaisuja voidaan vielä kehittää. Erityishuomiota tuleekin kohdistaa toiminnan kannalta kriittisiin tietoverkkoihin sekä kriittisiin järjestelmiin ja laitteisiin, kuten potilastietojärjestelmiin ja lääkinnällisiin laitteisiin. Monien toimintaa häirinneiden tapauksien taustalla on myös henkilöstön osaamiseen liittyviä haasteita kyberturvallisuuden perusteista tai tietotekniikan käyttöön liittyvästä tietoturvasta (IBM, 2019 b). Henkilöstön osaamista voidaan parantaa koulutuksella ja harjoittelemalla häiriötilanteissa toimimista. Henkilöstön kyvykkyyden kehittämisellä voidaan myös lisätä nykyistä tilannetietoisuutta toimintaan liittyvistä uhkista, vähentää hyökkäyksien onnistumisen mahdollisuuksia tai niiden vaikutuksen leviämistä sairaalan eri järjestelmiin. Monet kyberturvallisuuden ongelmista eivät ole ainutlaatuisia terveydenhuollossa, mutta niillä on välitön vaikutus sairaalan toimintaan, potilasturvallisuuteen ja hoitoon. Rikolliset ovat tietoisia potilastietojen arvosta ja tietojärjestelmien kriittisyydestä sairaalan toimintaan. Tietoisuus on lisännyt viime vuosina sairaaloiden houkuttelevuutta hyökkäyskohteena.

Kyberturvallisuuden haasteet liittyvät koko sairaalaympäristöön, jossa on paljon elinkaarensa eri vaiheissa olevia tietoverkkoja, -järjestelmiä, -laitteita ja ohjelmistoja. Yhdessä sairaalassa saattaa olla jopa yli neljäsataa järjestelmä- tai laitekokonaisuutta ja huomattava määrä niiden välisiä tiedonsiirtoverkkoja. Osaan järjestelmiä ja laitteita ei ole saatavana tämän hetken vaatimuksia vastaavia tietoturvapäivityksiä. Sairaaloihin tuodaan yhä enemmän myös henkilökunnan ja potilaiden omia tietoteknillisiä laitteita (BYOD-laitteita). Sairaalaympäristön laaja kirjo järjestelmiä ja laitteita muodostaa kyberhyökkäyksille rajapintoja, joita rikolliset voivat hyödyntää. Tilanne edellyttää kyberturvallisuuden tilannetietoisuuden, arkkitehtuurin ja suojausratkaisujen kehittämistä, toiminnan riskitarkastelua ja toiminnan jatkuvuuden hallintaan varautumissuunnittelua.

## 5.3 Organisaation tilannetietoisuuden haasteita

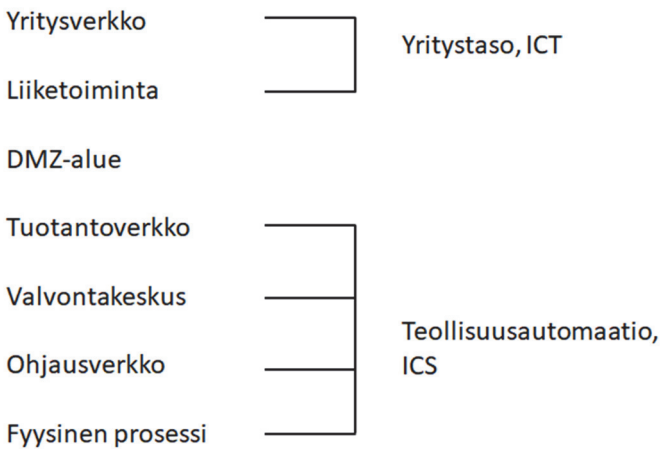
Millaisia kyberturvallisuuden tilannetietoisuuden haasteita liittyy organisaation ICT-varantoihin ja automaatiojärjestelmiin?

P3. Pöyhönen, J., Kotilainen P., Kalmari J., Poikolainen J., Neittaanmäki P. (2019). Cyber security of vehicle CAN bus. ECCWS 2019: Proceedings of the 18th European Conference on Cyber Warfare and Security (pp. 354-363). Published by Academic Conferences and Publishing International Limited. Reading. UK.

P5. Pöyhönen, J., Nuojua V., Lehto M., Rajamäki J. (2019) Cyber Situational Awareness in Critical Infrastructure Organizations. Springer artikkeli lähetetty joulukuussa 2019.

RR5. Pöyhönen J., Nuojua V. (2018). Tilannekuvatieto kriittisen infrastruktuurin yrityksen tietojärjestelmien tietoturvallisuudessa, Tutkimusongelman kuvaus. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 59/2018.

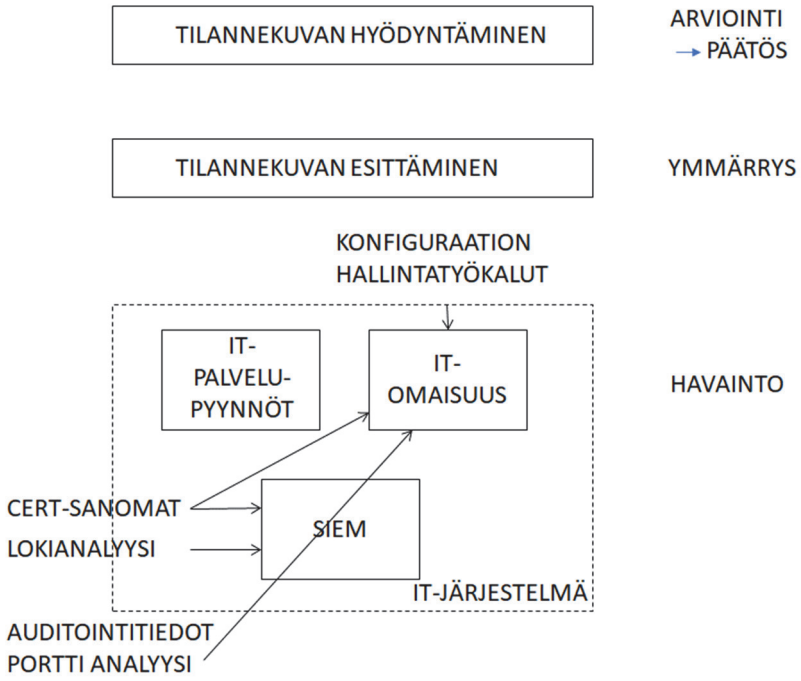
Organisaation kyberturvallisuuden tilannetietoisuuden merkittävimmät haasteet liittyvät monimutkaisten teknillisten järjestelmäkokonaisuuksien haavoittuvuuksien ja toiminnan poikkeamien havainnointiin (Kokkonen, 2016). Väitöstutkimuksen aikana tuli esille, että kriittisen infrastruktuuriin lukeutuva organisaatio pitää tärkeänä ITIL-palvelumallin (Information Technology Infrastructure Library, ITIL) mukaisten tietojärjestelmiensä ja tietovarantojensa reaaliaikaisen tilannekuvan aikaansaamista. Tilannetietoisuuden aikaansaamisen haasteet teollisuusautomaatiojärjestelmästä olivat esillä AaTi-tutkimushakeenn yhteydessä. Kuviossa 13 on esitetty yleistetyllä järjestelmätasolla organisaation tarve tilannekuvan aikaansaamiseksi omista ICT-järjestelmistään (Knowlesa, ym., 2015, muokattu). Tarve jakaantuu kahteen haasteeseen, jotka ovat tilannekuvan tarve ensiksi yritystason ICT-varannoista ja toisaalta teollisuusautomaatiosta. Kuvioon liittyen esimerkiksi terveydenhuollon osalta sairaalajärjestelmät voidaan rinnastaa teollisuuden automaatiojärjestelmiin.




KUVIO 13 Kybertoimintaympäristön rakenne järjestelmätasolla.

**Organisaatiotason ICT-järjestelmät**

Organisaation tietojärjestelmiensä ja tietovarantojensa tietoturvan tilannekuvan muodostaminen on esitetty kuviossa 14. Endsleyn tilannekuvan rakenteen havaintokohteita (Level 1) siinä edustavat tietojärjestelmät ja tietovarannot (Assets), organisaation palvelupyynnöt (Ticket system) sekä Kyberturvallisuuskeskuksen CERT-sanomat ja SOC:n lokianalyysit SIEM-järjestelmän kautta (Security Information and Even Management, SIEM). Tavoitteena on aikaansaada niistä tietoturvaa kuvaava reaaliaikainen ilmaisu. Havainnoista muodostettavan tilannekuvan esittäminen on puolestaan edellytys havaintojen ymmärtämiseen. Tämän jälkeen muodostuvat edellytykset havaintojen mukaisten vaikutusten arvioimiseksi tilannekuvaa hyväksi käyttäen sekä tilannekuvan tulkitsijan tietojärjestelmäkokoonpanon tuntemusta ja teknillistä osaamista hyödyntäen. Lopullisena tavoitteena on luonnollisesti tilannekohtaisten oikeiden päätösten tekeminen ja päätösten mukaisten tietojärjestelmien ja tietovarantojen suorituskykyä ylläpitävien toimenpiteiden ohjaus.




KUVIO 14 Tietoteknillisten järjestelmien tietoturvan tilannekuvan muodostaminen.

Tietojärjestelmiä ja tietovarantoja voidaan hallita konfiguraation hallinnan työkaluilla (Discovery-työkalut). Tyypillisesti niiden avulla saadaan selville tietojärjestelmissä toimivien palomuurien ominaisuudet ja tietojärjestelmissä toimivat palvelut. Organisaation ITIL-palvelumallin mukaisten tietojärjestelmien ja tietovarantojen reaaliaikaisen käyttökokemuksen tilannetieto koostuu niihin kohdistuvista palvelun tukipyynnöistä (Ticket system). SIEM-järjestelmän (Security Information and Event Management, SIEM) avulla puolestaan muodostetaan tilannetietoisuutta tunnetuista uhkatekijöistä (CERT-sanomat, Computer Emergency

Response Team, CERT) ja tarkastelun kohteena olevista tietojärjestelmien lokeista (Lokianalyysi). Jokainen edellä mainituista järjestelyistä tuottaa siis omalta osaltaan tilannetietoisuutta. Lopullisena tavoitteena on aikaansaada näiden tietojen automaattinen yhdistäminen, joka kohdistuu kohdeorganisaation ITIL-palvelujen mukaiseen tietojärjestelmävarantoon.

Organisaation kyberturvallisuuden tietojärjestelmävarantojen (kuvassa 14 IT-omaisuus) konfiguraation ja reaaliaikaisen tilannekuvan aikaansaaminen ovat edellytyksinä edellä mainittujen tietojen yhdistämisellä. Käytännön tasolla tietojen yhdistämisestä on muodostunut haaste ja siten tilannetietoisuuden muodostaminen ja ylläpitäminen voivat olla myös toiminnan jatkuvuuden hallinnan haasteena. CyberTrust-tutkimushankkeessa tehdyn selvityksen (RR4) perusteella voidaan sanoa, että asiaa on tutkittu melko vähän ja käyttökohteeseen sovellettavia tuotteita ei ole markkinoilla tarjolla.

**Teollisuusautomaatio**

Toinen haasteellinen alue liittyy teollisuusautomaatiojärjestelmien kyberturvallisuuden varmistamiseen. Siihen liittyvää tilannekuvan ja tilannetietoisuuden aikaansaamisen haastetta on tutkittu Jyväskylän yliopiston AaTi-hankkeesa, joka käsitteli auton automaatioväylän tietoturvaa (P5). Autojen automaatioratkaisuissa käytetään laajasti CAN-automaatioväylää (Controller Area Network, CAN). CAN-väylä on auton automaatioväylä, joka alun perin suunniteltiin autoihin hajautettujen ohjausjärjestelmien reaaliaikaiseen tiedonsiirtoon, kuten esimerkiksi moottorinohjausyksikön, ABS-jarruyksikköjen ja vaihteistonohjausyksikön väliseen kommunikointiin. (Alanen, 2000).

Myös erilaisissa koneissa ja laitteissa sekä rakennus- ja teollisuusautomaatiossa on hyödynnetty CAN-väylärakennetta. Väylärakenne laajentui digitalisaation yleistyttyä teollisuusautomaatiojärjestelmien sisäisen tiedonsiirron lähiverkkoratkaisuksi. Teollisuusautomaatiojärjestelmien tiedonsiirtoratkaisut ovat myöhemmin kehittyneet CAN-väylän priorisoidun liikenteen rakenteesta kohti väylän jaettuun kommunikaatioon perustuvia pakettipohjaisia lähiverkkoratkaisuja. CAN-väylä on sopivampi käytettäväksi vaativissa reaaliaikasovelluksissa, kuin yhteydelliset protokollat, kuten TCP/IP, vaikka niissä käytettäisiin moninkertaisia nopeuksia (Voss & Comprehensible, 2005).

CAN-väylän normaalista poikkeavan liikenteen ilmaisun haasteet ovat kuitenkin hyvä esimerkki kuvaamaan teollisuusautomaation tilannekuvan haasteita yleisemminkin.

Arbitraatio on CAN-väylämekanismi väyläliikenteen konfliktien ratkaisuun verkon solmujen välillä. Kun verkko on vapaa, mikä tahansa viestisolmu voi aloittaa viestin lähettämisen. Mahdollisen samanaikaisen lähetyksen tapauksessa lähetysjärjestys ratkaistaan bittitason arbitraatiomekanismilla. Arbitraation aikana solmut ovat lähettäneet viestejään samanaikaisesti. Viestin tunnistekentän arvon perusteella voidaan määritellä lähetystä jatkava solmu muiden keskeyttäessä oman viestinsä lähettämisen. Viestit välitetään prioriteettijärjestyksessä. Viestin lähetyksessä sanoman tunnistekentän pienimmällä arvolla on suurin prioriteetti. Tämä tarkoittaa sitä, että jos solmu havaitsee jonkin muun viestin tunnuksen olevan korkeammalla prioriteetilla, niin se luovuttaa lähetysvuoronsa

dominoivaa sanomaa lähettävälle solmulle. Toimintamallia kutsutaan arbitraatioprosessiksi. Käytännössä arbitraatio perustuu siihen, että pienemmän viestitunnisteen omaavilla viesteillä on korkeampi prioriteetti. (Johansson, Törngren, & Nielsen, 2005)

Näiden suunnitteluperiaatteiden pohjalta CAN-väylä muodostui broadcast-tyyppiseksi verkoksi, jossa mikä tahansa solmu voi lähettää viestinsä aina tarvittaessa, sillä kaikki solmut kuuntelevat verkkoa ja reagoivat itselleen merkityksellisiin viesteihin. Viestien läpimenoa ei vahvisteta, koska tämä lisäisi väylän liikennettä. Vastaanottavat verkkolaitteet tarkastavat viestien protokollan mukaisen oikeellisuuden. (Voss & Comprehensible, 2005)

CAN-väylän toimintaperiaatteeseen kuuluu, ettei sen väyläliikennettä erikseen valvota millään tavalla. Toisin sanoen sen ohjausyksiköillä ei ole mekanismeja väärennettyjen viestipakettien havaitsemiseen. Tämän ominaisuuden takia CAN-väylät ovat lähtökohtaisesti alttiita monenlaisille hyökkäyksille mukaan lukien datan väärentäminen, datan luvaton käyttö ja palvelunestohyökkäykset. Auton toiminnallisuudelle tämän tyyppiset hyökkäykset voivat tarkoittaa ajoneuvon järjestelmien hallinnan menetystä, väärää toiminnallisuutta, toimintakyvyttömäksi saattamista tai komponenttien ennenaikaista kulumista. (Carsten, ym., 2015)

Yleisen automaation ja lisääntyvän verkottumisen tarpeen seurauksena CAN-väylän hyökkäysrajapinnat voidaankin tänä päivänä jaotella etäkäytettäviin- ja fyysistä yhteyttä käyttäviin rajapintoihin. Tämän lisäksi eräät tutkijat ovat laajentaneet fyysisten yhteyksien käyttöä rakentamalla koeasetelmia, jotka mahdollistavat man-in-the-middle tyyppiset hyökkäykset väylään. (Lebrun & Demay, 2016)

Ajoneuvoverkkojen on todettu olevan avoimia ja tästä syystä hyökkäysmahdollisuuksia on monella tasolla. Hyökkääjä voi hyödyntää ajoneuvon langattomia yhteyksiä ja tiedonsiirtoväyliä. (Wolf, Weimerskirch & Paar, 2004)

CAN-väylän kyberturvallisuuteen liittyvissä akateemisissa artikkeleissa kerrotut verkkohäiriöiden havainnointimenetelmät voidaan jaotella tilanteisiin, joissa viestiliikenteen kuvaus on tiedossa tai viestiliikenteen profiili tunnistetaan. Edellisessä periaatteessa häiriöiden tunnistus ja niihin reagointi perustuu tunnetuista viestikuvauksista (väyläsanomista) erottuvan poikkeavan liikenteen havainnointiin. Jälkimmäisessä periaatteessa kyseeseen tulevat viestien ajoitukseen, datan semantiikkaan, entropiaan, toistuviin viestisekvensseihin, protokollan oikeellisuuteen tai viestien signaalitason ominaisuuksiin liittyvät havainnointi- ja reagointikeinot. (Johansson, Törngren & Nielsen, 2005; Larson, Nilsson & Jonsson, 2008; Hoppe, Kiltz & Dittmann, 2009; Taylor, Japkowicz & Leblanc, 2015)

AaTi-tutkimuksen pääpaino oli erilaisten häiriöllisten poikkeamien havaitsemismenetelmien kartoittamisessa ajoneuvon automaatioväylästä nauhoitettujen viestien avulla. Tutkimuksen mukaan väylään kohdistuvat hyökkäykset voidaan jakaa hyökkäystavan mukaan kolmeen luokkaan. Ensiksikin voidaan lähettää erikoisviestejä (mm. diagnostiikkaviestejä) tai normaaleja viestejä häirintätarkoituksessa aitojen sekaan tai lähetetään normaaleja viestejä häirintätarkoituksessa. Yleisin tilanne lienee normaaliviestien lähetys, kun aito viestien lähettäjä

on vielä toiminnassa. Tämä pystytään normaalista, aikaväleiltään säännöllisestä liikenteestä, havaitsemaan väyläsanomien aikavälejä tarkkailemalla.

Aluksi tutkimuksessa kokeiltiin neuroverkkoratkaisua viestisisältöjen tunnistamiseen ja sitä kautta tapahtuvaan häiriöiden ilmaisemiseen. Sen avulla toivottiin muodostuvan teknillinen kyky, joka oppii erilaiset viestisisällöt. Tavoitteena oli, että neuroverkko kykenee ennustamaan seuraavan viestin datasisällön edellisten viestien perusteella ja ilmaisemaan poikkeavat viestit. Viestien dataosioiden tarkkailuun rakennettiin neuroverkko artikkelin "Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks" (2016) pohjalta. Neuroverkkoa hyödyntävä menetelmä muodostaa mallin normaalille datavirralle tarkkailemalla väyläliikennettä. Artikkelissa kuvatulla menetelmällä oli saatu rohkaisevia tuloksia. Ajatuksena oli, että poikkeaman tunnistamiseksi voitaisiin käyttää eri metriikoita ennusteen ja viestin eron mittaamiseen, joita on esitelty useita artikkelissa. (Taylor, Leblanc & Japkowicz, 2016)

Tutkimuksessa käytetty neuroverkkoarkkitehtuurin (Long short-term memory –verkko, LSTM) verkon koostui kerroksista solmuista, joissa on takaisinkytkentä, jota on mahdollisuus säännellä. Näin verkolla on 'muisti', mutta se pystyy myös unohtamaan. Suuri osa CAN-liikenteestä on dataltaan säännöllistä ja viestisisällöt muuttuvat vähän kerrallaan yleensä selvien trendien mukaan, joten ennustamisen pitäisi olla ainakin osalle liikenteestä mahdollista. Neuroverkko koulutettiin ennustamaan seuraavan viestin dataosion bitit edellisten viestien databittien perusteella. Sen ongelmaksi nousi kuitenkin tehtävän vaatima laskennallinen suorituskyky ja puutteellinen ennustustarkkuus. Tämän jälkeen tutkimuksessa keskityttiin kokeiluihin, jotka perustuivat väyläsanomien saapumisaikoihin eli niiden ajoituksen perusteella tapahtuvaan häiriötilanteen ilmaisuun.

Väyläsanomien saapumisaikoihin keskittyneessä tutkimusosiossa hyödynnettiin aluksi yhden luokan tukivektorikonetta (One-class Support Vector Machine, OCSVM), joka on variaatio ohjatusta koneoppimismenetelmästä. Menetelmä määrittää rajat normaalin käyttäytymisen ympärille, ja sen ulkopuolelle jäävät viestit luokitellaan poikkeaviksi. Toteutuksessa data-alkiona oli viesti-ikkuna, johon kuului vakiomäärä väyläviestejä. Menetelmässä näistä viesteistä lasketaan tukivektorikoneen luokitteluun käyttämät piirteet, joiden perusteella koko ikkuna todetaan joko normaaliksi tai poikkeavaksi. Piirteinä toteutuksessa käytettiin ikkunan viestien keskiarvointervallia ja intervallien keskihajontaa.

Lisäksi tutkimuksessa selvitettiin saapumisintervallien tarkkailuun soveltuvia muita tekniikoita. Ensiksi esillä oli ydinestimointitekniikka, joka mallintaa viestitunnisteille ominaisen intervallijakauman. Näin saatua jakaumaa voidaan verrata uusiin saapuviin viesteihin häiriöpoikkeamien havaitsemiseksi. Mallinnetusta jakaumasta saadaan intervalleille tiheysfunktio, jonka avulla voidaan laskea luotettavuusarvoja uusille viesteille. Jos laskettu luotettavuus putoaa liian alhaiseksi, on kyseessä poikkeama, josta voidaan antaa hälytys. Koska edellä kuvattu ydinestimointimenetelmä oli laskennallisesti vaativa, eikä kerätyssä datassa havaittu testeissä monihuippuisuutta, päätettiin tehdä yksinkertaistettu menetelmä noudattaen samaa periaatetta. Siinä pyritään mallintamaan viestitunnisteellisten viestien intervallien jakauma, mutta pelkästään tunnusluvuilla.

Näin toteutetulla absoluuttisen poikkeuman menetelmällä saadaan merkittävää suorituskykyetua, eikä kerätyssä datassa saadun tunnistusvoiman pitäisi huonontua. Tätä intervallien jakaumaa päätettiin mallintaa normaalijakaumalla, jolloin se pystytiin kuvamaan kahdella tunnusluvulla; keskiarvolla ja keskihajonnalla. Käytännön ratkaisun koulutusvaiheessa kullekin viestitunnisteelle lasketaan keskiarvo, sekä ala- ja ylärajakynnysarvot viestien luokittelua varten. Dataalkiona käytettiin jälleen viesti-ikkunaa, joka luokiteltiin sen keskiarvointervallin perusteella. Jos ikkunan keskiarvo alitti alarajakynnysarvon tai ylitti ylärajakynnysarvon, luokiteltiin ikkuna poikkeamaksi ja siten häiriöksi väyläliikenteessä.

Kaikissa edellä mainituissa menetelmissä oli haasteina ratkaisujen vaatimat laskennan resurssit ja jossain määrin myös niiden ennustustarkkuuden epäluotettavuus.

Tutkimusosion lopussa edellä kuvattujen tutkimuksesta saatujen kokemusten perusteella päädyttiin kehittämään CAN-väylän häiriöiden tunnistamiseksi väyläsanomien saapumisaikoihin perustuva tilastollisen tarkastelun menetelmä, josta on jätetty patenttihakemus. Menetelmän kuvaus on osa patenttihakemusta. Sen toiminta mallinnettiin tietokoneympäristössä.

AaTi-tutkimuksen tulosten voidaan arvioida olevan yleistettäviä CAN-automaatioväylän muihin käyttökohteisiin. Automaatioväylää on hyödynnetty erilaisissa työkoneissa, laitteissa, kuten lääkinnällisissä laitteissa, meri- ja ilmailuelektroniikassa, sekä rakennus- ja teollisuusautomaatiossa (Lazare, 5).

Cybersecurity and Infrastructure Security Agency, CISA, on yhdysvaltalainen kyberturvallisuudesta vastaava organisaatio. Se on todennut CAN-väylästä, että sitä käytetään laajalti kriittisillä valmistus-, terveydenhuolto-, kansanterveys- ja kuljetusjärjestelmien aloilla. Vuoden 2017 aikana organisaatio on varoittanut väylää käyttäviä tahoja haavoittuvuudesta, joka mahdollistaa sitä onnistuneesti hyödyntäville tahoille fyysisen pääsyn automaatiojärjestelmään ja laajan tietämyksen omaavalle hyökkääjälle mahdollisuuden suunnitella verkkoliikenteeseen DoS-hyökkäyksen, joka häiritsee kohteen toimintaa. Hyökkäyksen vakavuus riippuen siitä, kuinka CAN-väylä on toteutettu kohdejärjestelmässä ja kuinka helposti potentiaalinen hyökkääjä voi käyttää sen tuloporttia (tyypillisesti OBD-II). Tämä hyökkäys eroaa aiemmin ilmoitetuista kehyspohjaisista hyökkäyksistä, jotka yleensä havaitaan IDS / IPS-järjestelmissä. Hyödyntäminen keskittyy väylää hallitseviin sanomabitteihin ja aiheuttaa toimintahäiriöitä CAN-solmuissa oikeiden sanomakehysten lähettämiseen. (CISA, 2017).

# 6 ORGANISAATION TOIMINNAN KEHITTÄMINEN

> Millaisia ja miten kyberturvallisuuden menettelyjä voitaisiin hyödyntää kriittisen infrastruktuurin organisaation kyberturvallisuuden kehittämisessä ja johtamisessa?

Luku 6 muodostaa SSM-tutkimusprosessin vaiheet neljä ja kuusi. Luku 6.1 on johdanto kehitystoimenpiteisiin ja luku 6.2 pitää sisällään organisaation kyberturvallisuuden tavoitetiloja parhaina käytänteinä ja uusien teknologioiden tarkasteluna. Luvussa 6.3 kuvataan organisaation kyberturvallisuuden systeemiajattelua. Luvussa 6.4 kuvataan organisaation kyberturvallisuuden tunnistamisen haasteita. Luvut 6.5 – 6.9 pitävät sisällään kehittämistavoitteita, joilla luvusta 5 johdettaviin kehitystarpeisiin voidaan vastata. Luvussa 6.10 on esitetty malli kehitystoimenpiteiden käytännön implementointiin organisaatiossa.

## 6.1 Johdanto kehitystoimenpiteisiin

Tietojärjestelmien yleinen kyberrakenne on muodostanut tutkimuksen viitekehyksen. Viisikerroksista rakennemallia voidaan pitää organisaation kyberturvallisuuden systeemitason kuvauksena ja siten teknillisen systeemikäsitteen viitekehyksenä organisaation toimintaa ja digitaalisia rakenteita tarkastellessa. Tämän lisäksi johtamisen näkökulmasta tutkimuksessa on kiinnitetty huomiota organisaation kolmelle päätöksentekotasolle kyberturvallisuutta kehitettäessä. Ne ovat strateginen taso, operatiivinen taso ja teknillinen/taktinen taso.

Väitöstyön tutkimustulokset ja taustatutkimukset johtavat pääkysymyksen osalta ajatukseen organisaation kyberturvallisuustoimenpiteiden kehittämiseksi kokonaisvaltaista systeemiajatusta hyödyntämällä. Systeemitason ajattelu mahdollistaa holististien näkökulma muodostamisen organisaaton suojaustoimenpiteistä tutkimuksen viitekehyksen kaikille tasoille. Toimenpiteiden kehittämisessä ja onnistumisessa johtamisen näkökulmat ovat ratkaisevassa asemassa.

Systeemiajatuksen mukaan muodostettava organisaation kyberturvallisuuden kehittäminen koostuu toimenpidejoukosta, jonka lähtökohtana on prosessi

turvallisuusarkkitehtuurikehikon hahmottamiseksi ja sen perusteella optimoitujen toimenpiteiden toteuttamiseksi. Tutkimuksessa esille tuotujen uusien teknisten ratkaisujen kehittäminen mahdollistaa teknillisten suojaustoimeniteiden tehostamisen. Toimenpidejoukkoon lukeutuvat myös riskienhallinta ja tuntemattomiin häiriötilanteisiin varautuminen. Toimintaan voidaan tällöin saavuttaa proaktiivisuutta, ja siten ennalta ehkäistä reaktiivisen toiminnan tarvetta. Systeemitason kyberturvallisuuden havaintokyvyn ja tilannekuvan kehittäminen parantavat tilannetietoisuutta eri päätöksentekotasoilla, ja siten tarvittavien toimenpiteiden reaaliaikaista seurantaa sekä suojaustoimeniteiden optimointia. Tutkimuksessa kiinnittyy myös huomio tilannetietoisuuden haasteisiin. Haasteet korostuvat tilannekuvan ja siten myös tilannetietoisuuden muodostamiseen erityisesti kyberrakenteen teknillisiltä tasoilta. Organisaation henkilöstön kyberturvallisuuteen liittyvät kyvykkyydet ovat ratkaisevassa asemassa tilannetietoisuuden muodostamisessa ja hyödyntämisessä.

## 6.2 Organisaation kyberturvallisuuden tavoitteita

RR8. Pöyhönen J., Lehto M., Lehto M. (2019). Kyberturvallisuus sairaalajärjestelmissä, toiminnan kehittäminen University of Jyväskylä, Faculty of Information Technology, research paper, 75/2019.

RR9. Lehto M., Pöyhönen J., Lehto M. (2019). Kyberturvallisuus sosiaali- ja terveydenhuollossa. Loppuvaportti Vol 2. VFH- ja WHC-hankekokonaisuus. Jyväskylä yliopisto, IT-tiedekunta. Jyväskylä yliopisto, Informaatioteknologian tiedekunta.

### 6.2.1 Toimintaympäristön huomioiminen

Tekniikan nopea kehittyminen perustuu digitalisaation aikaan saamaan ”kierteeseen”, jossa esimerkiksi organisaatioiden erilaiset tuotantoprosessit automatisoituvat ja digitalisoituvat aiempaa laajemmin. Tämä kehityskulku on monissa yhteyksissä nimetty Teollisuus 4.0: ksi. Siihen liittyvät oleellisina osina kyberfyysiset järjestelmät (Cyber-physical system, CPS) ja esineiden tai asioiden internet (Internet of Things, IoT). Kyberfyysinen järjestelmä on järjestelmä, joka verkon avulla yhdistää ohjelmistoja ja fyysisiä laitteita. Ne pitävät sisällään ohjelmistoja, jotka valvovat, ohjaavat ja suojaavat fyysisiä toimintaprosesseja toimilaitteiden avulla. (Sadeghi, Wachsmann, & Waidner, 2015)

Tulevaisuuden uusi teknologinen kehitysvaihe, Teollisuus 4.0:n, mahdollistaa muun muassa älykkäiden sairaaloiden suunnittelun ja toteutuksen. Sama kehityskulku on nähtävissä myös teollisuusautomaatiossa, jossa esimerkiksi erilaisten laitteiden välinen kommunikaatio (Machine to Machine, M2M) tulee lisääntymään. Älykkään alustaratkaisut tulevat edelleen lisäämään kyberhyökkäysmahdollisuuksia ICT-rakenteisiin. Niihin liittyvät myös organisaation oman henkilöstön ja muiden sidosryhmien toiminta yhä monimutkaistuvassa teknilli-

sessä kokonaisuudessa. Toimintaprosessien rakenne tulee näin ollen yhä kompleksisemmaksi kokonaisuudeksi, jolloin erityistä huomiota tulee kiinnittää niiden kyberturvallisuuteen liittyviin ratkaisuihin.

Organisaatioiden toimintaprosessit, niin ydinprosessit kuin tukiprosessitkin, muodostavat operatiivisen toiminnan perustan. Niiden kyberturvallisuutta uhkaavat hyökkääjät, jotka etsivät prosesseista heikkouksia ja pyrkivät siten löytämään väyliä erityisesti teknillisen/taktisen tason järjestelmiin tunkeutumiselle. Teknilliseltä/taktiselta tasolta ovat suorat yhteydet kyberfyysiseen vaikutukseen ja siten myös hyökkäykset voivat aiheuttaa uhkia operatiivisten prosessien toiminnan jatkuvuuteen. Toiminta edellyttää hyökkääjältä usein yksityiskohtaista prosessituntemusta, mikä on avainasemassa sekä hyökkäyksen suunnittelussa, sen toteutusmahdollisuuksien analysoinnissa ja toteutuksessa, ja siten asia on huomioitava suojaustoimenpiteiden toteutuksessa. ENISA pitää raportissaan ”Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends” erityisen tärkeänä tunnistaa organisaation operatiivisella päätöksentekotasolla toimintaprosesseihin kohdistuvat uhkat ja niiden toimintalogiikat (ENISA, 2017).

Digitalisaation nopea kehittyminen on antanut mahdollisuuden organisaatioille tuottaa erilaisia palveluja uusilla tavoilla ja verkostoitua aiempaa laajemmin tietoverkkoja hyödyntämällä. Kehitystä ohjaavat edelleen ratkaisut, jotka ovat osana käynnissä olevaa teknologista kasvua. Siitä on osoituksena esimerkiksi tekoälyn ja esineiden internetin (IoT) käytön jatkuva laajentuminen. Nämä tekniikat tulevatkin lukeutumaan organisaatioiden liiketoimintaprosesseihin ja muihin prosesseihin kiinteästi. Merkittävää on, että tekoälyn ja IoT-laitteiden maailmanlaajuisen käytön lisääntyminen tuottaa ratkaisuja, joissa älykkäät järjestelmät, laitteet ja sensorit kokoavat, välittävät ja hyödyntävät digitalisessa muodossa olevaa tietoa automaattisesti. Erilaisten tietoverkkojen ja niihin kytkeytyvän älykkyyden muodostama kokonaisuus tietovarantoineen aiheuttaa toisaalta myös haasteita organisaation kyberturvallisuuden hallintaan. Siitä esimerkkinä toimivat tilanteet, joissa esiintyy haavoittuvia laitteita ja ohjelmistosovelluksia osana aiempaa laajempaa prosessien verkottunutta toimintaympäristöä ja siten myös osana merkittävää määrää kyberfyysisiä järjestelmiä. Haavoittuvuuksista voi aiheutua vaaratilanteita organisaation koko liiketoimintaan. Toimintaprosessien tilannetietoisuuden ylläpitämisen tarve kasvaa. Kyberturvallisuuden kehittämiseen tulee kiinnittää jatkuvasti huomiota ja sen tulee koskea laajasti eri toimijoita ja sidosryhmiä.

Organisaation kybertoimintaympäristö koostuu jo tällä hetkellä erilaisista ICT-järjestelmistä ja -laitteista sekä niiden käytöstä eri tarkoituksiin muodostuvassa verkottuneessa kokonaisuudessa. Sen tarkasteluun soveltuu systeemiajattelun mukainen lähestyminen. Systeemiajattelu mahdollistaa monimutkaisten ja kompleksisten järjestelmien eri osien (System of Systems) keskinäisten vaikutusten hahmottamisen kokonaisuutena ja sitä kautta organisaation toimintaprosessien seuraamisen ja toiminnan analysoinnin. Edellä kuvattu toimintaympäristön kehittyminen kohti autonomisia artefakteja tukee systeemiajattelun käyttöä organisaatioiden kyberturvallisuuden edistämisessä.

EU:n verkko- ja tietoturvadirektiivin (ns. NIS-direktiivi) tuo velvoitteita kriittisen infrastruktuurin organisaatioille ja niiden toimintaympäristön seuraamiselle. Direktiivin asettamat kyberturvallisuuteen liittyviä velvoitteet painottuvat kriittisessä infrastruktuurissa yhteiskunnan keskeisille palvelujen tarjoajille ja digitaalisten palvelujen tarjoajille. Toimijoita koskevat turvallisuus- ja ilmoitusvaatimukset, joten organisaation toimintaympäristöön kytkeytyy aiempaa laajemmin eri sidosryhmiä. Kyberturvallisuuden varautuminen edellyttääkin yhteiskunnan eri toimijoiden, julkishallinnon ja elinkeinoelämän välistä yhteistyötä, josta seuraa, että digitaalisen toimintaympäristön keskinäisriippuvuudet edellyttävät kyberturvallisuuden huomioivaa kokonaisarkkitehtuuria (Turvallisuuskomitea, 2019). Tällöin tuloksena tulee olla jo organisaatiotasolta muodostettu kyberturvallisuuden arkkitehtuurirakenne, jonka avulla voidaan tukea koko kriittisen infrastruktuurin arkkitehtuurin muodostumista.

### 6.2.2 Parhaita käytänteitä

Standardointijärjestöt laativat standardeja siten, että niissä on huomioitu parhaat käytänteet. Standardisointi on toimintatapojen laatimista tarkoituksena helpottaa viranomaisten, elinkeinoelämän ja kuluttajien toimintaa. Standardisoinnilla lisätään tuotteiden yhteensopivuutta ja turvallisuutta, suojellaan kuluttajaa ja ympäristöä sekä helpotetaan kotimaista ja kansainväistä kauppaa. (Suomen Standardisoimisliitto SFS ry.)

Standardit ja muut erilaiset ohjeet ja suositukset pitävät sisällään sekä yleisiä että toimialakohtaisia parhaita käytänteitä ja tavoitteita. Ne on kehitetty asiantuntijoiden laajassa lausunto– ja konsensusprosessissa. Organisaatiolle niiden käyttö on vapaaehtoista. Ne ovat hyödyllistä organisaatioiden kehittämisessä ja yhteisen toiminnan sopimuspohjana. Kyberturvallisuuden osalta standardit ja ohjeet avustavat käyttäjäänsä muun muassa parannettaessa organisaation toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tällöin toiminnot voivat olla esimerkiksi kyberturvallisuuden johtamisen ja hallinnoinnin tai teknillistä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa tai käyttöä.

Yhdysvaltalaisen NIST-standardin kyberturvallisuuden viitekehys, ”Framework for Improving Critical Infrastructure Cybersecurity” tarjoaa organisaation kyberturvallisuuden kehittämiselle yhteisen kielen, ymmärryksen ja hallinnan sisäisille ja ulkoisille sidosryhmille. Sen avulla voidaan organisaation strategisella ja operatiivisella päätöksentekotasolla tunnistaa ja priorisoida toimia kyberturvallisuuden riskien vähentämiseksi, luoda toimintapolitiikka ja yhdenmukaistaa tekniset lähestymistavat liiketoiminnan jatkuvuuden varmistamiseksi. Organisaatio voi soveltaa standardin periaatteita sekä oman proaktiivisen kyberturvallisuuden kehittämiseen että laajentaa soveltamista tarvittaessa koskemaan myös ulkoisia sidosryhmiään. Toiminnallinen viitekehys loogisesti etenevän joukon toimenpiteitä kyberturvallisuuden kehittämiseksi. Loogisuus muodostuu viitekehyksen neljästä elementistä, jotka ovat toiminto ja sen kategoria, alakate-

goria ja niihin liittyvät informatiiviset viitteet. Oheiseen luetteloon on koottu viitekehyksen kyberturvallisuuteen liittyvät päätoiminnot ja niitä kuvaavat sisällöt: (National Institute of Standards and Technology, 2018, 7-8)

- **Tunnista** - Kehitä organisaation ymmärrystä kyberturvallisuuden riskien hallintaan.
- **Suojaa** - Kehitä ja toteuta asianmukaiset suojatoimet toimintaprosessien varmistamiseksi.
- **Havaitse** - Kehitä ja toteuta asianmukaiset toiminnot kyberturvallisuustapahtumien tilannetietoisuuteen.
- **Vastaa** - Kehitä ja toteuta asianmukaiset toiminnot toimintaprosessien jatkuvuuden hallintaan.
- **Palaudu** - Kehitä ja toteuta asianmukaiset toiminnot, joilla voidaan palauttaa kyvykkyydet tai palvelut, jotka olivat heikentyneet kyberturvallisuustapahtuman vuoksi. Laadi suunnitelmat, joilla ylläpidetään sietokykyä.

Viitekehyksen kyberturvallisuuden kategoriat ovat päätoimintojen osa-alueita, jotka ovat edelleen jaettavissa alakategorioihin. Kategorioita ovat esimerkiksi ”pääsyn hallinta” tai ”tunnistusprosessit, tunnistus, tunnistaminen ". Ne puolestaan jakaantuvat edelleen teknillisiin kohtiin ja/tai hallintatoimintaa. Informatiiviset viitteet puolestaan ovat standardien ja ohjeiden osia, jotka ovat parhaita käytänteitä kyseseisin kohdan tarkasteluun.

ENISA suosittaa tarkastelemaan kyberturvallisuuden hyviä käytänteitä organisaatiotason ja teknillisen tason näkökulmista. Organisaatiotasolla näkökulmat ovat: (ENISA, 2016, 46-48)

- Kyberturvallisuuden hallinto
- Riskienhallinta
- Toiminnan vaatimustenmukaisuus

Teknillisellä tasolla näkökulmat ovat: (ENISA, 2016, 49-50).

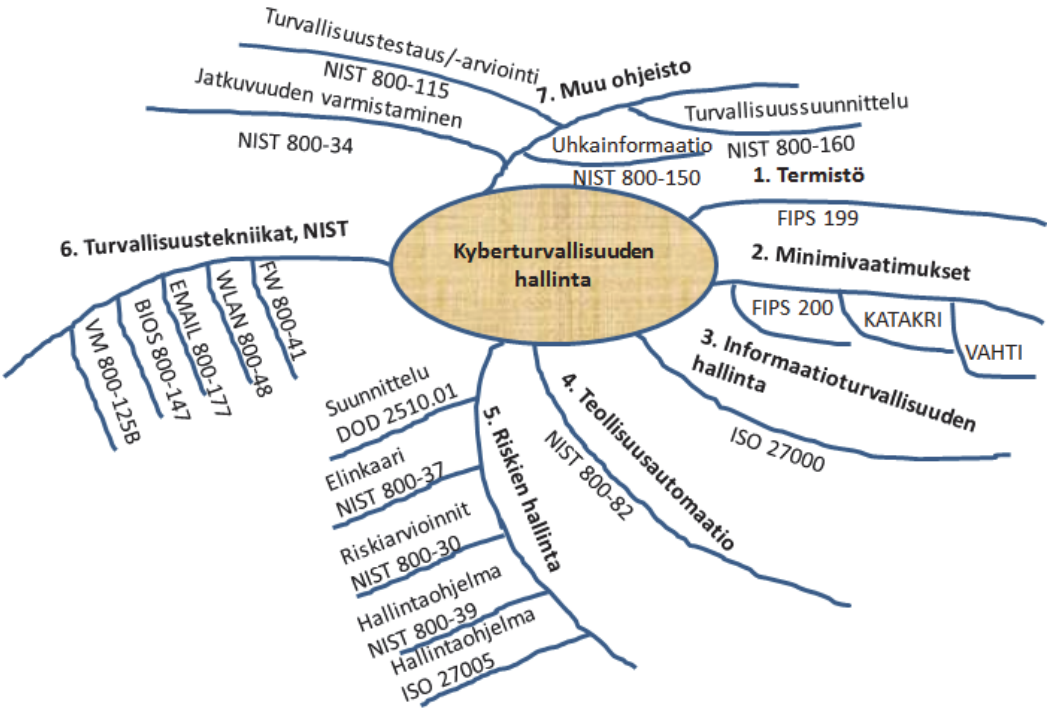
- Kyberturvallisuusarkkitehtuuri ja suojaustoimenpiteet
- ICT-omaisuuden suojaus
- Datan suojaaminen
- Mobiililaitteiden turvallisuus

Lisäksi ENISA suosittaa teknillisinä parhaina käytänteinä kiinnittämään huomiota verkon segmentointiin, valvontaan ja tunkeutumisen havainnointiin, salaukseen sekä käytön autentikointiin ja valtuutukseen sekä kiinnittämään erityistä huomiota konkreettinen häiriötilanteiden toiminta- ja palautumissuunnitelmiin. (ENISA, 2016, 53)

Toimintamenetelmien ja erilaisten teknillisten ratkaisujen lisäksi organisaation kyberturvallisuutta voidaan lisätä kehittämällä henkilöstön toimintavalmiuksia. Parhaina käytänteinä tässä yhteydessä toimivat erilaiset työpajat, kokoukset, konferenssit ja harjoitukset. Organisaatioiden on kehitettävä kyberosaamisohjelmia kouluttaakseen toimintaketjujensa päätöksentekijöitä. (Csulak, ym., 2017, 40)

Väitöstutkimukseen liittyvien taustatutkimusten (RR6, RR7) haastattelujen perusteella voidaan todeta, että useiden organisaatioiden kyberturvallisuuteen liittyvää toimintaa leimaa edelleen häiriötilanteisiin reagoiva toimintatapa. Reagoiva toimintatavassa häiriötilanteissa toimitaan usein vajaan tilannetiedon varassa, toimintaan kuuluvat nopeat päätelmät ja kiireelliset toiminnan jatkuvuuteen tähtäävät toimenpiteet. Kyberturvallisuuden kehittäminen parhaita käytänteitä hyödyntäen edistetään organisaatiossa erityisesti proaktiivista toimintaa. Standardeja, ohjeina ja suosituksina voidaan käyttää parhaina käytänteinä organisaation kyberturvallisuuden kehittämisessä. Kybertoimintaympäristössä ne avustavat käyttäjäänsä kehitettäessä organisaation toimintojen luotettavuutta, toiminnan jatkuvuutta, laatua, riskienhallintaa ja varautumista. Toiminnot liittyvät strategisella ja operatiivisella päätöksentekotasolla kyberturvallisuuden johtamiseen ja hallinnointiin sekä teknillisellä/taktisella päätöksentekotasolla tietojärjestelmien, tietoverkkojen ja palvelujen kehittämiseen, ylläpitoon ja käyttöön.

Kuvioon 15 on koottu luettelonomaisesti eräitä keskeisimpiä kyberturvallisuuden hallintaan liittyviä kansallisia ja kasainvälisiä suosituksia, ohjeita ja standardeja, jotka tukevat myös NIST-standardin kyberturvallisuuden viitekehyksen mukaisia kehittämisprosesseja, ENISA:n suosituksia ja henkilöstön huomioimista. Kuviossa ne on luokiteltu seitsemään eri kokonaisuuteen niiden käyttötarkoituksen havainnollistamiseksi kyberturvallisuuden kehitystyössä.




KUVIO 15 Kyberturvallisuuden hallintaan liittyviä keskeisiä normeja.

Liitteessä 2 on lyhyet kuvaukset kuviossa mainituista standardeista ja ohjeista. Niitä on myös hyödynnetty soveltuvilta osiltaan tässä väitöstutkimuksessa.

### 6.2.3 Uudet teknologiat

Uusi käynnissä oleva teknologinen vallankumous, Teollisuus 4.0 (Industrial 4.0), muuttaa erityisesti valmistavan teollisuuden toimintaa. PricewaterhouseCoopersin (PwC) vuoden 2016 selvityksen mukaan yli 80 % yrityksistä uskoo data-analytiikalla olevan viiden vuoden kuluessa merkittävä vaikutus päätöksentekoon ja operatiiviseen toimintaan. Data-analytiikka mahdollistaa saada tietoja muun muassa tuotteiden käytöstä, laitteiden toiminnasta tai sen avulla voidaan edistää pitkäkestoisia asiakassuhteita. Tulosten avulla tuotteita voidaan kehittää asiakastarpeen mukaan ja niiden oheen voidaan tuoda personoituja palveluita. (PricewaterhouseCooper, 2016, 23)

Digitalisaation yhteydessä on tullut esiin tietoverkkojen kautta tapahtuva vaikuttaminen fyysisen maailman toimintaan. Teknillinen järjestelmä, joka mahdollistaa toiminnan on määritelty kyberfyysiseksi järjestelmäksi, jossa yhteen liitetyt ohjelmistot kontrolloivat fyysisiä laitteita. Kyberfyysiset järjestelmät ovatkin ohjelmistoalustoja, joilla valvotaan, ohjataan ja suojataan toimintaprosesseja (Sadeghi, Wachsmann & Waidner, 2015, 1 - 2). Nämä ohjelmistoalustat tarvitsevat myös palvelimia ja muita laitteistoja, jolloin kokonaisuudesta muodostuu eräänlainen digitaalinen toiminta-alusta, jonka kehitystä sanelee edellä mainittu teollinen vallankumous – Teollisuus 4.0.

Väitöstyöhön liittyvien taustatutkimuksien (RR6, RR7) haastatteluissa tuli esille, että parhaimmillaan organisaatioilla on käytössään korkeatasoisia kyberturvallisuuspalveluja ja teknillisiä ratkaisuja. Toisaalta systeemien monimutkaisuus ja kompleksisuus edellyttävät kyberturvallisuusjärjestelmien jatkokehittämistä siten, että niissä on kyky tunnistaa organisaatiolle kohdistuvat ulkoiset ja sisäiset uhat, ja joihin on rakennettu kokonaisvaltainen turvallisuusjärjestelmä älykkyyttä sisältävän kyberturvallisuusarkkitehtuurin kautta. Uusia keinoja uhkien paljastamiseen ja uhkilta suojautumiseen tarvitaan, sillä organisaatiohin voi kohdentua jopa 200 000 tietoturvatapahtumaa päivässä SOC-toiminnan ilmaisemana.

Organisaation toimintaan kohdistuvien tietoturvatapahtumien seuranta ja tarkistaminen ihmistyönä on mahdotonta. Tekoälyyn perustuvia ratkaisuja voidaan hyödyntää ihmistyö apuna, koska sen avulla voidaan käsitellä käytännössä reaaliajassa suuri määrä tapahtumia ja tarvittaessa verrata hetkessä satoja tuhansia asiakirjoja ja tietolähteitä ongelmien ratkaisemiseksi. Tekoälyavusteisilla integroiduilla ratkaisuilla voidaan tavoitella myös aikaisempaa parempaa näkyvyyttä ICT-järjestelmien ja – laitteiden rakenteisiin, jolloin kyberhyökkäyksiltä suojautuminen ja vastatoimet voidaan rakenteissa toteuttaa kokonaisuutena eikä yksittäisinä erillisinä toimenpiteinä. Esimerkkinä tekoälyn käytöstä edellä mainittuun tarkoitukseen voidaan käyttää yhdysvaltalaisen teknillisen korkeakoulun MIT:n (Massachusetts Institute of Technology, MTI) tutkijoiden ja koneoppimiseen erikoistuneen yrityksen, PatternExin, yhteistyössä kehittämää tekoälyalustaa. Alusta voi ennustaa kyberhyökkäyksiä automaation avulla saatuja ja

yhdistää löydöksiä asiantuntijoiden tietoihin (Veeramachaneni, 2016, 49). Ratkaisun avulla on voitu havaita kyberhyökkäyksiä 85 %: todennäköisyydellä Conner-Simons, 2016)

Tekoälyn ohella mielenkiitoinen tekniikka-alue on virtualisointi. Virtualisointitekniikka mahdollistaa useiden käyttöjärjestelmien tai sovellusten yhtäaikaisen käytön samassa ICT-palvelinalustassa. Kyberturvallisuuden näkökulmasta tarkasteltuna tekniikan avulla voidaan suojautua tai puolustautua kyberhyökkäyksiä vastaan käyttämällä osoitealueita, joita alustan peruskäyttöjärjestelmässä ei ole käytettävissä. Lähtökohtaisesti virtualisointi on kehitetty optimoimaan tietokoneiden käyttöastetta ja laskentaresurssien käyttöä. Tietokoneiden arkkitehtuurin takia ne voivat suorittaa vain yhtä käyttöjärjestelmää ja sovellusohjelmaa kerrallaan. Virtualisointi mahdollistaa useiden käyttöjärjestelmien ja sovellusohjelmien toiminnan yhdellä fyysisellä palvelimella, jolloin jokainen itsenäinen virtuaalitoiminto on eristetty muista toiminnoista. Tekniikassa hyödynnetään niin kutsuttuja virtualisointikomentoja, joilla käyttöjärjestelmä siirretään virtuaalikoneeksi (on-the-fly) ja lisäksi luodaan ”hypervisor” (tai Virtual Machine Monitor, VMM), joka ohjaa laitteita. ”Hypervisor” voidaan määrittää tarttumaan poikkeaviin tapahtumiin. (Zaidenberg, 2017, 135)

Tulevaisuuden Teollisuus 4.0 ympäristössä liikkuu valtava määrä dataa siihen integroitujen eri osien välillä. Toiminta asettaa tietojen salattavuudelle erikoisvaateita muun muassa siksi, että voidaan varmistaa organisaation aineettoman omaisuuden suojaaminen, sekä tiedon luottamuksellisuus, käytettävyys ja eheys. Kyberturvallisuuden edistäminen edellyttää salausteknisten ratkaisujen ja – algoritmien siirtämistä kokonaisuudesta muodostuvan integroidun alustan tapauksessa toiminnallisuudeksi. Haasteeksi muodostuu salaisten tietojen käytettävyys. Asiaan liittyy ainakin seuraavia näkökulmia ja ominaisuuksia: (Heitmann, 2017, 1)

- Alkuperäisten tietojen muuttaminen.
  - anonymisointi ja sekoittaminen - runsaasti hyötyjä ja vähän suojaa
- Alkuperäisten tietojen peittäminen ennen käsittelyä.
  - käytettävyyden menettäminen - vaikea hyödyntää monenkeskisesti
- Salaisen tiedon käyttäminen sellaisenaan laskennassa (ilman salauksen purkamista).
  - pieni käytettävyyden menetys - hidas käsittely laskennassa (monimutkainen)
- Lohkoketjutekniikan hyödyntäminen.
  - tarjoaa laajassa mitassa luotettavuutta

Data suojausta kehitettäessä on sen käsittelyyn osallistuvien osapuolten toimintaprosesseissa huomioitava seuraavia toimenpiteitä: (Heitmann, 2017, 1)

- Luodaan toimintamallit salatun datan käsittelyyn.
- Toimintamallit salataan ja jaetaan salattuina osallistujaosapuolille.
- Osallistujaosapuolet käyttävät salattua toimintamallia vain omassa toiminnassaan.

- Toimintamallien kehittäminen suojataan.
- Toimintamalleja ei anneta ulkopuolisten käyttöön.

Tekoälyyn perustuvien haittaohjelmistojen aiheuttamia kyberhyökkäyksiä ICT-infrastruktuuria vastaan on odotettavissa jatkossa yhä enemmän. Ne ovat perinteisiä hyökkäysmuotoja epäsymmetrisempiä verrattuna kyberpuolustukseen. Tulevaisuuden haasteet liittyvät siihen, miten voidaan kehittää vastaavasti tekoälyyn pohjautuvia suojausmenetelmiä. Henkilöstön kyberturvallisuuteen liittyvän kyvykkyyden kehittäminen pätee edelleen yhtenä keskeisenä suojaustoimintona myös tekoälyn muodostamassa uhkassa. Henkilöstön kyvykkyyttä kehittää hyvä koulutus (käyttäjät, ICT-henkilöstö). Prosessien kyvykkyyttä kehittää se, että organisaation toiminnassa sovelletaan kehittyneimpiä ja parannettuja turvallisuusmenetelmiä (ml. toimintapolitiikka). Teknillistä kyvykkyyttä kehitetään lähdekoodin laatua ja läpinäkyvyyttä parantamalla sekä huolehtimalla ohjelmistopäivityksistä. Henkilöstön jatkokoulutuksessa ja osaamisessa tulee huomioida erityisesti Teollisuus 4.0 tekniikoiden muodostama toimintaympäristö. (Destre, 2017.)

Teollisuus 4.0 ympäristössä esiintyvistä erilaisista digitaalisignaaleista ja -sanomista on mahdollista kehittää toimintaprosessien kunnonvalvonta, jolloin sitä voidaan hyödyntää myös kyberhyökkäysten havainnoinnissa. Siinä prosessimallin kuvaus muuttujineen, signaalien ja sanomien analyysitiedot voivat muodostaa johtopäätösten perustan. Kyberturvallisuuden kannalta erityisesti langattomiin yhteyksiin pohjautuvien mitta-anturin ja vastaavien muiden langattomien yhteyksien toiminnan mallinnukseen perustuvan vianhavaitsemiskyky on erityisen kiinnostava kehitysalue. Toimintaprosessien vikadiagnosointia voidaan käyttää kyberhyökkäyksien havainnointiin mitta-antureissa ja toimilaitteissa muodostavien tietojen perusteella esimerkiksi tekoälyä hyödyntämällä. (Dai, 2017)

## 6.3 Systeeminäkökulman kehittäminen

Miten organisaation kyberturvallisuuden systeeminäkökulma voidaan rakentaa?

P6. Pöyhönen, J., Lehto M., (2020) Cyber security; Trust based architecture in the management of an organization security. ECCWS 2020: Proceedings of the 19th European Conference on Cyber Warfare and Security. Artikkeli hyväksytty 28.4.2020.

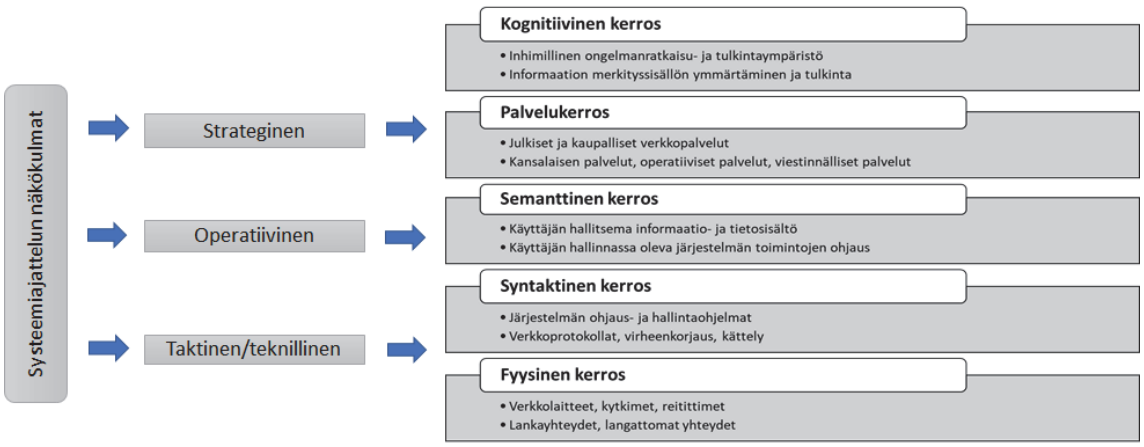
Organisaation kyberturvallisuusstrategian toteutusarkkitehtuurin mallintamista käsittelevässä artikkelissa ”Cyber Security Strategy Implementation Architecture in a Value System” (Kuusisto & Kuusisto, 2018) painotetaan organisaation strategisen, operatiivisen ja taktisen tason toimenpiteitä kattavan implementoinnin toteutuksessa. Myös kirjassa ”Kyberturvallisuus” (Limnéll, Majewski & Salminen, 2014) todetaan, että organisaation kyberturvallisuuden kattava rakentaminen edellyttää toimenpiteitä strategisella, operatiivisella ja teknillisellä/taktillisella tasolla. Nämä organisaation päätöksenteon näkökulmat ovat väitöstyössä yhdistetty kyberrakenteeseen eli tutkimuksen viitekehykseen myöhemmin alla

kuvatulla tavalla. Kokonaisuus pitää sisällään väitöstyön systeemiajattelun perusteet.

Organisaation kyberturvallisuuden systeemitason suojauksen kehittämisen lähestymistä voidaan tarkastella organisaation päätöksentekotasoittain seuraavasti:

1. Strategisen päätöksentekotasolla haetaan yhdistelmä toimenpiteitä, joilla vastataan kysymykseen ”Miksi kyberturvallisuutta on organisaatiossa edistettävä?” Samalla haetaan organisaation ylimmän johdon sitoutuminen kyberturvallisuuden edistämiseen. Sitoutuminen puolestaan mahdollistaa toimenpiteiden toteutuksen ja resursoinnin.
2. Operatiivisella päätöksentekotasolla toimenpiteiden ensisijaisena tarkoituksena on organisaation toimintaprosessien jatkuvuuden varmistaminen. Tällöin haetaan ratkaisuja, joilla vastataan kysymykseen ”Mitä pitää suojata?”. Tällöin päätökset kohdistuvat ensisijaisesti toimintaprosessien riskitasojen tunnistamiseen ja riskien hallintaan. Riskienhallintaprosessiin liittyvät toimenpiteet niin kumppaneiden kuin oma organisaation sidosryhmien kesken.
3. Teknillisellä/taktisen päätöksentekotason toimenpiteiden voi katsoa painottuvan käytännön ICT-järjestelmien ja -laiteiden toiminnan sekä niiden käytön suojaukseen. Tällöin ratkaisuja haetaan kysymykseen ”Miten suojaudutaan?”. Lähtökohtana voidaan pitää suojattavien prosessien ja sitä kautta laitteiden ja järjestelmien tunnistamista sekä kykyä ymmärtää ja hallita niiden kyberturvallisuusriskejä tekniikkaan ja käyttöön liittyvillä käytännön suojaustoimenpiteillä. Toimenpiteet kohdistuvat suojaustekniikkaan ja -palveluihin. Henkilöstön kyvykkyys toimia taktisella tasolla on myös suojautumisessa ratkaisevan tärkeää. Uusilla teknillisillä ratkaisuilla voidaan edistää erityisesti teknillisen/taktisen tason suojausta.

Kuviossa 16 on systeemiajattelun näkökulmat liitettynä organisaation kyberrakenteeseen ja siten on muodostettu systeemitason näkymä organisaation kyberturvallisuuteen.




KUVIO 16 Systeemitason näkymä organisaation kyberturvallisuuteen.

## 6.4 Kyberturvallisuusuhkien tunnistamisen haasteet

Häiriötapauksissa kybertoimintaympäristön ominaisuuksiin kuuluu niiden kehittyminen suurella nopeudella ja vaikutuksiltaan laajakantoisesti. Organisaation kybertoimintaympäristö muodostuu teknillisesti monimutkaisista rakenteista ja laajasti verkottuneista sidosryhmistä, jolloin kokonaisuudesta muodostuu kompleksinen. Sen toiminnan täydellinen ennakointi on mahdotonta. Häiriötapauksissa niiden laajuuden selvittäminen sekä korjaavien toimenpiteiden aikaan saaminen saattavat kestää pitkään, mikä voi johtaa häiriön selvittämiseen tarvittavan ajan kasvamiseen ja toimintaprosessien käytettävyyden romahtamiseen. (Kuusisto, 2018).

Kansallisen kyberturvallisuuden johtamista käsitelleen tutkimuksen ”Kyberturvallisuuden strateginen johtaminen Suomessa” tutkimushaastatteluissa tuli esille organisaatioiden haasteet häiriötilanteisiin johtavien ilmiöiden tunnistamisessa ja niihin reagoimisessa. Samoja haasteita todettiin myös aiemmassa tutkimuksessa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”. Kyseisen tutkimuksen mukaan häiriöiden tunnistamiseen vaikuttavat erityisesti tapahtumien hektisyys ja järjestelmien kompleksisuus. Myös eri kyberhyökkäysmuotojen ja haittaohjelmien tunnistamisessa on haasteita. Kybertoimintaympäristölle on leimallista muutosnopeus, mikä edellyttää suojaustoimien osalta nopeaa reagointikykyä – ketteryyttä, sekä varautumista myös tilanteisiin, joita ei täysin kyetä ennakoimaan. Tavoitteellisessa kyberturvallisuuden johtamisessa ilmentyy kolme tekijää, jotka ovat: strateginen herkkyys, resurssien joustavuus ja johtamisen yhtenäisyys. (Lehto, ym. 2017; Lehto, ym. 2018)

Toiminnan epävarmuuden tarkastelu voidaan perustaa tapahtumien esiintymisen todennäköisyyteen (tiedossa tai tuntematon) ja sen vaikutuksen (tunnettu tai tuntematon) arviointiin. Tarkastelu johtaa neljään mahdollisuuteen tapahtumien suhteen, jotka ovat: (Kim, 2012).

- Tunnetut (tietämys),
- Tuntematon - tiedetään (vaikutus ei ole tiedossa, mutta olemassaolo on tiedossa),
- Tunnetut tuntemattomat (riskit) ja
- Tuntematon - tuntemattomat (epämääräinen, epävarmuus).

Tunnistamattomat riskit, joita kutsutaan myös tuntemattomiksi tuntemattomiksi (Unknown, Unknown), jäävät riskienhallinnan ulkopuolella, koska niitä on mahdotonta etsiä tai kuvitella etukäteen.

Organisaation kyberturvallisuuden hallinnan kehittämisessä voidaan luokitella toimenpiteet edellä kuvatun luettelon jakoa noudattaen taulukon 10 mukaisesti.

TAULUKKO 10 Organisaation kyberturvallisuustoimenpiteiden luokittelu.

| **Kyberuhan tietoisuus** | **Kehitystoimenpide** |
|---|---|
| Tunnetut (tietämys), | Systeemitason suojaustoimenpiteet |
| Tuntematon - tiedetään (vaikutus ei ole tiedossa, mutta olemassaolo on tiedossa) | Systeemitason suojaustoimenpiteet |
| Tunnetut tuntemattomat (riskit) | Systeemitason riskitarkastelu |
| Tuntematon - tuntemattomat (epämääräinen, epävarmuus) | Systeemitason varautuminen, resiliessin kehittäminen |

Systeemitasolla kyberturvallisuuden toimenpiteet käsittävät organisaation kyberrakenteen hahmottamisen eli holistisen käsityksen muodostamisen kohteen fyysistä ICT-varannoista aina kognitiiviselle tasolle asti tutkimuksenviitekehyksen mukaisesti. Hahmottamisen avuksi on (luku 6.5) muodostettu ensiksi kohteen arkkitehtuurikehikko eri näkökulmineen ja sen jälkeen voidaan tunnistaa näkökulmien mukaan toimenpiteitä kattavasti organisaation eri tasoille toteutettavaksi.

Systeemitason suojaustoimenpiteet voidaan suunnitella ja toteuttaa kyberturvallisuuteen vaikuttavien tunnettujen uhkin kautta. Organisaation osalta uhat voivat olla tunnettuja siten, että joko niiden vaikutukset kohteen osalta tunnetaan, tai vaikutuksia ei tunneta. Molemmissa tapauksissa suojaustoimenpiteet voidaan muodostaa samalla periaatteella.

Systeemitason riskitarkastelu täydentää organisaation arkkitehtuurikehikon ja systeemiajattelun kautta ohjautuvia toimenpiteitä. Se on organisaation toimintaprosessien jatkuvuuden hallinnan toinen ulottuvuus ja vastaa organisaation tilanteeseen, jossa kyberturvallisuuden uhkat tiedostetaan, mutta ei tiedetä tarkasti niiden olemassaoloa prosesseissa eikä vaikutusta toimintaan. Riskitarkastelu mahdollistaa riskitekijöiden ja suojaustoimenpiteiden luokittelun riskien pienentämiseksi tai välttämiseksi. Riskejä voidaan myös siirtää toisen tahon hoidettavaksi joko ulkoistamalla joitakin prosesseja tai osatoimintoja esimerkiksi paremman kyberosaamisen hyödyntämiseksi. Toimintaa voidaan myös vakuuttaa. Riskitarkastelussa toimintaan voi jäädä riskejä, joita kutsutaan jäännösriskeiksi.

Organisaation kybertoimintaympäristön kompleksisuus ja sitä kautta mahdollisesti muodostuva tapahtumien tuntemattomuus ja ennakoimattomuus jättää toimintaan riskejä, joita ei tunneta eikä voida ottaa riskitarkastelussa huomioon. Toiminnan epämääräisyys ja epävarmuus korostuvat. Organisaation suojaustoimenpiteiden ja riskitarkastelun lisäksi tarvitaan ennakoimattomaan tilanteeseen vastaamiseksi systeemitason varautumissuunnittelua. Varautumissuunnittelu parantaa organisaation resilienssiä. Se on myös kyberturvallisuuden toimenpiteiden kolmas ulottuvuus, jolla voidaan vastata toimintaprosessien jatkuvuuden hallintaan.

## 6.5 Kyberturvallisuusarkkitehtuurin muodostaminen

Miten organisaation kyberturvallisuuden arkkitehtuuri voidaan muodostaa?

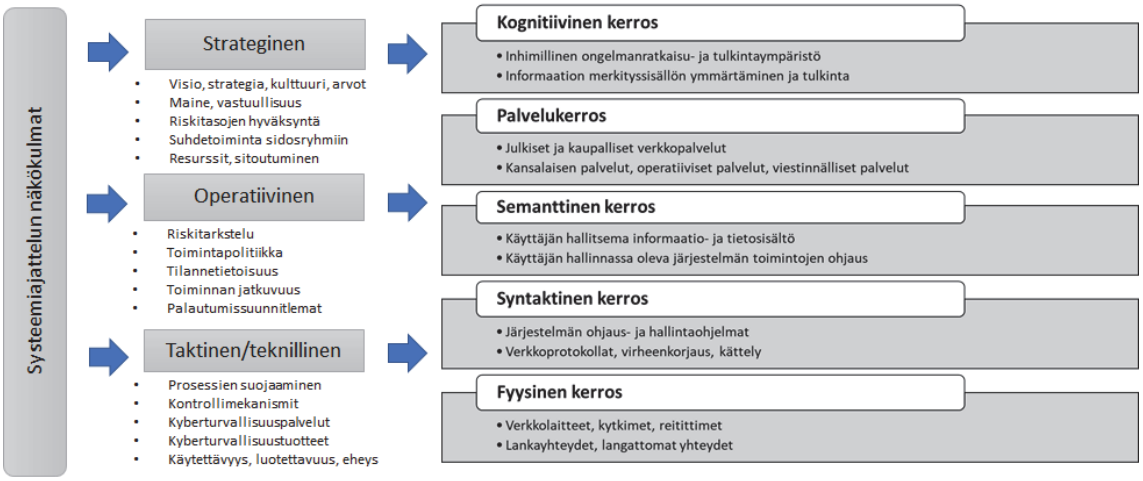
P6. Pöyhönen, J., Lehto M., (2020) Cyber security; Trust based architecture in the management of an organization security. ECCWS 2020: Proceedings of the 19th European Conference on Cyber Warfare and Security. Artikkeli hyväksytty 28.4.2020.

Suomen kyberturvallisuusstrategiassa 2019 todetaan kyberturvallisuusarkkitehtuurin tarpeesta seuraavasti: (Turvallisuuskomitea, 2019)

> ”Digitaalisen toimintaympäristön keskinäisriippuvuudet edellyttävät kyberturvallisuuden huomioivaa kokonaisarkkitehtuuria.”

Systeemiajattelu mahdollistaa organisaation kyberturvallisuuden kokonaisvaltaisen, holistisen, tarkastelun. Organisaation kyberturvallisuusarkkitehtuurin muodostaminen on osaltaan edistämässä edellä mainittua strategian tavoitetta.

Kyberturvallisuuden systeemiajattelun kautta on saatu kokonaisvaltainen näkymä organisaation kyberturvallisuuteen. Kun siihen yhdistetään kyberluottamusta lisääviä toimenpiteitä (Kuvio 3), niin voidaan muodostaa kyberturvallisuusarkkitehtuurin kehikko. Kehikon toimenpiteiden toteutukseen voidaan käyttää standardeista esimerkiksi menettelyjä organisaation riskienhallintaa ohjaavasta standardista, NIST 800-39 (2011), ISO/IEC 9000-laatustandardin seitsemää perusperiaatetta (Suomen Standardisoimisliitto ry., 2016) ja ISO/IEC 27000-informaatioturvallisuuden standardin keskeisimpiä pääkohtia (Suomen Standardisoimisliitto ry., 2012). Kuviossa 17 on esitetty näkökulmat organisaation kolmella eri päätöksentekotasolla, niihin liittyvät toimenpiteet ja kyberrakenne.




KUVIO 17 Organisaation kyberturvallisuusarkkitehtuurin kehikko.

Organisaation kyberturvallisuuteen liittyvällä kyvykkyydellä tuetaan arkkitehtuurikehikon toimenpiteitä. Arkkitehtuurikehikko pitää sisällään myös organisaation toiminnan jatkuvan parantamisen aihioita.

ISO/IEC 9000-standarin suosittelema PDCA-kehitysmenetelmä on dynaaminen neljään vaiheeseen jaksotettu kehitystyökalu, joka voidaan soveltaa kehitystoimenpiteiden implementoinnissa. Siinä yhdistyvät suunnittelu, toteutus, valvonta ja jatkuva parantaminen. (9001 quality., 2020)

Organisaation toteuttama toiminnan ja tavoitteiden visiointityö antaa mahdollisuuden tarkastella sen asemoitumista toimintaympäristöönsä. Se on myös osa strategiatyötä. Kyberturvallisuuden tavoitteiden ja kehittämisen perusteet voidaan liittää tähän työhön. Johdon laatima visiointi tulevaisuudestaan ja asemoitumisestaan siinä luo perustan toiminnan kehittämiseksi. Visiointityön kautta muodostettu näkökulma muutetaan strategisiksi tavoitteiksi, operatiivisen tason toimenpiteiksi, ohjeiksi ja toteutuspolitiikaksi. Teknillisellä/taktisella tasolla toteutetaan strategiasta johdettuja käytännön toimenpiteitä. Toimenpiteiden onnistumisen mahdollistavat organisaation kyvykkyystekijät. NIST-organisaation (National Institute of Standards and Technology, NIST) ohje "Framework for Improving Critical Infrastructure Cybersecurity" huomioi alla olevan näkökulmajaon organisaation toiminnan kehittämisessä. (National Institute of Standards and Technology, 2018)

### 6.5.1 Strateginen näkökulma

Kansallisen kriittisen infrastruktuurin suojaaminen ja siitä johdettavissa olevat ylätason suoritusvaatimukset antavat perusten kunkin organisaation strategiatyölle. Organisaation kyberturvallisuutta ja luottamusta lisäävät toimenpiteet kytkeytyvät siten myös suojattavaan kokonaisuuteen ja ohjaavat sen omia toimenpiteitä luottamuksen jatkuvaan kehittämiseen ja ylläpitämiseen osana kriittistä infrastruktuuria. Strategiset valinnat liittyvät luontevasti kansalliseen vastuuseen, organisaation maineen hallintaan, luottamuksen ylläpitämiseen, prosessien toiminnan ja jatkuvuuden varmistamiseen. Johdolta edellytetään konkreettisia strategisia valintoja sekä valittujen toimenpiteiden suorittamisen tukemista ja ohjaamista läpi koko organisaation. Johdon tärkeimpinä tehtävinä ovat organisaation riskitasojen hyväksyntä, huolehtia toimenpiteiden riittävästä resursoinnista sekä tarvittavien kehitystoimenpiteiden läpivienti. Valituista toimenpiteitä tulee viestittää kattavasti organisaation henkilöstölle ja muille sidosryhmille. Kyberturvallisuuden kytkeminen organisaation arvoihin tukee turvallisuuskulttuurin kehittymistä.

### 6.5.2 Operatiivinen näkökulma

Operatiivisen tason toimenpiteillä mahdollistetaan strategisten tavoitteiden toteuttaminen. Organisaation kyberturvallisuuden kehittäminen ja toimintaprosessien luottamusta lisäävät toimenpiteet edellyttävät kokonaisvaltaista kyberturvallisuuden hallintaa, joka perustuu prosessiriskien tunnistamiseen, analysointiin ja rikien käsittelyyn. Organisaation ylimmän tason tehtävänä on linjata

hyväksyttävät riskitasot. Operatiivisella tasolla toteutetaan riskien pienentämiseen liittyviä toimenpiteitä muun muassa toimintapolitiikan avulla. Organisaation on siten tärkeää julistaa ja viestittää toimintapolitiikkaa, jolla johto sitoutuu toiminnan kehittämisen edellyttämiin toimenpiteisiin. Kyberturvallisuutta edistävien toimintatapojen kehittäminen voidaan yhdistää organisaation yleiseen toimintapolitiikkaan operatiivisella tasolla. Operatiivisen tason konkreettiset käytännön toimenpiteet tulee ohjata tietoturvaratkaisujen varmistamiseen riskiperusteisesti sekä organisaation toiminnan jatkuvuus- ja toipumissuunnitelmien laadintaan. Tavoitteena tulee olla toimintaprosessien tunnistaminen, luokittelu ja niiden käytettävyyden jatkuva seuranta. Operatiivisen kyberturvallisuuden tilannetietoisuuden ylläpitäminen tukee toimintaprosessien jatkuvuuden varmistamista. Toimintaprosessien häiriötilanteiden varautumiseen liittyvät toiminta- ja palautumissuunnitelmat, joilla voidaan parantaa organisaation resilienssiä häiriötapauksissa.

### 6.5.3 Teknillinen/taktinen näkökulma

Teknillisen/taktisen tason kehittämisen tavoitteiden voi katsoa liittyvän kiinteästi käytännön toimenpiteisiin organisaation tietoverkkojen, ICT-järjestelmien ja -laitteiden sekä niiden käytön suojaamiseksi. Lähtökohtana on suojattavien toimintaprosessien sekä niiden järjestelmien ja laitteiden tunnistaminen. Tähän liittyy myös toimijoiden kyky tunnistaa uhkien ja haavoittuvuuksien kautta muodostuvia kyberturvallisuusriskejä järjestelmissä ja laitteissa. Suojaustoimenpiteitä voidaan kehittää ja toteuttaa toimintaympäristöön soveltuvilla ajantasaisilla ja asianmukaisilla kyberturvallisuustuotteilla ja -palveluilla-. Tyypilliset kyberturvallisuustuotteet ja -palvelut liittyvät verkon segmentointiin, valvontaan ja tunkeutumisen havainnointiin, salaukseen sekä käytön autentikointiin ja valtuutukseen. Taktisen tason toimijoiden kyvykkyyttä voidaan kehittää jatkuvalla koulutuksella ja harjoittelulla sekä ylläpitämällä ohjausmekanismeja, kuten salasanakäytäntöjä ja menettelyjä laitteista huolehtimiseen. Teknillisellä/taktisella tasolla korostuvat tietoturvaan liittyvät attribuutit eli tiedon saatavuus (käytettävyys), luotettavuus ja eheys.

## 6.6 Suojautumisen kehittäminen

RR8. Pöyhönen J., Lehto M., Lehto M. (2019). Kyberturvallisuus sairaalajärjestelmissä, toiminnan kehittäminen. University of Jyväskylä, Faculty of Information Technology, research paper, 75/2019.

RR9. Lehto M., Pöyhönen J., Lehto M. (2019). Kyberturvallisuus sosiaali- ja terveydenhuollossa. Loppuvaportti Vol 2. VFH- ja WHC-hankekokonaisuus. Jyväskylä yliopisto, IT-tiedekunta. Jyväskylä yliopisto, Informaatioteknologian tiedekunta.

Edellisessä luvussa on todettu, että organisaation johdon tulevaisuuden visiointi ja strategiatyö luo perustan myös kyberturvallisuuden kehittämiselle. Lisäksi luvussa on todettu, että visiointityön kautta muodostettu näkökulma muutetaan strategisiksi tavoitteiksi sekä operatiivisen ja teknillisen/taktisen tason toimenpiteiksi. Niiden onnistumiseen liittyvät organisaation kyberturvallisuuden kyvykkyystekijät eli ihmiset, prosessit ja teknologia.

Esimerkiksi sairaalan osalta kyberturvallisuuden kehittämisen lähtökohdat voidaan muodostaa hyödyntämällä terveydenhuollon kyberturvallisuustyöryhmän (Health Care Industry Cybersecurity, HCIC) määrittelyjä ja suosituksia toimintatapojen järjestämiseksi. Nekin liittyvät edellä esitettyihin organisaation kehittämisen näkökulmiin, kuten organisaation johtajuuteen ja hallintoon, häiriötilanteiden sietokykyyn, henkilöstön osaamiseen sekä tutkimukseen ja tiedonvaihtoon. (Csulak, ym., 2017, 1,2)

ENISA:n näkökulmat kyberturvallisuuden ja tietoturvan kehittämiseen sairaalaesimerkin osalta ovat muun muassa seuraavia: (ENISA, 2016)

- Strategisella päätöksentekotasolla on huomioitava tietoturvastrategioiden ja kustannus-hyötyanalyysien merkitys päätöksissä riittävistä kyberturvallisuutta edistävistä suojausratkaisuista.
- Operatiivisen tason tehtävänä on luoda toimintapolitiikka, joka huomio erityisesti mobiililaitteiden ja henkilökunnan omien laitteiden (Bring Your Own Device, BYOD) käytöstä aiheutuvat riskit ja muodostaa selkeät periaatteet niiden käytölle.
- Teknisellä/taktisella tasolla tulee tunnistaa käytettävät laitteet ja miten ne liittyvät toisiinsa (tai ovat yhteydessä Internet-verkkoon) sekä määrittää ja toteutetaan turvallisuusperusteet kaikille tärkeimmille järjestelmille.
- Kaikilla päätöksentekotasoilla roolit ja vastuut sekä säännöllinen koulutus ja tietoisuuden lisääminen ovat keskeisiä tekijöitä proaktiivisen lähestymistavan aikaansaamiseksi tietoturvaan.

Organisaation ICT-järjestelmistä, -laitteista ja niiden käytöstä muodostuvat kokonaisuudet edustavat systeemiajatuksen mukaan sen osajärjestelmiä ja organisaatiokokonaisuus on kriittisen infrastruktuurin osajärjestelmä. Systeemitason näkökulmasta tarkasteltuna on tärkeää, että kaikilla järjestelmätasoilla ovat riittävät kyberturvallisuusvalmiudet ja, että niissä sovelletaan parhaita käytänteitä organisaation koosta tai sijainnista riippumatta. Seuraavassa alaluvuissa esitetään organisaation kehittämiseen toimenpiteitä sekä referoidaan alueella tehtyjä tutkimustuloksia, joilla edistetään väitöstutkimuksessa haasteellisiksi tilanteiksi tunnistettujen kohtien kyberturvallisuutta.

### 6.6.1 Systeemitason suojauksen kehittäminen

Kriittisen infrastruktuuriin lukeutuvat sekä julkiset että yksityiset organisaatiot, joilla on rooli infrastruktuurin palvelujen turvaamisessa. Kukin toimija suorittaa toimintoja, joita tukee laaja teknologia-alue, kuten tietoverkot ja tietotekniikka

(ICT), teollisuuden ohjausjärjestelmät (ICS), kyberfyysiset järjestelmät (CPS) sekä verkkoon kytketyt laitteet yleisemmin, mukaan lukien esineiden internet (IoT). Tämä riippuvuus tekniikasta ja verkottuneista yhteyksistä on muuttanut ja lisääntynyt potentiaalisia riskejä koko infrastruktuurin toiminnalle. Organisaatioiden näkökulmista voidaan tunnistaa alla olevia kehittämistavoitteita päätöksentekotasoittain.

**Strateginen taso**

Strategisella tasolla organisaatio tunnistaa liiketoiminnan tavoitteet ja painopisteet. Tämän tiedon avulla organisaation on mahdollista tehdä niihin liittyvät kyberturvallisuuden kehityksen toteutusta koskevat keskeisimmät päätökset sekä määrittää toimintaprosessien ja niiden järjestelmien suojaustasot liiketoiminnan riskejä vastaaviksi. Ylätason riskimäärittelyt voidaan liittää osaksi organisaation toiminnan kokonaisriskejä. Samalla varataan kehitystyön resurssit, joilla tuetaan valittua toimintalinjaa tai prosessia. Resurssikehystä mukauttamalla voidaan luoda painopisteitä kehitystoimenpiteille, joilla voidaan tukea eri liiketoiminnan tarpeita riippuen niihin liittyvästä riskinkantokyvystä. Strategisen tason päätökset muodostavat perustan muiden tasojen kehitystoimenpiteille.

**Operatiivinen taso**

Operatiivisen tason kyberturvallisuuteen liittyy riskien tunnistaminen liiketoimintaprosesseissa ja toimintaverkostoissa. Suojautumista voidaan kehittää tunnistamalla ja arvioimalla prosesseihin vaikuttavia tuotteita ja palveluja, jotka voivat sisältää mahdollisesti haitallisia toimintoja. Ne voivat sisältää jo lähtökohdistaan virheellisiä toimintoja tai niissä voi esiintyä suunnitteluvirheitä, ja siten ne voivat aiheuttaa riskejä koko toimintaketjussa. Toimintaketjujen riskien hallintaa voidaan kehittää määrittämällä ketjujen sidosryhmille kyberturvallisuusvaatimuksia. Vaatimusten käyttöönotto voidaan vahvistaa sopimuksilla, jotka voivat pitää sisällään menettelyt vaatimusten varmentamisesta, validoinnista ja seurauksista. Operatiivisella tasolla kehitetään erityisesti kyberturvallisuuden kyvykkyyksistä prosesseja.

**Teknillinen/taktinen taso**

Organisaation määriteltyä kyberturvallisuuden kehittämisohjelman soveltamiskohteet liiketoiminnastaan tai toimintaprosesseistaan, organisaatio voi tunnistaa niihin liittyvät tietoverkot, ICT-järjestelmät laitteineen ja muun tietoteknisen omaisuuden sekä määrittää niihin kohdistuvat kehittämisvaatimukset. Kehitystoimenpiteissä on oleellista tunnistaan näihin järjestelmiin ja laitteisiin sekä muuhun omaisuuteen kohdistuvat uhkat ja haavoittuvuudet. Teknillisen/taktisen tason suojaustoimenpiteiden kehittämistarpeet painottuvan laiteiden ja järjestelmien käytännön tason teknilliseen suojaamiseen ja sen kehittämiseen uusilla teknisillä ratkaisuilla. Kehitystoimenpiteet kohdistuvat kyberturvallisuuden teknilliseen kyvykkyyteen. Järjestelmien ja laitteiden käytön turvaamiseen liittyvät henkilöstön kyvykkyydet ja niiden kehittäminen. Turvallisen toiminnan ohjausmekanismit, kuten salasanakäytännöt, autentikoidut käyttäjät ja laitteista huolehtiminen, yhdessä toimintakulttuurin kehittämisen ja toiminnan arvopohjan huomioimisen kanssa ovat keskeisiä tekijöitä toimintaprosessien käytettävyysvaateiden sekä tiedon luotettavuus- ja tiedon eheysvaateiden osilta.

Tällä hetkellä on jo useita kyberturvallisuusratkaisuja ja -työkaluja tarjolla organisaatioiden tarpeisiin. Perinteisesti ne liittyvät hallinnollisten ICT-järjestelmien ja -laitteiden suojaukseen. Teollisuusautomaatiojärjestelmät ovat oleellinen osa useiden organisaatioiden toimintaprosesseja. Niihin liittyviä kyberturvallisuuden hallinnollisia ja teknillisiä ratkaisuja on kehitetty KYBER-TEO-tutkimushankkeessa, joita voidaan soveltaa myös tämän väitöstyön osalta. Hankkeen vuoden 2015 raportista on poimittu tähän yhteyteen oheiset kehitystarpeet: (Huoltovarmuuskeskus, 2015)

1. Verkkohyökkäysriskien hallintaan liittyvät automaatioverkon monitorointijärjestelyt muun muassa seuraavasti:
   - Automaatioverkkoon kytkettäväksi suunniteltu palomuuri,
   - automaation järjestelmälokien analyysi ja raportointi,
   - automaatioverkkoon tunkeutumisen ilmaisusysteemi (Intrusion Detection System, IDS),
   - verkko/laitekirjautumisten tunnistus,
   - verkkoliikenteen tietovuoseuranta ja yllättävien poikkeavuuksien tunnistus ja
   - hälytysten raportointi.
2. Valvomo-ohjelmistoriskin hallintaan liittyvä automaation tietoturvatestaus mm. seuraavasti:
   - verkkoskannerit,
   - tietoturva-aukkojen testausväline ”fuzzer” ja
   - penetraatiotestauksen työkalut.
3. Kyberturvallisten teknillisten ratkaisujen lisäksi KYBER-TEO raportissa on mainittu tuotantoon liittyviä hallinnollisia toimenpiteitä seuraavasti:
   - Yhtenäinen tietoturvapolitiikka,
   - käytännön ohjeet tietoturvan ylläpitämiseen,
   - automaatioverkossa sallitut etäyhteyskäytännöt, tekniikat ja yhteyspisteet,
   - automaatio- ja verkkojärjestelmien kyberturvallisuustarkastukset ja kartoitukset,
   - työlupien hallinta huoltotöissä ja
   - muutoshallinta kaikkien automaatiojärjestelmien ja -verkkojen asetusten/kokoonpanojen osilta.

ENISA:n suosittelemia tärkeimpiä suojaustoimenpiteitä ovat: (ENISA, 2016, 53)

- Verkon segmentointi (älykkäät palomuurit),
- verkon valvonta ja tunkeutumisen havaitseminen,
- vankka salaus,
- kulunvalvonta sekä
- käytön autentikointi ja valtuutus.

Organisaatioiden tietoverkkojen-, -järjestelmien ja -laitteiden sekä tietosisältöjen (datan) suojaamisen peruslähtökohta on perinteisten ajantasaisten ja tarkoituksenmukaisten suojaustekniikoiden ja -palvelujen käyttö. Tällöin mahdollistetaan tiedon käytettävyyden (saatavuuden), luotettavuuden ja eheyden varmistaminen tavanomaisia uhkia vastaan. Haasteeksi jäävät muun muassa ATP-hyökkäykset, joita on vaikea tunnistaa perinteisten tietoturvallisuuden edellyttämin keinoin.

Teknologisen kehityksen ja tulevaisuudessa erityisesti Teollisuus 4.0:n tarjoaman organisaation digitaalisen toimintaympäristön kyseessä ollen on odotettavissa, että organisaation ICT-infrastruktuurista muodostuu aiempaa laajempi laitteiden, ohjelmistojen ja ihmisten yhteenliittymä. Toimintaympäristön rakenteen voi katsoa teknillisesti monimutkaistuvan ja toiminallisesti kehittyvän yhä kompleksisempaan suuntaan. Perinteiset organisaation ICT-infrastruktuurin syvyyssuuntaisiin vyöhykkeisiin suojauskehiin (Suomen Automaatioseura ry., 2010, 69-70) perustuvat turvallisuusratkaisut eivät vastaakaan enää riittävästi kehittyviin uhkiin. Teknologisen kehityksen myötä organisaatioon kohdistuvat hyökkäysmahdollisuudet lisääntyvät ja uhkakuvat monipuolistuvat. Ne tulevat laajalta alueelta sekä organisaation sisäpuolelta ja ulkopuolelta. Kehityskulku asettaa uusia vaatimuksia järjestelmien perinteisen syvyyssuuntaisen vyöhykesuojausstrategian kehittämiseen. Tarvitaan uusia tekniikoita suojauksen kehittämiseen.

### 6.6.2 Uusien tekniikoiden soveltaminen suojaukseen

Organisaation ICT-infrastruktuurin vyöhykesuojaukseen integroiduilla uuden teknologian ratkaisuilla voidaan parantaa kyberturvallisuutta kehittämällä sekä suojaustasoa että näkyvyyttä järjestelmätasoilla. Tekoälyn kyvykkyyttä voidaan hyödyntää erityisesti henkilöstöä avustavana toimintana tapahtumien analyyseissä ja havaintojen läpikäynnissä. Tekoäly kykenee käsittelemään lähes reaaliaikaisesti laajoja tietomääriä rakenteellisista tietolähteistä ja rakenteettomista tietolähteistä, kuten erilaista teksteistä ja kuva-aineistoista. Kyberturvallisuutta käsitteleviä artikkeleita ja raportteja julkaistaan suuria määriä päivittäin, jolloin niiden käsittelyssä ja hyödyntämisessä voidaan käyttää tekoälyä. Sen kehittyminen avaa myös mahdollisuuksia kyberturvallisuuden menettelyjen automatisointiin.

Perinteiset ja joissain tapauksissa ”fragmentoituneet” suojausratkaisut haastetaan tämän päivän kehittyneillä kyberhyökkäysmenetelmillä, joissa hyödynnetään organisaation sisäisiä ja ulkoisia hyökkäysrajapintoja. Kyberturvallisuuden kehittämiseksi organisaatioiden tuleekin lähestyä turvallisuutta kuten immuunijärjestelmää. Tällöin turvallisuusratkaisujen tavoitteena on integroida ne toiminnalliseksi kehykseksi, joka koostuu käyttöön saatavista tärkeimmistä ja ajantasaisimmista toiminnallisuuksista. Integroitu toimintamalli voi hakea kyberturvallisuuteen liittyviä tietoja organisaation ICT-ympäristöstä (esim. lokitietoja, tietovirtoja, häiriötietoja ja - tapahtumia, turvapoikkeamia) sekä tietoja organisaation ulkopuolelta (esim. blogeja, tutkimustietoja ja verkkosivustoja). Integroidussa kyberturvallisuusratkaisussa analytiikka muodostaa ytimen, minkä avulla voidaan parantaa näkyvyyttä kybertoimintaympäristöön. (Falco, 2016)

Integroidun kyberturvallisuuskonseptin tavoitteina voidaan pitää ajatusta, jossa teknillisillä ratkaisuilla luodaan vyöhykkeisiä suojauskehiä täydentävä käyttöä, tietoverkkoa, -järjestelmiä ja laitteita koskeva suojauskokonaisuus. Siihen voidaan integroida muun muassa päätelaitteiden hallintaa ja käytön turvallisuusmenettelyjä, datavirtojen aktiivista monitorointia, poikkeamien havaintokyvykkyyttä ja erilaisten hyökkäysvektoreiden torjuntamenetelmiä (Falco, 2016).

Uusimpia teknillisiä ratkaisuja hyödyntävän integroidun järjestelmän kehittäminen edellyttää kyvykkyyttä hahmottaa niiden soveltamista organisaation toimintaympäristöön sekä tunnistaa toimintaa liittyviä haavoittuvuuksia ja niihin kohdistuvia perinteisiä ja uusia hyökkäysmuotoja. Systeemiajatukseen liitettynä integroiduissa kyberturvallisuusratkaisuissa voidaan luoda kokonaisuus tai alusta, joka tarjoaa laajan kohdennetun ekosysteemin erilaisia turvallisuusratkaisuja. Alustaratkaisut antavat mahdollisuuden tehokkaaseen asiantuntijoiden ja uuden tekniikan väliseen yhteistyön sekä turvaprosessien ja -tekniikan kehittämiseen, jolloin henkilöstön, prosessien ja tekniikan kyberturvallisuuden kyvykkyydet kehittyvät. Seuraavaksi uusien tekniikoiden soveltamista ja kehittämistä on hahmoteltu organisaation systeemitason suojaukseen tutkimuksen viitekehystasolla.

Kyberrakenteen kognitiiviselle kerrokselle liittyvät organisaation johdon toimenpiteet, kuten strategiapäätökset, julistetut toimintapolitiikat ja toiminnan riskitasojen hyväksynnät. Operatiivisen tason kyberturvallisuuden toimenpiteet kohdistuvat erityisesti toimintaprosessien jatkuvuuden hallintaan. Tällöin niitä ovat muun muassa toimintaprosessien riskien seuranta, verkottumiseen liittyvät kyberturvallisuustoimenpiteet ja erillisten yhteistyöfoorumien ylläpito. Lisäksi kerroksen ominaisuuksia ovat organisaation yleinen toimintakulttuuri, arvopohja ja henkilöstön kyvykkyys sekä toimenpiteinä niiden edistäminen. Ajatuksen on, että tekoälyratkaisuja voidaan käyttää laitteiden käytön avustamiseen ja toimintaympäristön seurantaan sekä käyttöoikeuksien hallintaan laajasti eri laitteissa ja järjestelmissä. Lisäksi organisaation tietovirroille ja datan käsittelyyn tarvitaan luotettavia menettelyjä sekä sisäisessä toiminnassa että verkottuneessa toiminnassa yhteistyötä tekevien osapuolten väleille. Lohkoketjutekniikka mahdollistaa kattavan suojan tietosisällöille tietovirroissa ja monenvälisissä sopimuksissa.

Palvelukerros pitää sisällään organisaation tarvitseman yhteyden Internetverkkoon ja sen palveluihin. Tekoälyratkaisuja voidaan kehittää verkkoliikenteen valvontaan ja seulontaan sekä käyttöön hyväksyttyjen sovellusten tunnistamiseen ja poikkeavan toiminnan ilmaisemiseen Toimenpiteet parantavat myös tilannekuvaa ja -tietoisuutta verkkokäytön osalta.

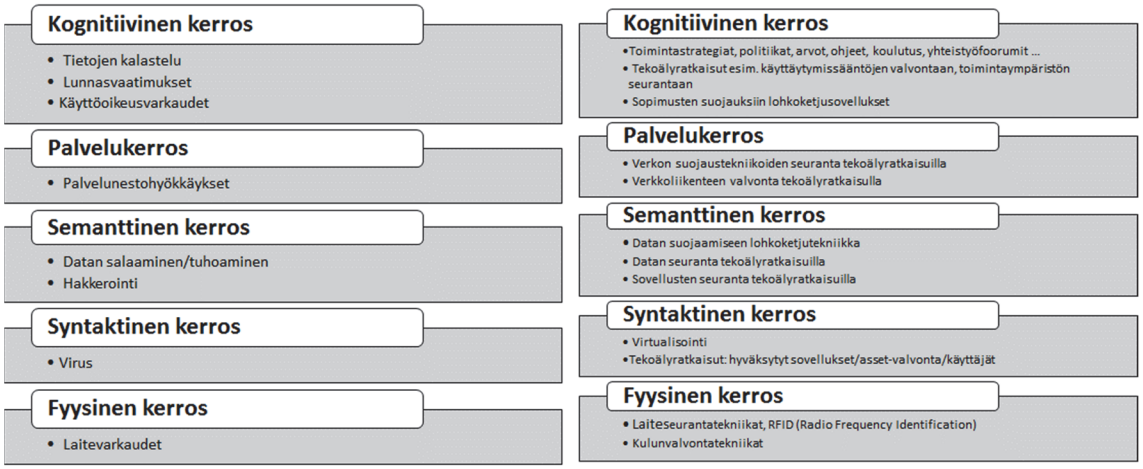
Kyberrakenteen semanttinen kerros pitää sisällään organisaation tietovarannon, datan, jota muodostetaan rakenteen eri kerroksilla, kootaan ja käsitellään organisaatiokohtaisesti tarkoituksenmukaisella tavalla. Teknologian kehittymisen myötä sekä datamäärä että sen käyttötarve lisääntyvät. Datan saatavuus (käytettävyys), luotettavuus ja eheys korostuvat. Tekoälyratkaisut kykenevät käsittelemään rakenteetonta ja rakenteellista dataa sekä relaatiotietokantoja ja muita tietovarantoja erilaisine tietokantoineen. Onkin nähtävissä, että tekoälyä

voidaan kehittää organisaation datan tietoturva-analyysien tekemiseen. Tavoitteena voidaan pitää myös tekoälyn soveltamista dataa tuottavien sovellusten seurantaan, johon voisi liittyä datan riskiluokittelu, käsittelyn tunnistaminen, poikkeavuuksien havainnointi, uhkien tunnistaminen ja tietomurtojen pysäyttäminen. Lohkoketjutekniikkaa voidaan kehittää datan suojaamista. Toimenpiteet parantavat myös tilannekuvaa ja -tietoisuutta tietovarantojen osalta.

Kyberrakenteen syntaktinen kerros pitää sisällään organisaation ICT- ja automaatiojärjestelmät ja niiden laitteiden toiminta-, ohjaus- ja hallintaohjelmat, niiden lankayhteydet ja langattomat yhteydet sekä tiedonsiirtoverkkojen sanomarakenteet. Tekoälyn osalta tavoitteena voidaan pitää sen avustuksella muodostettavaa ja kerroksen rakenteen sisältämiin erilaisiin digitaalisignaaleihin perustuvan diagnostiikan hyödyntämistä kyberhyökkäysten havainnoinnissa. Diagnostiikkaa voidaan hyödyntää myös langattomiin yhteyksiin pohjautuvien laitteiden vianilmaisussa ja yhteyksien käytön mallinnukseen perustuvassa vianhavaitsemisjärjestelmässä. Toiminta liittyy erityisesti prosessien kunnonvalvontaan ja niiden datan käytettävyyden seurantaan, mutta sitä voidaan hyödyntää myös kyberturvallisuuden menettelynä. Virtualisointitekniikan kehittyminen osaksi kyberturvallisuuden menettelyjä on käynnissä. Kehityksen myötä rakenteen tällä kerroksella sen avulla voidaan hyökkäyksiltä suojautua tai puolustautua palvelinten käyttöjärjestelmätasolla. Virtualisointi mahdollistaa useiden käyttöjärjestelmien ja sovellusten toiminnan yhdellä fyysisellä palvelimella ja ne ovat teknillisesti eristetty toisistaan. Toimintaa ohjaava tekniikka ja sen ”hypervisor” (tai Virtual Machine Monitor, VMM) voidaan ohjelmoida tarttumaan poikkeaviin tapahtumiin. Toimenpiteet parantavat myös prosessien toiminnan tilannekuvaa ja -tietoisuutta.

Kyberrakenteen fyysinen kerros pitää sisällään organisaation teknillisen laitetason. Niitä ovat kaikki käyttölaitteet, palvelinkokonaisuudet, ohjaus-, säätö- ja toimilaitteet, verkkolaitteet sekä fyysiset kaapeloinnit ja langattomien yhteyksien laitteet. RFID-tekniikkaa (Radio Frequency Identification, RFID) hyödyntämällä kehitetään erityisesti liikuteltavien laitteiden seurantaa ja paikantamista. Laitetiloja voidaan suojata kehittyneillä kulunvalvontaratkaisuilla. Toimenpiteet parantavat myös laitetason ja niiden sisältämien tietovarantojen paikkatiedon tilannekuvaa ja -tietoisuutta.

Oheisessa kuviossa 18 on yhdistetty organisaation kyberrakenteen eri kerroksille terveydenhuoltoon viime vuosina kohdistuneita hyökkäysmalleja väitöstyön viitetutkimuksen tausta-aineistosta ja liitetty niihin uuden teknologian mahdollistavia suojausratkaisuja (RR8, RR9). Kuvio toimii yleistettävänä esimerkkinä organisaation uhkien ja niiltä suojautumisen kehittämisestä uusia teknillisiä ratkaisuja hyödyntämällä tavoiteltaessa rakenteeseen integroitua suojausmenettelyä.




KUVIO 18 Sairaalajärjestelmien uhkakuvat ja uudet suojausratkaisut.

## 6.7 Riskien hallinta

Kyberturvallisuudessa uhka, haavoittuvuus ja riski muodostavat toisiinsa liittyvän kokonaisuuden. Organisaatiot kartoittaessaan riskejään, voivat arvioida ja luokitella niitä suhteessa mahdolliseen liiketoiminnan tai muun toimintaprosessin menetykseen tai vahingoittumiseen, kun hyökkääjä hyödyntää haavoittuvuutta eli uhka realisoituu. Riskit liittyvät muun muassa taloudellisiin tappioihin liiketoiminnan häiriötilanteissa, yksityisyyden menetyksiin, maineeseen ja mahdollisiin oikeudellisiin seuraamuksiin ja voivat jopa sisältää ihmishenkien menetyksiä. Lisäksi järjestelmän toiminnan palauttaminen aiheuttaa merkittäviä kustannuksia. Organisaation toiminnan ja järjestelmien kompleksisuus tekee mahdottomaksi eliminoida täysin kaikkia haavoittuvuuksia eikä myöskään voida kattavasti havaita ja jäljittää tunkeutumisia systeemin sisälle. Organisaatioiden verkottuminen lisää toimintaprosessien tehokkuutta ja suorituskykyä, mutta samalla siihen liittyy kasvavia haasteita kyberturvallisuuden osalta. (Lehto, 2019, 20)

Organisaation kyberturvallisuuteen liittyvien riskien hallintaprosessi on yksi sen turvallisuusajattelun peruskomponenteista. Prosessin toimenpiteitä käytetään organisaation toiminnallisten riskien tunnistamiseen, arviointiin ja priorisointiin huomioiden organisaation järjestelmät, henkilöstö, sidosryhmät ja yhteiskunnalliset velvoitteen. Riskiarviointien tarkoituksena on tunnistaa ja kartoittaa päätöksentekijöille riskit seuraavasti: Organisaatioille aiheutuvat merkittävät uhat, toimintaverkoston välityksellä uhkaavat toimet omaan ja muihin organisaatioihin nähden, sisäiset haavoittuvuudet organisaation ulkopuolelle ja organisaatioiden keskinäisvaikutuksiin. Lisäksi toimenpiteisiin kuluvat riskien toteutumisen todennäköisyyksien ja niistä aiheutuvien vahinkojen arvioinnit. Lopputuloksena tulee olla riskien määrittämisen kuvaus. Tyypillisesti se esitetään riskien haitta-asteena ja tapahtumatodennäköisyytenä, josta lopullinen luokittelu esitetään näiden matemaattisena tulona. (National Institute of Standards and Technology, 2012, 1).

NIST 800-39 kyberturvallisuuden riskien käsittelyohje suosittaa riskiarviointien suorittamista organisaation kaikille kolmelle hierarkiatasolle, jotka ohje on nimennyt seuraavasti: Organisaatiotaso, liiketoimintaprosessitaso ja tietojärjestelmätaso (National Institute of Standards and Technology, 2011). Tämä riskienhallinnan hierarkia tarjoaa riskinäkökulmia organisaation strategiselle, operatiiviselle ja taktiselle päätöksentekotasolle. Standardissa todetaan, että perinteiset riskinarvioinnit keskittyvät yleensä tietojärjestelmän tasolle, ja sen seurauksena yleensä jää sivuun merkittäviä riskitekijöitä, jotka voidaan arvioida tarkoituksenmukaisemmin organisaatio- ja liiketoimintaprosessitasoilla. Riskiarviointien tulee tukea organisaation päätöksentekoa sen kaikilla päätöksentekotasoilla. Esimerkiksi organisaatiotason riskinarvioinnit voivat antaa hyödyllisiä tietoja sen liiketoimintojen jatkuvuuden osilta, taloudellisten riskien osilta, toiminnan vaatimustenmukaisuuden ja sääntelyn riskeistä, maineriskeistä ja hankintariski laajoissa hankkeissa sekä toimitusketjun- ja kumppanuusriskeistä. Liiketoimintatason riskinarvioinnit liittyvät organisaation operatiiviseen toimintaan. Riskinarvioinnit voi vaikuttaa esimerkiksi tietoturva-arkkitehtuurin suunnittelupäätöksiin, toimittajien, palvelujen ja urakoitsijoiden valintaan, liiketoiminnan kehittämisprosesseihin ja tietoturvapolitiikkojen valintaan. Tietojärjestelmätasolla riskiarviot voivat vaikuttaa esimerkiksi suunnittelupäätöksiin, jotka koskeva erilaisia tietoturvaan liittyviä valintoja, räätälöintejä ja turvatarkastuksia. Päätökset voivat liittyä erityisesti tietotekniikkatuotteisiin tai niiden valvontavaatimuksiin, tietojärjestelmien käytön valtuutuksiin ja ylläpidon järjestelyihin. Tietojärjestelmätasolta riskinarvioinnit voivat tuottaa tietoa tietojärjestelmiin liittyvistä kustannus-, aikataulu- ja suoritusriskeistä. Tälle päätöksentekotasolle tietoa tuottavat tietoturva-asiantuntijat, tietojärjestelmien omistajat, tulojen ja menojen hyväksyjät. (National Institute of Standards and Technology, 2012, 17-18).

ISO/IEC 27005-satandardi käsittelee organisaation tietoturvallisuusriskien hallintaa (Liite 2). Se tukee standardin ISO/IEC 27001 mukaisia tietoturvallisuuden hallintajärjestelmän vaatimuksia, mutta se ei pidä sisällään mitään tiettyä riskien tunnistamisen menettelytapaa. Organisaatio itse määrittelee siihen liittyvät toimintatapansa. Toimintatavan valintaan vaikuttavat esimerkiksi hallintajärjestelmän kattavuusvaatimukset, arviointiympäristö ja toimiala. Standardin menettelyjä voidaan soveltaa kaiken tyyppisissä organisaatioissa. (Suomen Standardisoimisliitto SFS ry., 2012)

Ohjeen ISO/IEC 27005 mukaiset riskeihin liittyvä tietoturvallisuuden hallintaprosessi koostuu seuraavista vaiheista: (Suomen Standardisoimisliitto SFS ry., 2012)

- Arviointiympäristön määrittämisestä,
- riskien arvioinnista,
- riskien käsittelystä,
- riskin hyväksynnästä,
- riskeistä viestimisestä sekä
- riskien tarkkailusta ja katselmoinnista.

Ohjeen ISO/IEC 27005 riskien iteratiivinen toimintamalli auttaa saavuttamaan tasapainon siten, että turvamekanismien tunnistaminen suoritetaan tehokkaasti ja samalla varmistetaan erityisesti merkittävimpien riskien tunnistaminen.

Organisaation kyberturvallisuuteen liittyvien riskien arviointiympäristöä on kuvattu luvun alussa (NIST 800-39). Arviointiympäristön määrittämisen jälkeen tehdään riskien arviointi, jonka jälkeen voidaan siirtyä riskien käsittelyyn. Lähtökohtana riskien arvioineissa voidaan pitää ajatusta niiden vaikutuksen saamista niin pieneksi kuin se käytännössä on mahdollista. Käsittelyvaihtoehtojen valinnassa ja arvioinnissa on huomioitava niiden toteuttamismahdollisuudet ja odotettavissa olevien kustannusten ja hyötyjen suhde. Käsittelyvaihtoehdot, joilla voidaan pienentää riskejä merkittävästi suhteessa alhaisin kustannuksin, tulee luokitella ensisijaisesti toteutettavaksi. Organisaation tulee tarkastella myös harvinaisia, mutta vakavia riskejä, jolloin saatetaan joutua toteuttamaan ratkaisuja, jotka perustuvat ensisijaisesti ristien hallintaa eikä niinkään taloudellisiin perusteisiin. Käsittelyvaihtoehdot, joilla nämä riskit voidaan minimoida, tulee luokitella myös ensisijaisesti toteutettavaksi.

Riskien hallintaprosessiin liittyy niiden käsittely. Riskejä voidaan tarkastella päätösprosessissa sekä taloudellisen arvon että maineen menettämisen kannalta. Riskien käsittelyvaihtoehdot ovat niiden halittu säilyttäminen, pienentäminen, välttäminen tai siirtäminen esimerkiksi vakuuttamalla toimintaa niin, että jäännösrikit ovat organisaatiossa hyväksyttävällä tasolla. Riskejä voidaan pienentää tai joiltakin osin jopa välttää sääntelytoimenpitein, kehittämällä organisaation prosesseja ja yhteisöllisyyttä sekä kehittämällä teknologisia ratkaisuja. Kyberturvallisuuteen liittyvien riskien osalta on suositeltavaa, että organisaatiossa toteutetaan jatkuvaa riskitarkastelua. Tutkimuksessa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet” (2017) tuli esille tarve vahvistaa tätä toimintaa erityisesti osana liiketoimintaprosessien jatkuvuuden hallintaa. Organisaation toimintaan tulee aina liittymään tapahtumia, jotka täyttävät tunnusmerkin ”Tunnetut tuntemattomat” ja niihin varautumisiin suositellaan sovellettavaksi liiketoimintaprosessikohtaista kattavaa riskitarkastelua.

Tuntemalla organisaation toimintaverkostot ja -prosessit sekä ICT- järjestelmien ja -laitteiden toiminnot kyberrakenteessa kerros kerrokselta (viisikerroksisessa rakenteessa), voidaan niihin liittyvät merkittävimmät uhkat, haavoittuvuudet, todennäköisimmät kyberhyökkäystavat ja niiden motiivit arvioida. Haavoittuvuuksien analysointi mahdollisia uhkia ja hyökkäystapoja vasten on järjestelmällinen apuväline prosessien toimintaan liittyvien riskien tunnistamiseen. Analyysi antaa siten nopeasti kokonaiskuvan prosessin toiminnan jatkuvuuteen liittyvistä uhkista.

Riskin suuruutta voidaan arvioida esimerkiksi vahingon seurausten ja tapahtuman todennäköisyyden suhteen. Eräs yleisesti käytetty asteikko pitää sisällään arviointiluokat vakava, haitallinen tai vähäinen. Todennäköisyydet puolestaan voidaan luokitella asteikolla todennäköinen, mahdollinen tai epätodennäköinen. Kun seuraukset ja todennäköisyydet numeroidaan esimerkiksi yhdestä viiteen kutakin kohtaa arvioitaessa ja muodostetaan niiden tulo, niin saadaan ris-

kit priorisoitua tulojen suuruusjärjestyksessä. Priorisoinnissa perusteella voidaan puolestaan kohdentaa toimenpiteet tärkeysjärjestyksessä riskien hallitsemiseksi.

## 6.8 Varautuminen ja resilienssi

Miten kriittisen infrastruktuurin organisaation toiminnan jatkuvuuden hallintaa voidaan kehittää häiriöihin varautumiseksi haasteellisessa kybertoimintaympäristössä?

P2. Pöyhönen, J., Nuojua V., Lehto M., Rajamäki J. (2018). Application of Cyber Resilience Review to an Electricity Company. ECCWS 2018: Proceedings of the 17th European Conference on Cyber Warfare and Security (pp. 380-389). Published by Academic Conferences and Publishing International Limited. Reading. UK.

Organisaatioiden toiminnan luottamus ja toimintaprosessien jatkuvuuden ylläpitäminen tehokkailla toimenpiteillä ovat keskeisiä asioita mietittäessä kyberturvallisuuteen vaikuttavia tekijöitä. Proaktiivista toimintaa voidaan kehittää huomioimalla kyberturvallisuuteen liittyvät riskit kattavasti suunniteltaessa luottamusta lisääviä toimia. Aiemmin tunnistamattomiin ja riskitarkastelulta piiloon jääneisiin tekijöihin (Tuntemattomiin, tuntemattomiin) tulee myös varautua osana toiminnan jatkuvuuden hallinnan näkökulmaa. Tämä tarkoittaa yllätyksellisiin toimintahäiriöihin varautumista systeemitason suunnittelun avulla. Varautumissuunnittelun osalta tutkimuksessa perehdyttiin sähköyhtiön organisaation toiminnan kyberturvallisuuden suunnitteluun, resilienssin käsitteeseen ja sen soveltamiseen organisaation kyberturvallisuuden kehittämiseen. Malliksi valittiin Igor Linkovin teorian mukainen tarkastelu. NIST-standardin mukainen ”Kyberturvallisuuden viitekehys” tukee Linkovin teorian mukaisen tarkastelun tarkoituksenmukaisuutta ja luetteloi seikkaperäisesti referenssejä sen toteutuksen avuksi (National Institute of Standards and Technology, 2018, 24-44).

Linkov ym. esittelevät artikkelissaan ” Measurable Resilience for Actionable Policy” resilienssimatriisin (jatkossa ns. Linkovin malli), joka yhdistää soluiksi neljä ajallisesti etenevää vaihetta 1) suunnittelu/varautuminen, 2) häiriön aikainen toiminta, 3) toipuminen ja 4) sopeutuminen ja neljää tarkastelutasoa 1) fyysinen, 2) informaatio, 3) kognitiivinen ja 4) sosiaalinen. Myöhemmin Linkov ym. sovelsivat artikkelissaan ”Resilience metrics for cyber systems” malliaan edelleen kyberjärjestelmiin. Tarkoituksena on kehittää tehokkaita mittareita kyberjärjestelmien resilienssin arvioimiseen ja suunnitteluun. (Linkov, ym., 2013a; 2013b)

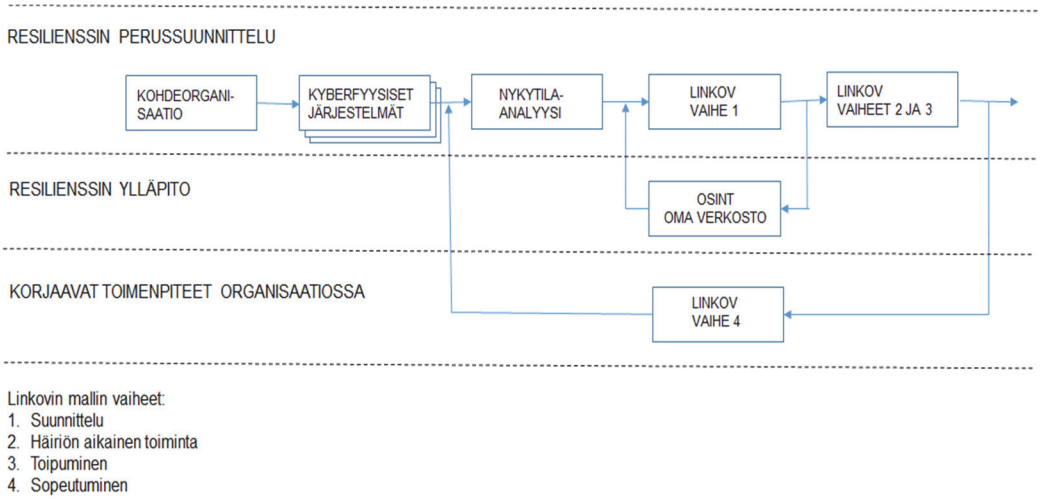
Kyberturvallisuuteen liittyvien järjestelmien tapauksessa resilienssimatriisin soluja tulkitaan tässä tutkimuksessa seuraavasti: Kuinka kyvykäs järjestelmä on varautumaan/toimimaan/toipumaan/sopeutumaan fyysisellä/informaatio-/kognitiivisella/sosiaalisella tasolla toteutettuun kyberhäiriöön. Yhden mittarin lisääminen tietylle tasolle edellyttää usein mittarin lisäämistä myös muille tasoille.

Resilienssimittareita käytetään tarpeiden tunnistamiseen ja priorisointiin, edistymisen seurantaan ja resurssien jakamiseen. Täten ne muodostavat olennaisen osan suunnittelua ja päätöksentekoa. (Linkov, ym.,2013b)

### 6.8.1 Resilienssiprosessi

Organisaation kyberturvallisuuteen liittyvän varautumisen tueksi kehitettiin väitöstyön yhteydessä (Tapaustutkimus 1) kuvion 19 mukainen resilienssin hallinnan prosessi Sen edellyttämien suunnitelmien toteuttamisen ja ylläpitämisen seuranta voidaan tarvittaessa liittää osaksi yrityksen johtamisjärjestelmää. Prosessimallissa kohdeorganisaation määrittelyn jälkeen tulee tunnistaa sen toimintaprosesseihin liittyvät kyberfyysiset ja muut ICT-järjestelmät niiden kyberrakenne huomioiden. Tämän jälkeen nykytila-analyysi voidaan kohdistaa teemahaastatteluna kyberrakenteen kautta organisaatioon SWOT-analyysillä (luku 4.2.1). Näin saatava tilannekuva mahdollistaa ja ohjaa prosessin vaiheiden 1 - 3 eli normaaliolojen aikana toteutettavia perussuunnitelmien laadintaa prosessin kaikille tasoille (fyysinen, informaatio, kognitiivinen, sosiaalinen). Vaihe 4 pitää sisällään myös edellä mainitut tasot, mutta niiden sisältöjen kehittämiseen tulee kiinnittää erityistä huomiota mahdollisen häiriötilanteen jälkiselvittely perusteella ja tilannekohtaisesti. Tällöin vaihe mahdollistaa jatkotoimet niin, että organisaatio hyötyy häiriötilanteen opeista mahdollisimman tehokkaasti. Häiriötilanteen jälkiselvittelyyn liittyen organisaation toimintaa tulee siis kehittää siitä saatujen kokemusten ja oppien perusteella sekä suorittaa kattava kyberturvallisuuden yleinen tilannekuvamäärittely SWOT-analyysi uusimalla. Sen jälkeen on tarkoituksenmukaista päivittää suunnitelmat korjaavana toimenpiteenä jokaisen mallin vaiheen osalta. Prosessimallissa normaaliolojen valmiussuunnittelua (vaihe 1) voidaan ylläpitää avoimiin lähteisiin perustuvan tiedonhankinnan avulla (Open Source Intelligence, OSINT) sekä hyödyntämällä yrityksen omia yhteistyö- ja tiedonhankintakanavia päivityksessä.

Huomionarvoista on myös se, että organisaation kyberfyysisten järjestelmien uusintojen yhteydessä prosessia voidaan hyödyntää muun muassa järjestelmien riippuvuussuhteiden arviointiin kyberturvallisuuden näkökulmasta tarkasteltuna.




KUVIO 19 Resilienssitoimenpiteiden toteutusprosessi.

Organisaation ICT-järjestelmien tunnistaminen ja niiden merkityksen todentaminen sekä kyberturvallisuuden näkökulmasta että toimintaprosessien käytettävyyteen muodostaa resilienssitoimenpiteiden lähtökohdan. Järjestelmät voivat olla myös monilta osiltaan keskinäisessä riippuvuussuhteessa ja tiedonsiirtoverkostojen kautta ne ovat riippuvuussuhteessa myös toimintaympäristöjensä kanssa. Tutkimuskohteen osalta tunnistettiin seuraavat kyberfyysiset ja muut ICT-järjestelmät, jotka vaikuttavat oleellisesti sähköntuotannon prosessiin. Järjestelmät liittyvät:

- Toimittajaverkoston hallintaan (yritystason ICT).
- Tuotantoprosessin hallintaan (ICS-toiminto).
- Jakeluverkoston hallintaan (yritystason ICT/ICS-toiminto).
- Kiinteistön automaation hallintaan (ICS-toiminto).
- Turvajärjestelmään (yritystason IVT/ICS-toiminto).

Tyypillisellä sähköyhtiöllä, jolla on sähköntuotantoa ja jakelua, operatiiviset liiketoimintaprosessit pitävät sisällään logistiikkajärjestelmiä, tuotantojärjestelmiä, jakelujärjestelmiä sekä organisaation tukiprosessien järjestelmiä. Kyberturvallisuuden valmiussuunnittelussa nämä prosessit tulee huomioida ja ottaa resilienssitarkastelun kohteeksi. Tunnistamalla organisaation operatiivisten prosessien rakenteet, toimintaan vaikuttavat teknillisen/taktisen tason tekijät, järjestelmien haavoittuvuudet ja niihin todennäköisimmin kohdistuvat kyberhyökkäystavat, varautumissuunnitteluun on käytettävissä tärkeimmät tiedot. Haavoittuvuuksien analysointi hyökkäystapoja vasten mahdollistaa järjestelmällisen lähestymisen prosessien toimintaan liittyvien riskien tunnistamisessa ja arvioinnissa sekä valittaessa tarkoituksenmukaisimpia varautumistoimenpiteitä.

Linkovin malli ja sen eri vaiheet sopivat erityisesti operatiivisen ja teknisen/taktisen tason valmiussuunnitteluun. Edellä lueteltujen järjestelmien rakenne huomioiden voidaan löytää kohdeorganisaation toiminnasta ne kohteet,

jotka ovat varautumisessa ja valmiussuunnittelussa keskeisessä asemassa. Yrityskohtainen toimenpiteiden sisältö tulee perustua ennen Linkovin mallin käyttöä tapahtuvaan nykytila-analyysiin ja sen kautta saatavaan tilannekuvaan kohdeorganisaation vahvuuksista, heikkouksista, mahdollisuuksista uhista sekä niiden keskinäisistä suhteista. Nykytila-analyysin perusteella Linkovin mallin mukaisiin suunnitteluvaiheisiin on saatavissa kunkin organisaation tarpeita vastaava sisältö. Nykytila-analyysi voidaan hyödyntää SWOT-analyysiä ja toteuttaa taulukon 11 mukainen teemahaastattelu. Haastatteluteemat ja niihin liittyvät näkökulmat voidaan sitoa tutkimuksen viitekehykseen luvussa 4.2.1 kuvatulla tavalla. Viitekehyksen (kyberrakenteen) käyttäminen helpottaa tulosten analysointia, kokonaistilannekuvan muodostamista ja riskiarviointia. Kokonaistilannekuva tulee tässä yhteydessä käsittää strategisen, operatiivisen ja teknillisen/taktisen tason tilannekuvina.

TAULUKKO 11 SWOT-analyysin haastatteluteemat

| **Vahvuudet ja heikkoudet/haastatteluteemat** | **Mahdollisuudet ja uhkat/haastatteluteemat** |
|---|---|
| • Johtaminen<br>• Henkilöstön osaaminen<br>• Kyberturvallisuustuotteet ja -palvelut<br>• Tilannetietoisuus<br>• Sidosryhmänäkemys<br>• Toiminnan jatkuvuuden varmistaminen<br>• Asiantuntijapalvelut | • Edistyksellisen tekniikan hankinta<br>• Uudet yhteistyötahot<br>• Uudet kehitysmahdollisuudet<br>• Toimintaympäristön analysointi<br>• Kyberuhkien analysointi<br>• Toimintaverkoston analysointi |

### 6.8.2 Resilienssiä lisäävät keskeisimmät toimenpiteet

Nykytila-analyysin jälkeen Linkovin mallin pohjalle rakennetussa resilienssitoimenpiteiden prosessimallissa fyysiselle tasolle suunnittelu- ja varautumisvaiheen (Vaihe 1) toimenpiteiksi muodostuivat tekniikan toimivuudesta, valvonnasta ja ohjauksesta huolehtiminen, tarvittaessa tehtävä järjestelmien eristämisen ja toiminnallisten saarekkeiden suunnittelu sekä vaihtoehtoisten tiedonsiirtoverkkojen ja reittien suunnittelu. Häiriötilanteen (Vaihe 2) sattuessa ensiksi varmistetaan tilannekuva tapahtumasta, sen luonteesta, häiriön levinneisyydestä ja vaikutuksesta. Tämän jälkeen otetaan tilanteen varalle laaditut suunnitelmat käyttöön tarvittavilta osiltaan. Toipumisvaiheessa (Vaihe 3) varmistetaan järjestelmien kyberturvallisuus ja toiminnallisuus kaikilta osiltaan sekä ohjataan kokonaisvaltainen toiminnan palauttaminen. Sopeutumisvaihe (Vaihe 4) määrittyy tapahtumasta kertyneiden kokemusten mukaisesti, mutta ainakin teknilliset suojaustoimet tulee tarkastella huolella.

Informaatiotason toimenpiteet painottuvat suunnittelu- ja varautumisvaiheessa dokumentointisuunnitteluun laajasti järjestelmätasolle tilannekohtainen

dokumentoinnin kattavuus huomioiden. Kriittisten toimenpiteiden ja niihin liittyvien resurssivaatimusten kirjaaminen jo suunnitteluvaiheessa on erityisesti huomioitava. Dokumentointi sekä palvelee toimintaa häiriötilanteessa että mahdollistaa tietojen kirjaamiseen häiriötilanteen aikana ja toipumisvaiheessa, jotta tilanteen kokemusten ja oppimisen hyödyntäminen sopeutumisvaiheessa on mahdollista. Myös keskeisten sidosryhmien ja eri viranomaisten informoinnin suunnittelu ja toteuttaminen jokaisessa vaiheessa on osa informaatiotason suunnittelua ja sen toteutusta.

Tutkimuskohteen osalta kognitiivisen tason suunnitelmasta on kaikista tasoista laajin. Sen merkityksen voikin arvioida olevan ratkaiseva johtamisessa, tilannekuvan muodostamisessa, toiminnallisten vastuiden määrittämisessä, toimenpiteiden priorisoinnissa, toiminnan resurssoinnissa, hallinnassa ja ohjauksessa. Näillä kaikilla toimenpiteillä on keskeinen merkitys häiriötilanteen aikaisessa toiminnassa, toipumisvaiheessa ja sopeutumisvaiheen oppien hyödyntämisessä.

Sosiaalisen tason suunnitteluvaihe pitää sisällään yhteydenpitosuunnitelman yhteyshenkilöineen informaatiotason suunnittelua laajemmalle sisäiselle ja ulkoiselle sidosryhmäkokonaisuudelle. Tilannekohtaisen tiedottamisen mahdollisuus laajasti häiriön eri vaiheissa on sosiaalisen tason suunnittelun tulosta. Lisäksi sosiaalisen tason suunnitteluun kuuluvat koko henkilöstön kouluttaminen ja harjoituttaminen kaikkien prosessin eri vaiheiden hallintaan.

Taulukossa 12 on lueteltu toimenpiteitä otsikkotasolla tutkimuksen kohteena olleen sähköyhtiön osalta. Taulukko kuvaa sähköyhtiön kyberturvallisuuden johtamisen ja kyberuhkiin varautumisen konkreettisia ja yleistettäviä toimenpiteitä suunnitteluvaiheessa, häiriötilanteiden toimintavaiheessa ja toipumisvaiheessa sekä häiriötienteiden jälkeiseen normaalitilanteeseen sopeutumisessa. Kohteena ollut organisaatio omistaa taulukon otsikoiden mukaisen yksityiskohtaisen toimintasuunnitelman.

TAULUKKO 12 Organisaation resilienssitoimenpiteitä

| | **Suunnittelu** | **Toiminta** | **Toipuminen** | **Sopeutuminen** |
|---|---|---|---|---|
| **Fyysinen taso** | Tekninen tilannetietoisuus<br>Verkon segmentointi<br>Vaihtoehtoiset resurssit | Häiriöiden tunnistaminen, niiden laajuus ja vaikutukset<br>Arkaluontoisten tietojen suojaus<br>Vaihtoehtoisten resurssien käyttöönotto<br>Häiriöiden eristäminen | Tilannetietoisuuden ylläpitäminen<br>Toiminnan palauttaminen<br>Toiminnan testaus | Järjestelmien päivitykset |
| **Informaatio taso** | Kriittisten järjestelmien luokittelu ja priorisointi<br>Vaikutukset liiketoimintaan<br>Arkaluotoisten tietojen suojauksen valmistelu<br>Toimintasuunnitelmat | Tilanteiden dokumentointi<br>Tilanteen informointi viranomaisille ja sidosryhmille | Tapahtumien dokumentointi<br>Tietojen välittäminen viranomaisille ja sidosryhmille | Asiakirjojen päivittäminen |
| **Kognitiivinen taso** | Tilannetietoisuuden hahmottamine<br>Toimintavaihtoehdot<br>Toiminnan resurssointi<br>Koulutus ja benchmarking<br>Palautejärjestelmä | Tilannehavainnointi ja -analyysi<br>Lisäresurssien hyödyntäminen<br>Jatkuvuuden hallinta | Asiantuntemuksen jakaminen<br>Tapahtumadatan ja lokitietojen keruu | Lokianalyysit<br>Tilanneanalyysit<br>Vaikutusanalyysit<br>Palauteanalyysit<br>Ohjeiden päivitykset<br>Jatkuva parantaminen |
| **Sosiaalinen taso** | Viestintäsuunnitelmat<br>Sidosryhmien yhteyshenkilöiden nimeäminen<br>Koulutus/harjoittelu poikkeustilanteisiin | Sidosryhmäyhteistyö | Toiminnasta tiedottaminen sidosryhmille | Henkilöstökoulutus<br>Tiedottaminen kehitystoiminnasta<br>Sidosryhmätietojen päivitys |

### 6.8.3 Suunnitelman ylläpitäminen OSINT:n avulla

Avoimien lähteiden tiedonsaantia (Open Source Intelligence, OSINT) voidaan hyödyntää merkittävän turvallisuustiedon keräämiseen. Tällaisia avoimia ja julkisia lähteitä ovat sekä sanoma- ja aikakauslehdet perinteisen median edustajina että Internet digitaalisen median edustajana. (Lee & Shon, 2016)

Seokcheol Lee ja Taeshik Shon esittelevät artikkelissaan ” Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures” OSINT:a hyödyntävän viitekehyksen kriittisen infrastruktuurin kyberuhkien tarkasteluun. Sen tavoitteena on kehittää kriittisen infrastruktuurin turvallisuustasoa analysoimalla aiemmin organisaatiossa havaitsematta jääneitä kyberuhkia ja mahdollistaa siten myös niin sanottujen nollapäivähaavoittuvuuksien ehkäisemisen. OSINT soveltuu erityisen hyvin kriittisen infrastruktuurin tietoverkkoon sen kommunikointimallien ja -ympäristöjen luonteen vuoksi. (Lee & Shon, 2016)

OSINT:a hyödyntävän tiedustelun on täytettävä kaksi ehtoa: analysoitavan tiedon sisällön ja lähteen on oltava vahvistettuja, sekä tiedustelun on oltava käyttötarkoitukseensa nähden hyödyllistä ja merkityksellistä. OSINT-suunnitelmaa laadittaessa valitaan ensin kohdejärjestelmä, minkä jälkeen päätetään menetelmä ja aikataulu julkisen tiedon keräämiselle. Valmisteluvaiheessa tarkastetaan ensin kohteeseen liittyvä sisäinen tieto ja sen perusteella luodaan alustava tiedustelutietokanta. Lopulta avoimien lähteiden tiedonkeruutyökaluja käytetään tiedon keräämiseen tarkasteltavasta kohteesta. Alustavassa tiedustelussa luotua tietokantaa hyödyntämällä vahvistetaan kerätyn tiedon luotettavuus, ja samalla päivitetään alustava tiedustelutieto. (Lee & Shon, 2016)

### 6.8.4 Yhteenveto varautumisesta osana johtamista

Yrityksen kybermaailman turvallisuutta ja luottamusta lisäävien toimenpiteiden aikaansaaminen on ensisijaisesti yrityksen ylimmän johdon vastuulla. Integroimalla tarvittavat toimenpiteet ajatukseen liiketoiminnan turvaamisesta kasvattaa niiden merkittävyyttä ja hyötyjä parantuneiden toimintaprosessien kautta koko organisaatiolle, sidosryhmille ja yhteiskunnalle. Tarkastelussa esiin tulevilla johdon näkemyksillä ja vaatimuksilla on keskeinen merkitys toimintaprosessin turvallisuussuunnittelua kehitettäessä. Samalla ilmenevät myös toimintaan sitoutuvat kustannukset ja muut resurssit. (NIST 800-82, 2011)

Kun organisaation osalta puhutaan johtamisesta ja, kun johtamista tehdään järjestelmällisesti, niin puhutaan organisaation johtamisjärjestelmästä. Tällöin johtamista voidaan tehdä laadukkaasti huomioiden asiakkaat, henkilöstön merkitys, toimintaprosessiensa tehokkuus ja ohjaus, toiminnan jatkuva kehittäminen ja sidosryhmäviestintä. Johtamisjärjestelmää voidaan hyödyntää myös organisaation varautumissuunnittelun toteutumisen seurannassa.

Organisaation johtamisjärjestelmä voi sisältää erilaisien standardien mukaisia hallintajärjestelmiä, kuten laadunhallintajärjestelmä, informaatioturvallisuuden hallintajärjestelmä tai ympäristöasioiden hallintajärjestelmä. Noudattaakseen käytännön toiminnassaan eri standardien mukaisia periaatteita organi-

saatio voi kuvata edellyttämänsä toimenpiteet toimintajärjestelmäänsä. Toimintajärjestelmä on kuvaus organisaation yhteisistä toimintatavoista. Johdon ja henkilöstön yhdessä määrittämien pelisääntöjen ja toimintamallien avulla pyritään määrätietoisesti pitämään yllä korkeaa toiminnan tasoa ja kehittämään toimintaa asetettuja tavoitteita silmällä pitäen asiakkaat ja sidosryhmät. Toimintajärjestelmän avulla prosessikuvaukset, ohjeistukset, tallenteet, mittarit, tehtävät sekä palautteet on koottavissa toimivaksi kokonaisuudeksi, joka ohjaa ja tukee organisaation missiota, visiota ja niitä toteuttavia toimenpiteitä.

Organisaation kyberturvallisuuteen liittyvät johtaminen ja sitä tukevat toimenpiteet tavoitteineen tulee dokumentoida organisaatiossa koko henkilöstön käyttöön esimerkiksi toimintakäsikirjassa ja sitoa ne siten osaksi organisaation kokonaisturvallisuutta.

Resilienssitoimenpiteiden toteutusprosessi palvelee organisaation kaikkia päätöksentekotasoja erityisesti valmiuden näkökulmasta. SWOT-analyysissä analysoidaan organisaation toimintakykyä ja sen toimintaympäristöä kokonaisuutena, jolloin se tukee erityisesti strategista suunnittelua. Se tuottaa tietoa myös muille päätöksentekotasoille oppimisessa ja ongelmien tunnistamisessa, arvioinnissa ja toimintaprosessien kehittämisessä. Resilienssin kehittämisen malli palvelee suoranaisesti yrityksen toiminnan jatkuvuuden hallinnan suunnittelua ja ylläpitämistä, jolloin se tukee operatiivisen tason ja teknillisen/taktisen tason toimintaa.

Sähköyhtiön kyberturvallisuuden johtamisen ja toiminnan luottamuksen kehittämisen osalta kyberuhkiin varautuminen ja konkreettinen valmiussuunnittelu muodostavat perustan organisaation proaktiiviselle varautumiselle sen kybertoimintaympäristössä. Nämä kyberresilienssiä lisäävät suunnitelmat ja toimenpiteet suositellaan liitettäväksi kiinteäksi osaksi yrityksen kokonaisturvallisuutta, jolloin ne tukevat organisaation johtamista sen kaikilla tasoilla.

Linkovin suunnittelumallin ja tutkimuksen viitekehyksenä toimivan kyberrakenteen välille voidaan johtaa analogia. Erityisesti Linkovin mallin fyysisen ja kognitiivisen tason suunnittelussa on hyötyä järjestelmärakenteen yksityiskohtaisesta tuntemuksesta. Informaatiotason suunnittelu kohdistuu jokaiseen tasoon ja lisäksi kaikkiin organisaation sidosryhmiin. Sosiaalinen suunnittelutaso palvelee kaikkien sidosryhmien huomioimista. Johtopäätökset mallien käytöstä ovat seuraavat:

1. Linkovin malli laajentaa valmiussuunnittelua kyberrakenteen ulkopuolelle.
2. Järjestelmien kyberrakenne mahdollistaa suunnittelun yksityiskohtaisen kohdentamisen järjestelmien kaikille tasoille.
3. Yhdistämällä mallit saadaan kyberfyysisten järjestelmien jatkuvuuden varmistamiseen kattava suunnitteluympäristö.

Käytännön esimerkkinä sähköyhtiön kyberturvallisuuden proaktiivisesta suunnittelutarpeesta toimii Ukrainassa 23. päivänä joulukuuta 2015 tapahtunut laaja sähkökatko. Sen syyksi on tutkinnassa selvinnyt ulkopuolisen tahon suorittama koordinoitu kyberhyökkäys kolmen sähkön jakelusta vastaavan yrityksen ohjausjärjestelmiin ja tietovarantoihin. Erääksi mahdollisista tunkeutumiskohteita

epäillään teollisuusautomaatiojärjestelmää, jonka toimintaan tunkeutujien arvioidaan päässeet käsiksi etäyhteyden kautta. Varauduttaessa teollisuuden automaatiojärjestelmiin kohdistuviin kyberhyökkäyksiin ja niiden sietokyvyn parantamiseen, organisaatioille suositellaan ensisijaiseksi toimenpiteeksi kyberturvallisuuden hallinnan parhaiden käytäntöjen käyttöönottamista. (ics-cert.us, 2016)

## 6.9 Tilannetietoisuuden kehittäminen

Millaisia menettelyjä kriittisen infrastruktuurin organisaation tilannetietoisuuden kehittämiseen liittyy? Kuinka organisaatiot vaihtavat kyberturvallisuuteen liittyviä tietojaan? Voidaanko organisaation kyberturvallisuusvalmiuksia hyödyntää laajemmin kriittisessä infrastruktuurissa?

P4. Pöyhönen, J., Nuojua V., Lehto M., Rajamäki J., (2019). Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations. Digital Transformation, Cyber Security and Resilience. DIGILIENCE 2019. Volume 43, no. 2 (2019): 236-256.

P7. Pöyhönen, J., Rajamäki, J., Ruoslahti, H., Lehto, M., 2020. Cyber Situational Awareness in Critical Infrastructure Protection. Cyber Security of Critical Infrastructure 2020 (SYSEC2020) conference, April 29th, 2020 - April 30th, 2020. Dubrovnik. Croatia. Artikkeli hyväksytty 2.3.2020.

Kriittisen infrastruktuurin tilannetietoisuus painottuu Yhteiskunnan turvallisuusstrategiassa, YTS, (2017) osana kansallisten elintärkeiden toimintojen ylläpitämistä. Tehokas häiriötilanteiden hallinta edellyttää tiivistä yhteistyötä johtamisen, tilannekuvan ja viestinnän välillä. Hyvä johtaminen edellyttää: (Turvallisuuskomitea, 2017 b, 15)

- Selkeää johtovastuuta,
- tilannekuvan muodostamista,
- kriisiviestintää,
- tiedon jakamista ja sitä tukevia teknisiä ratkaisuja,
- toiminnan jatkuvuudenhallintaa ja
- yhteistoimintaa.

Organisaatioiden ja sen eri päätöksentekotasojen tilannetietoisuuden muodostamista tuetaan tilannekuvajärjestelyillä. Tilannekuva on osa hyvän johtamisen edellyttämää tilannetietoisuutta, jonka avulla voidaan hakea päätöksentekoon oikeita ratkaisuja perusteluineen ja seurauksineen ja havainnoida toimintaympäristön reaktioita. Tilannetietoisuutta on käsitelty luvussa 3.8. Seuraavissa luvuissa esitetään organisaatioiden ja kriittisen infrastruktuurin tilannetietoisuuden kehittämiseen liittyviä näkökulmia ja toimenpiteitä hyvinä käytänteinä ja toiminnan tavoitteina.

### 6.9.1 Tilannetietoisuus ylimmän johdon tasolla

Organisaation ylimmän johdon keskeisimpiin tehtäviin kyberturvallisuuden osalta voidaan katsoa kuuluvan toiminnan luottamuksen jatkuva kehittäminen ja ylläpitäminen osana kansallista kriittistä infrastruktuuria. Johdolta edellytetään konkreettisia strategisia valintoja sekä valittujen toimenpiteiden suorittamisen tukemista ja ohjaamista läpi koko organisaation. Ylimmän johdon tarpeisiin on tärkeä muodostaa kyberturvallisuusarvioinnin malli, jolla sidosryhmille voidaan viestittää organisaation kyberturvallisuuden tasoa.

Suomen kansallisen kyberturvallisuuden toimeenpano-ohjelma 2017 -2020 kokoaa yhteen julkisen ja yksityisen sektorin merkittävät kyberturvallisuutta parantavat hankkeet ja toimenpiteet vastuineen. Toimeenpano-ohjelman etenemisen auttaa eri organisaatioiden kyvykkyyksien kehittymisen seuraamista kyseisellä tarkastelujaksolla. Se sisältää laajasti vaikuttavia toimenpiteitä, joita kehitetään hallinnonalakohtaisilla toimenpiteillä sekä kyber- ja tietoturvallisuuden että prosessien toiminnan jatkuvuuden hallinnan kehittämiseen liittyvällä työllä. Samalla seurannasta voi muodostua kansallisen kyberturvallisuuden tilannetietoisuus. (Turvallisuuskomitea, 2017; Lehto, ym., 2018)

A National Cyber Security Index (NCSI) mittari on kehitetty kansallisen tason kyberturvallisuuteen liittyvän kyvykkyyden seurantaan. Se perustuu kahteentoista osa-alueeseen, jotka ovat järjestetty neljään ryhmään seuraavasti: (EGA. e-Governance Academy, 2017)

- Yleiset kyberturvallisuusindikaattorit.
- Kyberturvallisuuden perusindikaattorit.
- Tapahtumien ja kriisinhallinnan indikaattorit.
- Kansainväliset tapahtumaindikaattorit.

Jokaista kahtatoista osa-aluetta kohti mittarissa on neljä kyberturvallisuuden näkökulmaa. Nämä ovat lainsäädäntö, toimivat yksiköt, yhteistyöjärjestelyt ja erilaisten prosessien tulokset. Mittarin toiminta perustuu asiantuntijaryhmän arvoihin. Tuloksia voidaan käyttää toiminnan kehittymisen seuraamiseen.

Taulukossa 13 on esitetty NCSI-mittarin pohjalta jatkokehitetty tutkimusten ”Kyberturvallisuuden strateginen johtaminen Suomessa” ja ”Tapaustutkimus 1” yhteyksissä yritysten ja muiden organisaatioiden käyttöön kyberturvallisuuden organisaatiokohtaista kyvykkyyttä seuraava mittari. Siinä toiminnan arviointia suoritetaan tapahtumina neljällä alueella siten, että onko asetettu toiminnalle vaatimuksia, onko huomioitu liiketoiminnassa, onko sidosryhmäyhteistyötä ja onko saavutettu tuloksia (taulukossa on esimerkki kunkin kohdan pisteytyksestä). Organisaation mittarissa kyberturvallisuuden osa-alueet on järjestetty neljään ryhmään seuraavasti:

- Yleiset indikaattorit.
- Perustason indikaattorit.
- Tapahtuma- ja häiriöhallinnan indikaattorit.
- Kansallisen vaikutuksen indikaattorit.

TAULUKKO 13 Organisaation kyvykkyysmittarin rakenne.

| | VAATIMUKSET, 1 pist. | LIIKETOIMINTA, 2-4 pist. | SIDOSRYHMÄYHTEISTYÖ, 2 pist. | TULOKSET, 1-3 pist. |
|---|---|---|---|---|
| **YLEISET INDIKAATTORIT**<br>• Kyky kehittää organisaation kyberturvallisuuskulttuuria<br>• Kyky analysoida kybertoimintaympäristöään<br>• Tietoturvakoulutuksen laajuus | | | | |
| **PERUSTASON INDIKAATTORIT**<br>• Toiminnan resurssien varmistaminen<br>• Riskiarvioinnit<br>• Tietojärjestelmien toiminnan tasovaatimukset<br>• Toiminnan seuranta ja mittarit | | | | |
| **TAPAHTUMA- JA HÄIRIÖHALLINNAN INDIKAATTORIT**<br>• Häiriötilanteisiin varautumisen suunnitelmataso<br>• Tilannetietoisuus 24/7<br>• Kyky hallita häiriötilanteita<br>• Kyky palautua häiriötilanteista | | | | |
| **KANSALLISEN VAIKUTUSTEN INDIKAATTORIT**<br>• Toiminta kyberturvallisuuden toimintaverkostoissa | | | | |
| **MITTARIN PISTEET** | | | | |

Mittarin käyttöönoton voi katsoa kohdistuvan kansallisen kyberturvallisuuden toimeenpano-ohjelman (2017) tavoitteeseen ”Kansallinen kevyt kyberturvallisuusarviointi, jonka avulla organisaatiot voivat huolehtia minimitason saavuttamisesta turvallisuuden osalta, on laadittu”. Mittarin organisaatiokohtaisella käyttöönotolla voidaan vastata siis edellä mainittuun tavoitteeseen. Mittarin laaja käyttöönotto kriittisen infrastruktuurin organisaatioissa mahdollistaisi

koko alueen kyberturvallisuuden kehityksen seuraamisen samalla kun se palvelee yksittäisten organisaatioiden strategisen tason tarpeita.

### 6.9.2 Tilannetietoisuus operatiivisella tasolla

Operatiivisen tason toimenpiteillä edistetään strategisia tavoitteita. Niiden lähtökohtana tulee olla kohteen prosessien riskiarviointi ja arvioinnin perusteella tehtävät toimenpiteet. Operatiivisen tason käytännön toimenpiteillä varmistetaan prosessien jatkuvuuden hallintaa. Tavoitteena tulee olla toimintaprosessien tilannetietoisuuden aikaansaaminen päätöksen tueksi.

Kyberturvallisuuskeskus ja Huoltovarmuuskeskus ovat yritystasolla tunnistettuja yhteyspisteitä valtionhallinnossa. Kyberturvallisuuskeskuksen CERT-toiminnon tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista keräämällä tietoa tapahtumista ja tiedottamalla niistä. Huoltovarmuuskeskuksen yhteydessä toimii yhteistyöeliminä sektoreita ja pooleja, joista erityisesti digipoli tukevat yrityksiä kybertoimintaympäristön tilannekuvan kehittämisessä ja ylläpitämisessä. Huoltovarmuuskeskus yhdistää merkittävän osan viranomaisista sekä tietotekniikka-, tietoverkko ja tietoturva-alan yrityksistä. Yksityinen sektori tunnistaa oman tehtävänsä kansallisen kyberturvallisuuden edistämisessä. Viranomaisten ja yksityisen sektorin välille on luotu yhteistoimintamalleja siten, että toimijat muodostavat niissä keskenään toimintaverkostoja. Krivat-palvelu on kehitetty kriittisen infrastruktuurin organisaatioille yhteistyöverkoksi. Tarkoituksena on tehostaa organisaatioiden tilannetietoisuutta ja siten yhteistyötä suurhäiriötilanteissa ja nopeuttaa niistä toipumista.

Merkittävimpien kriittisen infrastruktuurin organisaatioiden teknillinen suojauskyky ja sitä kautta saatava havainnointikyky on hyvällä tasolla. Erilaiset yhteistoimintaverkostot ovat laajasti käytössä. Organisaatioiden ja Kyberturvallisuuskeskuksen kesken pidetään säännöllisesti yhteyttä. Poikkeavan toiminnan analysointikyky ja häiriötilanteiden hallintakyky perustuvat osaavaan henkilöstöön ja toimiviin yhteistyöverkostoihin. (Lehto, ym. 2017, 42)

### 6.9.3 Tilannetietoisuus taktisella tasolla

Tilannetietoisuuden luomisessa korostuvat niin tekninen, verkostomainen kuin hallinnollinenkin tilannekuva. Suomeen on viime vuosien aikana kehittynyt kyberturvallisuuden tilannekuvan muodostuminen eri toimijoiden tietojenvaihtomekanismien kautta. Kyse on niin kansallisesta kuin kansainvälisestäkin yhteistoiminnasta. ”Tietojenvaihdon sekä havaintokyvyn parantaminen on edelleen Suomessa kehitettävä asia kyberturvallisuudessa.” (Lehto, ym. 2017, 69)

Kriittisen infrastruktuurin toimijoilla on käytössään ICT-järjestelmissään suojaustekniikoita, jotka ulottuvat Internet-verkon ja organisaation sisäverkon rajapinnasta aina yksittäisen työaseman tai laitteen suojaamiseen. Nämä teknilliset ratkaisut mahdollistavat erilaisten haitalliseksi tunnistettujen tai normaalista poikkeavien havaintojen todentamisen. Tyypillisesti tekniikat liittyvät turvallisuustuotteisiin, kuten verkkoliikenteen analysointiin (lokitiedon hallinta, Secu-

rity Information and Event Management, SIEM), palomuurisuojaukseen, tunkeutumisen esto- (Intrusion Prevention System, IPS) ja havainnointijärjestelmiin (Intrustion Detecetion System, IDS) ja virustorjuntaan. Tilannekuva muodostuu keskitettyihin valvomoihin eli SOC-keskuksiin (Security Operation Center, SOC).

Keskitetyssä valvomossa tapahtuu eri sensoreista tulevien tietojen yhdistäminen ja tilannekohtaisen analyysin muodostaminen. Analyysin perusteella käynnistetään tarvittava toimenpiteet. Analysointikykyyn liittyvät myös organisaation mahdollisuudet hyödyntää kansainvälisistä tai kansallisista toimintaverkostoista saatavia tietoja. Valvomotoiminta keskittää asiantuntija henkilöstöä ja siten organisaatioon liittyvää kyvykkyyttä tulkita havaintoja ja johtaa niistä tarkoituksenmukaisia toimenpiteitä. Tyypillinen häiriötilanteiden tai poikkeavan toiminnan aiheuttama reagointi tapahtuu aluksi toimintaan valtuutetun henkilön käynnistämänä (Incident responce manager, IR-manager) tilannekuvan ja sen analysoinnin perusteella. Häiriön laajuus ja vakavuus vaikuttavat toimenpiteisiin. Nopean reagoinnin lisäksi voidaan tarvittaessa kutsua kokoon organisaation johtoryhmä päättämään toimenpiteiden laajentamisesta ja toimintaa tarvittavien resurssien kohdentamiseksi. Häiriötilanteen laajuuden perusteella voidaan tarvittaessa informoida organisaation koko johto aina hallitustasolle asti.

Edellä kuvatut teknilliset ratkaisut voivat olla organisaation omassa hallinnassa tai palvelu voi olla ulkoistettua tietoturvaoperaattorin vastuulle. Keskeisenä tavoitteena on liiketoiminnallisten prosessien tilannetietoisuus ja suojaaminen. Reaaliaikaisen tilannekuvan muodostamiseen liittyy myös erityisiä haasteita, joita on käsitelty ICT- ja teollisuusautomaatiojärjestelmien osalta luvussa 5.3.

Viranomaisten tuella on kehitetty tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä (HAVARO), joka palvelee huoltovarmuuskriittisiä toimijoita. HAVARO-järjestelmä mahdollistaa tilannekuvan aikaansaamisen organisaation verkon ulkopuolisessa rajapinnassa. Liikenteen seuraamisella voidaan tunnistaa normaalista poikkeava verkkoliikenne.

Havainnointikykyyn liittyy myös ennakkovaroitus, joka voidaan saada joko organisaation kansainvälisistä tai kansallisista toimintaverkostoista. Toiminnan keskiössä on aina organisaation henkilöstön kyvykkyys huomioida järjestelmissä mahdollisesti esiintyvää poikkeavaa toimintaa. Kokonaishavainnointikykyä voidaan kehittää benchmarkig-toiminnalla ja harjoittelemalla.

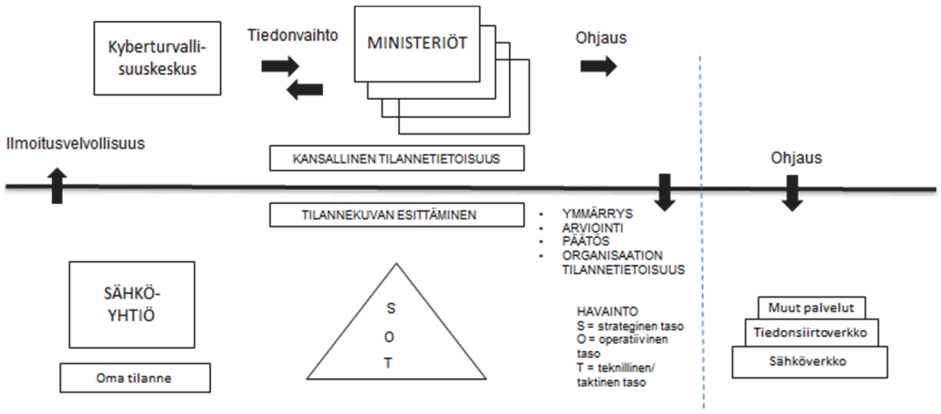
Organisaatiot toteuttavat häiriöiden tai poikkeavien tapahtumien analysointia omista lähtökohdistaan. Liiketoiminnallisten prosessien varmistaminen perustuu yhä enemmän tilannekohtaiseen analysointikykyyn. Suojaustoimenpiteiden tehostaminen tai esimerkiksi vaihtoehtoisten toimintamallien käyttöön ottaminen ovat toiminnan tärkeimpiä tavoitteita. Tilannekuvan ymmärrys ja analysointikyvykkyys ratkaisevat tarvittavien toimenpiteiden valinnan ja on näin ollen keskeisessä roolissa organisaation päätöksentekoprosessissa. Analysointikyvyn tulee mahdollistaa ilmiöiden vakavuusluokittelun ja kyberfyysisen näkymän aikaansaamisen.

Kansallisesti laajamittaisen häiriön tapauksessa kriittisen infrastruktuurin organisaatiot pitävät yhteyttä Kyberturvallisuuskeskukseen ja hyödyntävät virnaomaisverkoston lisäksi toimialan omaa verkostoa ja liiketoimintaan liittyviä

verkostojaan. Osalla kriittisen infrastruktuurin organisaatioista on NIS-direktiivin ilmoitusvelvollisuuden perusteella velvoite informoida viranomaisia häiriötilanteista.

### 6.9.4 Kriittisen infrastruktuurin tilannetietoisuus

NIS-direktiivi edellyttää selkeistä, tunnistettavista ja konkreettisista toimenpiteitä kansallisen tilannetiedonvaihdon kehittämiseksi. Yhteistyötahojen ja tietoa tuottavien toimijoiden tunnistaminen luovat edellytykset koko yhteiskunnan läpileikkaavaan tiedonvaihtoon ja sitä kautta tapahtuvan tilannetietoisuuden kehittämiselle. Kuviossa 20 on esitetty kansallisen tiedonvaihdon rakenne, joka mahdollistaa NIS-direktiivin mukaisen toiminnan.



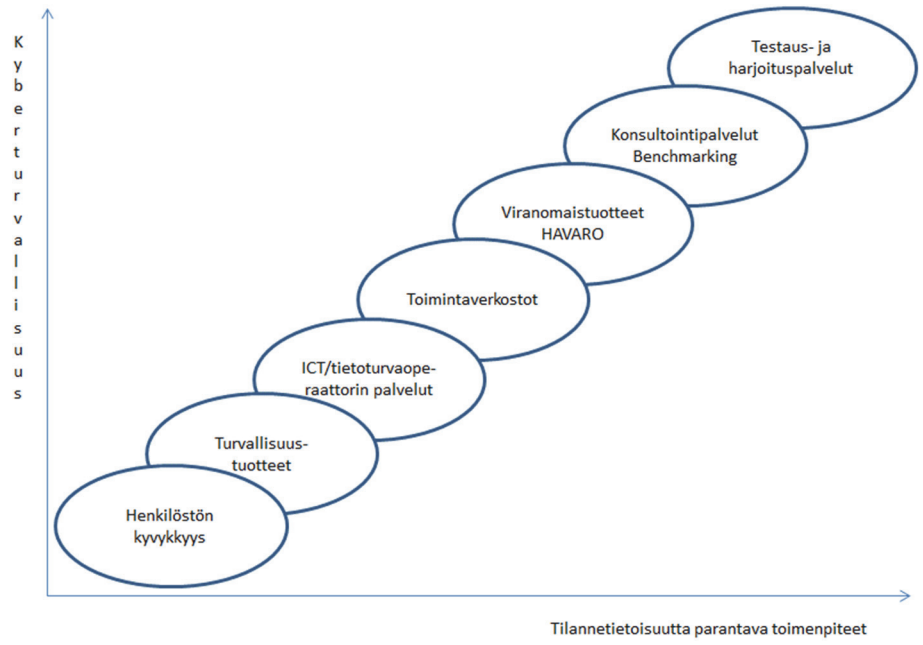

KUVIO 20 Tiedonvaihto kansallisella tasolla.

Eurooppalaisen organisaation, Energy Expert Cyber Security Platform (EECSP), asiantuntijaryhmän raportti ”Cyber Security in the Energy Sector” rohkaisee parhaiden käytäntöjen hyödyntämiseen tietojen jakamisessa esimerkiksi energia-alan tietojen osalta jonkinlaisen analysointikeskuksen tai analysointiprosessin kautta. Näin voidaan tukea eri sidosryhmien kautta tapahtuvaa parhaiden käytäntöjen jakamista ja niistä oppimista. Erityisesti uusien teknologioiden käyttöönottoihin liittyvät haasteet, markkinatoimijoiden keskinäisestä riippuvuudesta johtuvat haasteet tai energiajärjestelmien ja -verkkojen välisten yhteyksien muodostamat haasteet ovat tyypillisiä skenaarioita, joissa erityisesti voidaan hyötyä parhaista käytännön jakaminen. Lisäksi menettelyn avulla voidaan vaihtaa arkaluonteisia tietoja, jotka auttavat operaattoreita suojelemaan verkkoaan ennakoivasti. (EECSP, 2017)

Kansallisessa tiedonvaihdossa kriittisen infrastruktuurin organisaatio (kuvion 20 esimerkissä sähköyhtiö) muodostaa omista lähtökohdistaan kyberturvallisuuden tilannekuvan. Ideaalitapauksessa sen perustana ovat havainnot organisaation eri tasolta, jotka ovat strateginen, operatiivinen ja teknillinen/taktinen taso. Tietojen perusteella sähköyhtiö ylläpitää jatkuvaa omaa tilannetietoisuuttaan päätöksiensä tueksi. Kyberhäiriötilanteessa sähköyhtiö toimittaa ilmoitusvelvollisuuteensa perusteella tiedot tilannekohtaisesta analyysistään Kyberturvallisuuskeskukselle ja tarvittaessa myös vastuuministeriölle. Vastuuministeriö

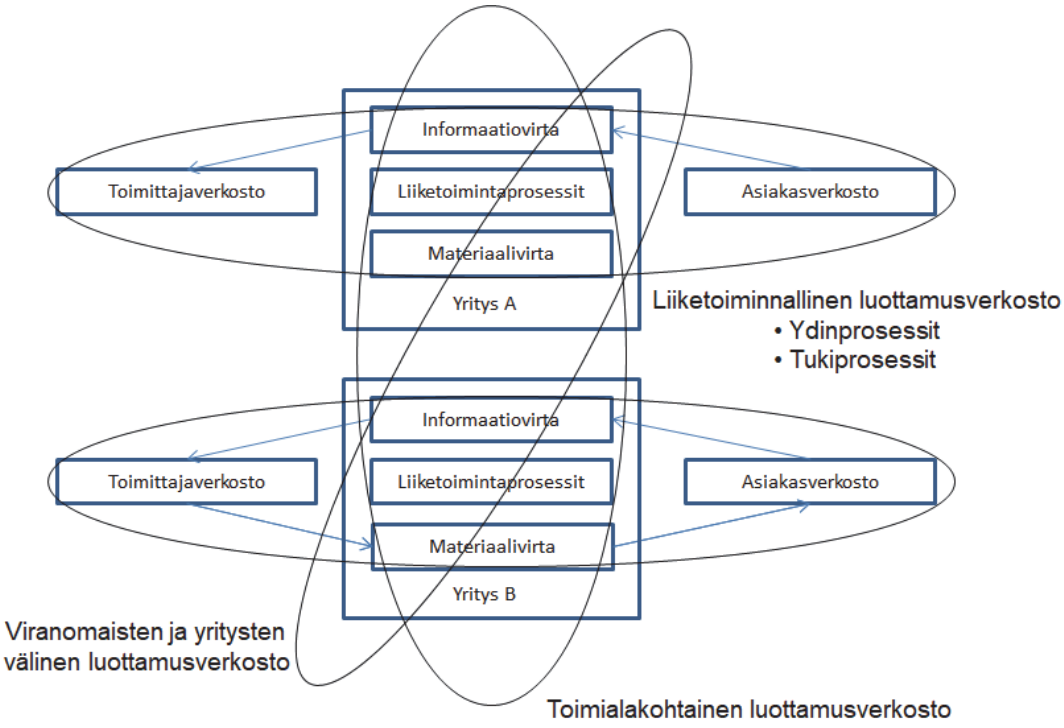
ja Kyberturvalliskeskus muodostavat tietojensa vaihdon perusteella kansallisen tilannetietoisuuden asiasta. Vastuuministeriö huolehtii asiaan liittyvistä tarvittavista ohjaustoimenpiteistä muille sidosryhmille ja vastuualansa organisaatioille. Kyberturvallisuuskeskus suorittaa myös jatkuvaa tiedonvaihtoa kriittisen infrastruktuurin organisaatioiden kanssa kyberturvallisuustilanteesta.

Kansallisesti merkittävimpiin kriittisen infrastruktuurin organisaatioihin on kehittynyt hyvä kybertilannekuva- ja havainnointikyky teknisten ja taktillisten valmiuksien osalta. Sitä parantaa myös organisaatioiden verkostoituminen toimialakohtaisesti ja osittain myös laajemmin. Verkostoitumista ja tietojen vaihtoa tukee hyvä viranomaisten ja yksityisen sektorin yhteistyö. Eri organisaatioiden hyvä tilannetietoisuus (tilannekuva ja sen analysointi) ja niiden sidosryhmien kautta tapahtuva tiedonvaihto on koko kansallisen kyberturvallisuuden olalta aivan keskeinen tekijä. Lähtökohtana on aina organisaation kyvykkyys tunnistaa käytössä olevissa järjestelmissä mahdollisesti esiintyvää poikkeavaa toimintaa sekä toimia luotettavasti ja järjestelmällisesti eri käyttötilanteissa. Henkilöstön kyberturvallisuuteen liittyvä kyvykkyyden kehittäminen on sidoksissa tilannetietoisuuden kehittämiseen. Ideaalitapauksessa toimintaa tuetaan teknillisillä järjestelmillä, käytettävissä olevin ICT- tai tietoturvaoperaattorien palveluin, toimintaverkostoa hyödyntämällä, viranomaisyhteistyöhön osallistumalla, hyödyntämällä konsultointipalveluja, benchmarking-toimintaa sekä testaamalla ja harjoittelemalla toimintaa. Kuvioon 21 on koottu tutkimuksessa esiin tulleita organisaation kyberturvallisuuden kyvykkyyttä edistäviä tekijöiden ja tilannetietoisuuden parantumisen välinen yhteys (Lehto, ym., 2018, 51,52).




KUVIO 21 Organisaation kybertilannetietoisuuden kehittäminen osana kokonaisvaltaista kyberturvallisuutta.

Väitöstyön taustatutkimuksissa (Lehto ym. 2017, Lehto ym., 2018) on korostunut Suomen kansallinen vahvuus organisaatioiden mahdollisuuksista erilaisten verkostojen hyödyntämiseen kyberturvallisuuden tiedonvaihdon osalta. Tässä yhteydessä organisaatioiden tiedonvaihtoon esitetään hyvinä käytänteinä kolmenlaisia luottamuksellisen tiedon vaihtoon soveltuvien verkostojen hyödyntämistä. Ne voidaan muodostaa liiketoiminnan yhteyteen tai jonkun toimialan organisaatioiden välille perustettavana luottamusverkostona siten, että verkostot voivat parhaimmillaan ulottua myös kansainväliseen yhteistyöhön. Molempia tiedonvaihdon verkostomalleja on jo kriittisen infrastruktuurin organisaatioilla osittain käytössä. Lisäksi kansallisesti toimii viranomaisten ja yksityisen sektorin välinen luottamusverkosto (Public Private Partnership, PPP-yhteistyö). Tämän verkostorakenteen yhtyeteen on luontevaa liittää NIS-direktiivin edellyttämiä ilmoitus- ja tiedonvaihtorakenteita. Kuvio 22 havainnollistaa edellä mainittuja luottamusverkostoja yrityskentässä.




KUVIO 22 Organisaation kybertilannetietoisuuden kehittämiseen liittyvät luottamusverkostot.

Erillisverkot-yhtiö on valtion kokonaan omistama erityistehtäväyhtiö ja sen päätehtävänä on turvata yhteiskunnan kriittinen johtaminen ja tietoyhteiskunnan palvelut kaikissa toimintaympäristöissä. Se tarjoaa viranomaisille ja huoltovarmuuskriittisille toimijoille turvalliset ja toimintavarmat ICT-palvelut. Tilannekuvan ja johtamisen alueella Erillisverkot-yhtiö tarjoaa KRIVAT-palvelua, joka on samalla keskinäinen toimintaverkosto kriittisen infrastruktuurin organisaatioille. Sen tarkoituksena on tehostaa organisaatioiden yhteistyötä suurhäiriötilanteissa

ja nopeuttaa niistä toipumista. KRIVAT-palvelualusta on siihen kuuluvien toimijoiden yhteisö, toimintamalli ja informaatiokanava. KRIVAT-palvelu tukee kriittisen infrastruktuurin organisaatioiden proaktiivista toimintaa varautumisessa toiminnan häiriötilanteisiin, joita ovat muun muassa myrskyt ja kyberhyökkäykset. Kriisin keskellä sen avulla hallinnoidaan työnjakoa. (Lehto, ym., 2018)

Yhteiskunnan elintärkeitä toimintoja ja organisaatioiden toimintaprosesseja uhkaavat kyberhyökkäykset edellyttävät yhteistyömenettelyjen mahdollistavan tiedonvaihdon lisäksi tehokkaista menettelyjä verkottuneen toiminnan johtamiseen ja päätöksentekoon.

John Boydin (1927-1997) OODA-silmukka tai päätöksentekosykli (Observation-Orientation-Decision-Action phases cycle, OODA-silmukka) mahdollistaa taktisen, operatiivisen ja strategisen ketteryyden johtamiseen ja päätöksentekoon. OODA-silmukkamallissa havainnoidaan toimintaympäristöä ja kerätään tietoja käynnissä olevista prosesseista, jolloin voidaan tehdä päätöksiä ja toteuttaa niitä prosessien edellyttämällä tavalla. (Boyd, 1995)

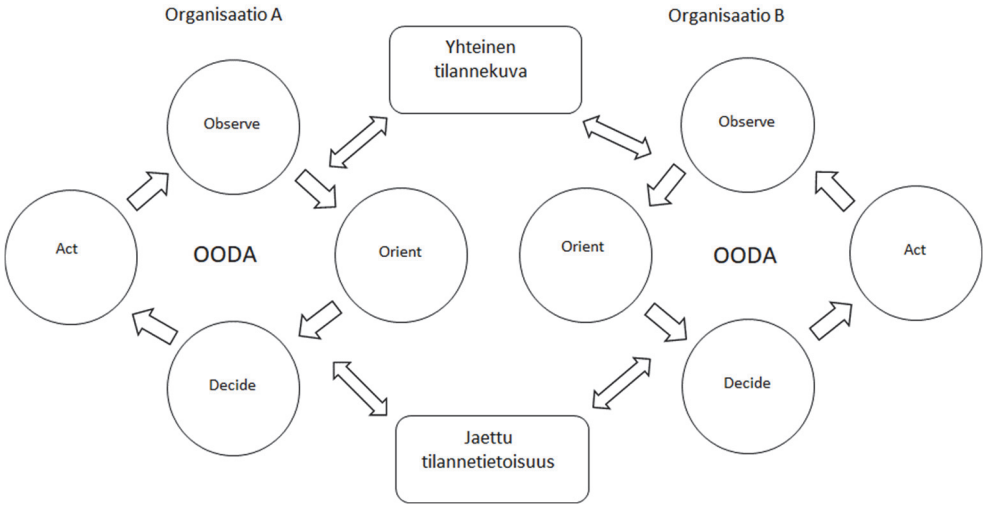
Tero Kokkonen on väitöstyössään (2016) käsitellyt OODA-silmukkamallin soveltuvuutta päätöksentekoon ja kyberpuolustustoimiin. OODA-silmukan perusmuoto edustaa sykliä, joka sisältää neljä vaihetta: havainnointi, suuntaus, päätös ja toiminta. Alun perin se on otettu käyttöön ilmavoimien operatiivisessa päätöksenteossa. Menettely on sovellettavissa myös kyberpuolustukseen. Siinä OODA-mallin toimii vaiheittain seuraavasti: havaintovaiheessa kerätään tietoja infrastruktuurista ja sen ilmiöistä; suuntaamisvaiheen aikana näitä tietoja analysoidaan; päätöksentekoprosessin aikana valitaan vastatoimenpiteet, tapauskohtaiset toimenpiteet, lieventämis- ja toipumistoimet; ja toimintavaiheen aikana näitä valittuja toimintoja käytetään. Uusi silmukkasykli alkaa uudella havaintovaiheella. (Kokkonen, 2016)

Martti Lehto (2018) on todennut, että OODA-silmukka on erityisen hyödyllinen kyberoperaatioiden mallinnuksessa ja hallinnassa. Kyberturvallisuuden tilannetta on tarkkailtava ja arvioitava useasta eri näkökulmasta, minkä jälkeen on tehtävä päätökset asianmukaisista toimista, jotka toteutetaan nopeammin kuin vastustaja. Toimija, joka pystyy sopeutumaan ja reagoimaan nopeimmin jatkuvasti muuttuviin kybertoimintaympäristöihin, hallitsee tilanteita. (Lehto M. & Neittaanmäki P. (Edit.), 2018)

ECHO-projekti (European network of Cybersecurity centres and competence Hub for innovation and Operations, ECHO) on osa EU-komission HORIZON 2020 hanketta vuosina 2019 – 2024. ECHO-projekti on Euroopan unionin ennakoivan kybersuojauksen tehostamista monialaisen yhteistyön avulla. Tutkimuskumppanit kehittävät hankekaudella kyberturvallisuuden tutkimus- ja osaamiskeskusten verkostoa. Osaamiskeskusajatus mahdollistaa monisektoristen toimintojen riippuvuuksien hallinnan, ennakkovaroitusjärjestelmän, Cyber Ranges -yhdistyksen ja laajentavan kumppanuuksien hallinnan. (European Commission)

Kyberturvallisuuden luottamusverkostoissa OODA-silmukka tarjoaa organisaatioiden käyttöön operatiivisten tilannekuvien, tilannetietoisuuden sekä kes-

kinäisen päätöksenteon menetelmän, jonka periaate on esitetty kuviossa 23. Tutkimusartikkelissa P7 käsitellään OODA-silmukkaa edellä mainitusta näkökulmasta. Artikkeli on myös osana ECHO-projektin konferenssiraportointia. ECHO-projektissa kehys voi tarjota ennakkovaroitusjärjestelmän kehittämisen kautta kansainvälisille luottamusverostoille johtamiseen rakenteen ja alustan, joka lisää kumppaneiden kyberturvallisuuden yhteistyötä ja tilannetietoisuutta.




KUVIO 23 OODA-silmukka organisaatioden tilannetietoisuudessa ja päätöksenteossa.

## 6.10 Toimenpiteiden toteuttaminen

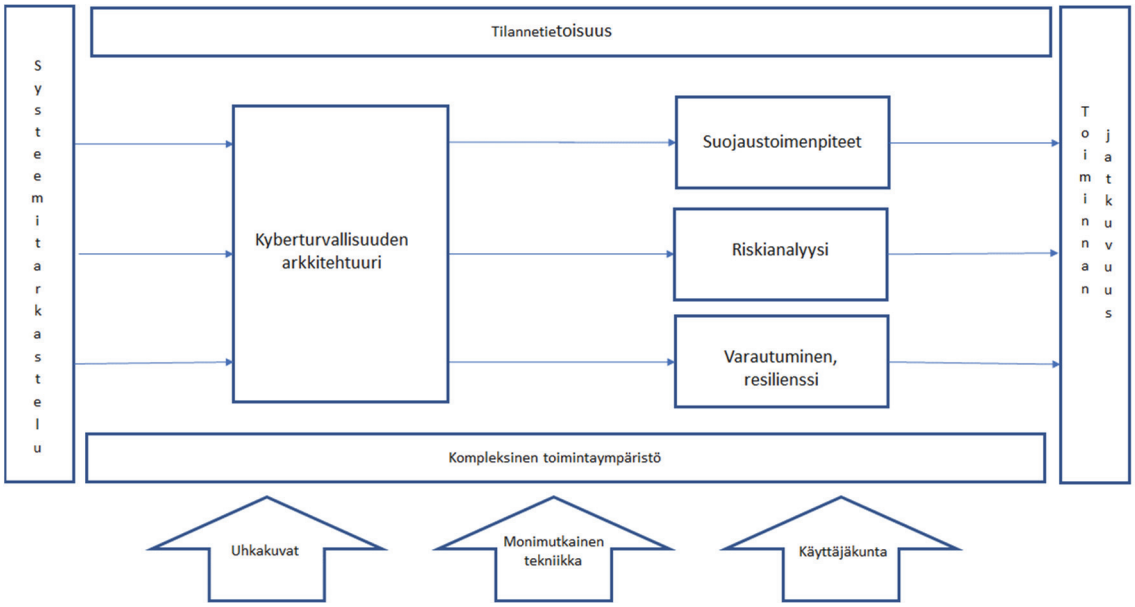
SSM-tutkimusprosessin vaiheeseen seitsemän, ongelmatilanteen parantaminen, ei sisälly menetelmää toimenpiteiden totuttamiseksi. Tässä luvussa kuvataan PDCA-menetelmää tutkimustulosten hyödyntämiseksi organisaation kyberturvallisuuden kehittämisessä. SSM-tutkimusprosessin vaiheeseen viisi kuuluu vertailu vaiheiden kaksi eli ”Tunnistettu ongelmatilanne” ja vaiheen neljä eli ”Käsitteelliset mallit muodostettuina” välillä ennen vaiheen kuusi muutostoimenpiteiden valintaa. Tässä tutkimuksessa vaihe viisi on korvattu toteutusvaiheessa sovellettavan PDCA-menetelmän sisältämällä vaikutusten arvioinnilla.

### 6.10.1 Kehitysehdotusten keskinäiset suhteet

Tutkimustulosten perusteella organisaation kyberturvallisuuden osalta voidaan systeemiajattelun kautta hahmottaa kompleksisen toimintaympäristön kokonaisvaltainen tarkastelu. Kyberturvallisuuden hallinnan kehittämisessä on oleellista tunnistaa kaikki ne haasteet, jotka liittyvät organisaation toiminnan jatkuvuuden hallintaan. Tilanteisiin varautumista on edellä kuvattu nelikentällä, jossa toiminnan jatkuvuutta varmistetaan niin, että uhkatekijät joko tunnetaan tai nii-

den olemassaolo tiedetään, mutta niiden vaikutus omaan tietoteknilliseen järjestelmään on tuntematon. Lisäksi on uhkia, joita ei mitenkään tunneta, mutta niissä voidaan tunnistaa toimintaa häiritsevien riskien esiintyminen. Viimeisenä nelikentässä on huomioitu ne tapaukset, joita ei voida käsitellä millään edellä mainituista menetelmistä, mutta tiedetään, että haitan tekijä voi aina vahingoittaa organisaation kyberturvallisuutta.

Edellä mainitun nelikentän kolmen ensimmäiseen tilanteen hallintaan tulee pyrkiä organisaatiokohtaisella kyberturvallisuusarkkitehtuuriin perustuvilla suojausratkaisulla ja huomioimalla riskit. Riskianalyysillä tuetaan toimintaa. Tapaukset, joita ei voida mitenkään tuntea ja siten ennakoida, esitetään hallittaviksi organisaation varautumissuunnittelun ja toiminnan resilienssin parantamisen kautta. Tilannetietoisuudella luodaan perusta tilannekohtaisille päätöksille. Kuviossa 24 on esitetty organisaation yhteydet systeemitarkastelun, kompleksisen toimintaympäristön, tilannetietoisuuden, aiemmin edellä mainittujen kehittämistoimenpiteiden ja toimintaprosessien jatkuvuuden hallinnan kesken.




KUVIO 24 Organisaation kyberturvallisuuden kehittämisehdotusten keskinäiset suhteet.

### 6.10.2 Toimenpiteiden implementointi

Väitöstutkimuksessa on selvitetty hyvien käytänteiden ja standardien perusteella menettelyjä kriittisen infrastruktuurin organisaation ICT-järjestelmien ja -laitteiden kyberturvallisuuden hallintaan ja siten koko organisaation toimintaprosessien jatkuvuuden hallintaan. Menettelyt liittyvät lopulta koko organisaation johtamiseen, laadunhallintaan ja toiminnan luottamuksen ylläpitämiseen. Kyberturvallisuuteen liittyviä toimia voidaan tarkastella, testata ja toimintaa voidaan kehittää ulkopuolisen tahon auditointina.

Kansainvälisessä organisaatioiden toimintaa koskevassa ISO/IEC 9000-standardisarjassa tuodaan esille, että laadunhallinta (Quality Management, QM) kuuluu osaksi laadukasta organisaation johtamista. Se on silloin osana organisaation johtamisjärjestelmää. Laadunhallinta tulee toteuttaa ensisijaisesti organisaation toiminnallisten prosessien hallinnan kautta. Tällöin toiminnan laatua voidaan myös arvioida ja mitata prosessien kautta. Väitöstutkimuksen tavoitteena oli luoda menettelyjä, joiden perusteella organisaation kyberturvallisuutta voidaan kehittää ja, joita vasten toimintaa voidaan arvioida. Organisaatio voi hakea toiminnalleen myös sertifiointia. Se antaa laadunvarmistuksen näkökulmasta organisaatiolle ulkopuolisen toimijan, auditoijan, todentamana käsityksen toiminnasta ja kehitystoimien tilanteesta. Auditointien ja sertifioinnin kautta toiminta kytkeytyy myös johtamisjärjestelmään.

**PDCA-menetelmä toiminnan kehittämistyökaluna**

Doddor Velev ja Nina Dobrinkova ovat organisaation tietotekniikka-alan yhtenäisen johtamisen ja hallinnon alustan kehittämistä käsittelevässä artikkelissaan ”The Logical Model of Unified, Innovative Platform for Automation and Management of Standards (PAMS)” (2019) selvittäneet useisiin kansainvälisesti tunnustettuihin standardeihin perustuvia menettelyjä, jotka mallintavat alustaan liittyviä prosesseja. Selvityksen perusteella on todettu, että standardeilla on monimuotoisuudestaan huolimatta monia yhteisiä elementtejä. Yksi esimerkki yhteisistä elementeistä on PDCA-menetelmä (Plan, Do, Check, Act, PDCA), joka tunnetaan myös nimellä Demingin laatuympyrä. Sitä käytetään standardeissa organisaation toiminnan jatkuvan parantamisen menetelmänä. PDCA-malli on mainittu useissa standardeissa, joista tässä yhteydessä mainitaan ISO/IEC 9000- ja ISO/IEC 27000- standardiperheet. Standardeissa menetelmää käytetään erilaisissa konteksteissa, kuten organisaatioon liittyvät kehittämistarpeet, prosessijohtaminen, riskien määrittäminen ja arviointi sekä eri sidosryhmien vaatimukset. (Velev & Dobrinkova, 2019, 116)

ISO/IEC 9000-standardiperheen vuoden 2015-standardi suosittelee organisaation toiminnan järjestelmälliseen kehittämiseen PDCA-menetelmää. PDCA-malli soveltuu myös standardin ISO/IEC 27001 mukaan tietoturvan johtamiseen, koska sen avulla organisaatio voi varmistaa jatkuvan parantamisen vaatimuksen toteutumisen (Suomen Standardisoimisliitto SFS ry., 2013, 22). ISO/IEC 27001-standardin mukaisessa PDCA-mallissa kuvataan jatkuvan kehittämisen prosessi, jonka avulla tietoturvallisuuden hallintajärjestelmää pidetään yllä.

Standardissa noudatetaan prosessimaista toimintamallia, johon yhdistyy PDCA-malli (suunnittele, toteuta, arvioi, toimi) ja riskiperusteinen ajattelu. Toimintamallin avulla organisaatio voi huomioida kaikki prosessinsa ja niiden vuorovaikutukset. PDCA-mallilla puolestaan voidaan varmistaa, että sen prosesseille on riittävät resurssit ja kehitystoimenpiteiden hallinta ja, että parantamismahdollisuudet määritetään ja hyödynnetään. Riskiperusteisen ajattelun avulla organisaatio voi tunnistaa ne tekijät, jotka voivat vaikuttaa prosessien toimintaan ja siten valita käyttöön ehkäiseviä hallintakeinoja. (Suomen Standardisoimisliitto SFS ry., 2016, 95)

PDCA-menetelmä perustuu neljän kehitysvaiheen kiertoon. Ensimmäinen vaihe koostuu suunnittelusta (Plan). Toimenpide edellyttää kohteen analysointia ja sen pohjalta laadittuja toimenpidevaihtoehtojen muodostamista. Toteutusvaiheessa (Do) pannaan toimeen valitut toimenpiteet. Tämän jälkeen tarkistetaan (Check) käytännössä, että toimenpiteet ovat toimivia, tehokaita ja tarkoituksenmukaisia. Viimeisessä ympyrämallin vaiheessa tehdään valituille toimenpiteille tarvittaessa korjaukset (Act) ja vakiinnutetaan ne käytäntöön. Yhden toteutuskierroksen jälkeen ympyrässä palataan alkuun ja uuden tilanneanalyysin perusteella valitut kehittämistoimenpiteet aloittavat uuden kierroksen. Kehittäminen voi siten edetä päättymättömänä prosessina, jossa jokaisen ympyrän kierroksen jälkeen ollaan uudella toiminnan tasolla. Menetelmä perustuu jatkuvan oppimisen ja toiminnan jatkuvan kehittämisen ajatukseen. (9001 quality., 2020)

Ympyrän yhden kierroksen toimenpiteet ovat lähes poikkeuksetta paljon suunnittelua vaativia ja toimenpiteiden osalta aikaa vieviä, joten kehityskierroksen toteuttamiseen on syytä varata riittävästi aikaa. Toimenpiteiden priorisointi ja valinta on siten tärkeää suhteuttaa niiden toteuttamiseen tarvittaviin resursseihin. Organisaation kehitystoiminnan kypsyysaste vaikuttaa toimenpiteiden toteutuksen arviointiin. Aiemmin luvussa 4.3.5 esillä olleen CATWOE-analyysin perusteella organisaation kehitystoimenpiteiden implementoinnin eri tekijät voidaan tunnistaa seuraavasti:

1. **Asiakas** (Customer):

Organisaation kyberturvallisuuden toimenpiteiden implementointi kehittää kriittisen infrastruktuurin palveluja tai tuotteita. Toimenpiteet hyödyttävät myös sisäisiä sidosryhmiä eli ydin- ja tukiprosessien asiakkuuksia sekä verkottuneeseen toimintaan liittyviä sidosryhmiä.

2. **Toimija** (Actor):

Organisaation kyberturvallisuuden kehittämisen ensisijaisia toimijoita ovat johtajat ja esimiehet strategisella-, operatiivisella- ja teknisellä/taktisella tasolla. He mahdollistavat eri päätöksentekotasoilla tarvittavat toimenpiteet. Toimijoina ovat myös organisaatioiden koko henkilöstö.

3. **Muutosprosessi** (Transformation process):

Organisaation kyberturvallisuuteen liittyvän kehitys- tai muutosprosessin syötteet muodostavat toimintaympäristön uhkista, haavoittuvuuksista ja tarpeesta reagoida niihin proaktiivisesti. Kehitys- tai muutosprosessin avulla kehitetään kyvykkyyttä vastata uhkiin ja haavoittuvuuksiin. Prosessin ulostulosta saatavan suorite on aiempaa parempi vaste organisaation toimintaprosessien jatkuvuuden hallintaan. Muutossyötteet voivat tulla myös organisaation ulkopuolelta kyberturvallisuuden viranomaisohjauksena. ICT-järjestelmien tai -laitteiden vanheneminen tai niiden käyttötavasta johtuvat muutostarpeet voivat ohjata myös muutosprosessia.

4. **Näkökulma** (World View):

Digitalisaatiosta johtuva organisaation globaalin kybertoimintaympäristön jatkuva muuttuminen haastaa tilannetietoisuuden ylläpitämistä. Tilannetietoisuuden ylläpitämiseen liittyy organisaation verkottumisen näkökulma. Verkostoa

on voitu jo hyödyntää tilannetietoisuuden osalta. Parhaimmillaan sitä voi muodostua tilannetietoisuuden ekosysteemi. Kyberturvallisuuden jatkuvan parantamisen periaatteeseen voidaan liittää johtamisen strateginen-, operatiivinen- tai taktinen näkökulma. Taktisen näkökulmaan kytkeytyy tietotekniikasta aiheutuva teknillinen näkökulma. Organisaation kyberturvallisuuden kyvykkyyden kokonaisnäkökulman muodostavat henkilöt, prosessit ja tekniikat. Organisaatio voi kehitystoimenpiteiden toteutuksessa hyödyntää yliopistoja, korkeakouluja, tutkimuslaitokset ja muita asiantuntijatahoja näkökulmiensa laajentamiseen ja teknillisten ratkaisujen etsintään. Teknologisesta näkökulmaa voidaan laajentaa selvittämällä uusien tekniikoiden hyödyntämismahdollisuuksia. Kriittisen infrastruktuurin ohjaustahot muodostavat kansallisen kokonaisturvallisuuden ja EU-tason näkökulmat. Näihin näkökulmiin kytkeytyy kansallinen huoltovarmuus.

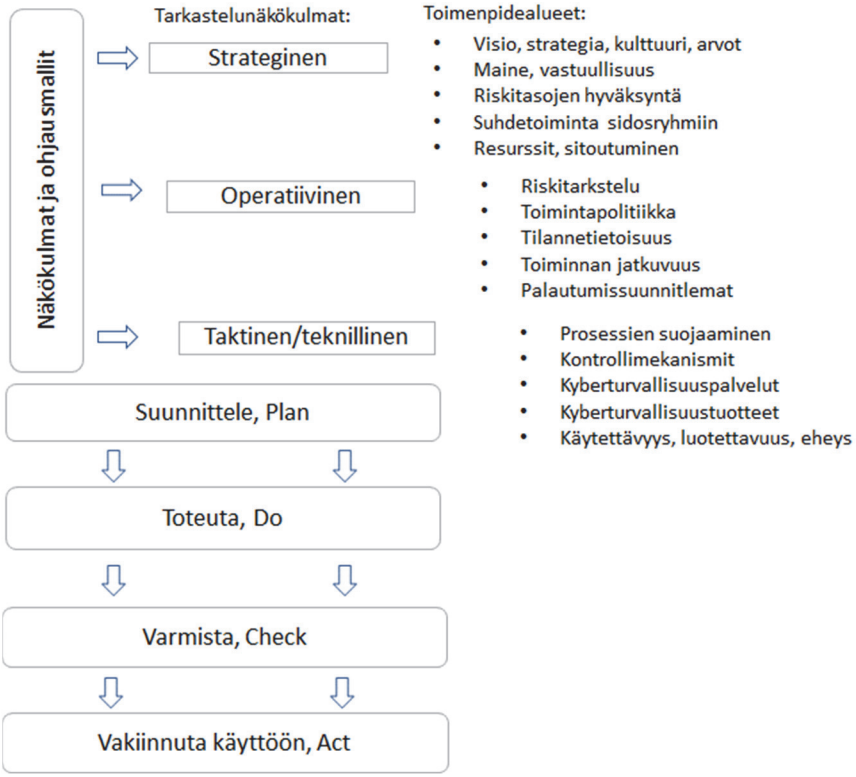
5. **Omistaja** (Owner):

Organisaation kyberturvallisuuden kehittämiseen liittyvien ongelmien omistajat sisältyvät strategiselle, operatiiviselle tai teknilliselle/taktiselle päätöksentekotasolle. Ensisijaiset omistajat ovat näiden päätöksentekotasoilla olevia johtajia ja esimiehiä. He voivat vaikuttaa muutoksen toteutukseen eniten. Myös organisaation henkilöstö kuuluu ongelman omistajiin. Henkilöstön kyberturvallisuuden kyvykkyys ratkaisee lopulta toimenpiteiden onnistumisen. Henkilöstön kyvykkyys on myös ratkaisevassa asemassa ongelmiin liittyvän tilannetietoisuuden rakentumisessa. Organisaation kumppanit toimivat ongelma omistajina silloin, kun kehittämistoimenpiteitä vaaditaan koko toimintaverkostoon. Kriittisen infrastruktuurin ohjaustahot voivat myös näkyä ongelman omistajina kansallisesta kokonaisturvallisuuden näkökulmasta tarkasteltuna. Tässä roolissa on Huoltovarmuuskeskus tuottanut ratkaisulähtöisiä kyberturvallisuuden tutkimushankkeita ja palveluja alueen organisaatioiden käyttöön.

6. **Toimintaympäristö** (Environment):

Organisaation ulkoinen kybertoimintaympäristö on jatkuvassa muutostilassa. Digitalisaatio tuo uusia ulottuvuuksia siihen muun muassa teknologian kehityksen myötä. Organisaatiolla voi olla tarve laajentaa toimintaansa uusille liiketoiminta-alueille teknologian kehityksen vuoksi. Organisaatiolla ei kaikissa tilanteissa ole myöskään mahdollisuutta kehittää kyberturvallisuuttaan ja siihen liittyvää kyvykkyyttään täysin vapaasti ja vain omista lähtökohdistaan. Kehittämisen tulee aina perustua voimassa oleviin lakeihin ja asetuksiin. Myös hallinnonalankohtaiset normit ja ohjeet voivat asettaa vaatimuksia kehittämistoimenpiteisiin. Toimintaympäristöön voi liittyä myös organisaatioon kohdistuvia rajallisia resursseja niin teknologian kuin osaamisenkin osalta.

Luvussa 6.5 on esitetty organisaation kyberturvallisuuden arkkitehtuurikehys. Kuviossa 25 arkkitehtuurikehys on yhdistetty PDCA-menetelmään. Kuviossa ilmenevät arkkitehtuurin näkökulmat pääasiallisine sisältöineen ja kehitystoimenpiteiden implementointiprosessi PDCA-menetelmän vaiheineen.




KUVIO 25 Kyberturvallisuuden kehitystoimenpiteiden implementointi.

Ohessa on esitetty vaiheittain malli kyberturvallisuuden johtamisen kehittämiseksi kuvion 25 PDCA-kehitysmenetelmää hyödyntäen. Malliesimerkki PDCA-kehitysmenetelmän vaiheista:

**PLAN, suunnitteluvaihe**

- Muodosta nykytilakuva:
  - muutosprosessin tarve
  - näkökulmat
  - toimintaympäristö
- Analysoi ongelmat ja määritä korjaavat toimenpiteet:
  - arvio toteutusmahdollisuudet
  - määritä käytettävissä olevat toimenpiteet
- Valitse kehityskohde (toimenpiteet tai -alueet).
- Määritä tavoita ja aikataulu.
- Varaa resurssit ja valtuuta vastuutahot.

**DO, toteutusvaihe**

- Huomio asiakkaat, toimijat, omistajat, prosessit ja tekniikka.
- Toteuta valitut toimenpiteet.
- Järjestä henkilöstön informointi ja koulutus.

**CHECK, tarkistusvaihe**

- Analysoi toimenpiteiden vaikutukset:
  - vertaa analyysin tuloksia suunnitteluvaiheeseen
  - palaa kohtaan, mikäli tavoitteet eivät tyydytä

**ACT; vakiinnuta toimenpiteet**

- Huomio sidosryhmät.
- Vakiinnuta valitut kehitystoimenpiteet:
  - päivitä tarvittavat ohjeet, prosessit ja teknilliset ratkaisut
  - jatka henkilöstön koulutusta
- Tee johtopäätökset ja tulevaisuuden suunnitelmat:
  - jatka kehittämistä uusilla tavoitteilla
  - päivitä uhka- ja riskiarvioinnit
  - paranna toimintaa jatkuvasti

Edellä esitetyn CATWOE-analyysin mukaisia systeemin osatekijöitä voidaan hyödyntää kehitystoimenpiteissä. Menetelmässä suunnitteluvaihe ratkaisee kehityskohteen valinnan ja sen toteutuksen vastuujaon eri päätöksentekotasoille organisaatiossa.

# 7 JOHTOPÄÄTÖKSET

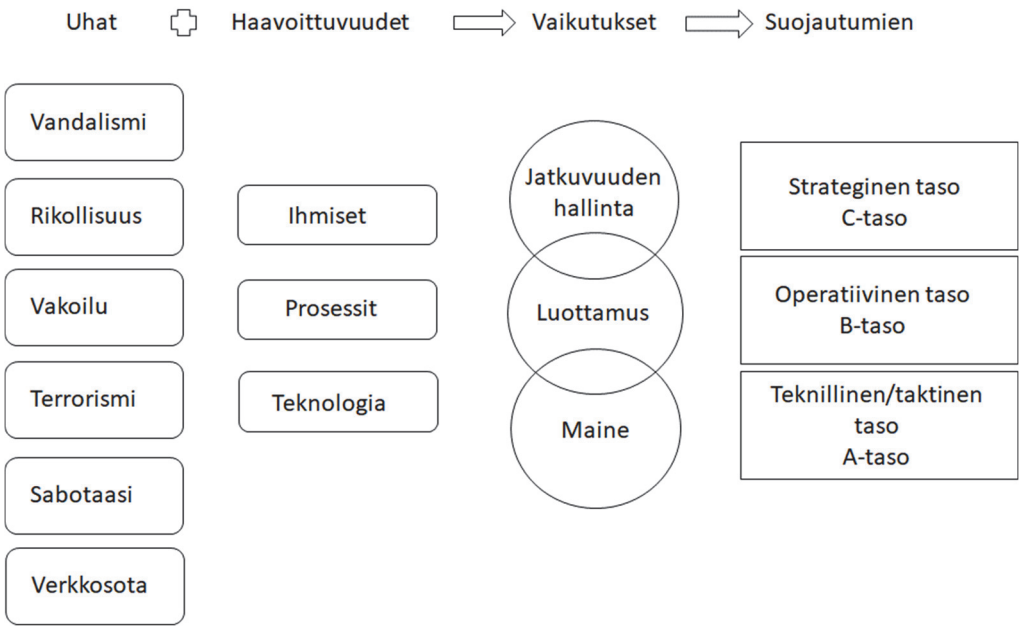
## 7.1 Yhteenveto tutkimustuloksista

Väitöstutkimuksen aikana kansallisen kriittisen infrastruktuurin suurimpiin organisaatioihin suoritetut haastattelut osoittivat, että kyseiset organisaatiot tunnistavat kyberuhkia, omaavat kyberturvallisuuden tilannetietoisuuden järjestelyjä, häiriötapausten analysointikyvykkyyttä ja vaihtavat uhkakuviin liittyviä tietoja verkostojaan hyödyntäen. Kyberturvallisuuteen liittyvistä riskiarvioinneista ja arviointeihin perustuvista toimenpidevaihtoehtojen analyyseista on tulossa yhä merkittävämpi osa organisaatioiden johtamista ja liiketoiminnan prosessien jatkuvuuden hallintaa. Haastatteluissa mukana olleilla yksityisen sektorin organisaatioilla on resursseja hyödyntää parhaita tietoturvaratkaisuja ja -palveluja. Osin julkisella sektorilla ja Helsingin kappakamarin tutkimusten mukaan myös muissa yrityskokoluokissa kybertuvallisuuden hallinnan kokonaistilanne on haasteellisempi. Haasteita liittyy myös yleisesti organisaatioiden kyberturvallisuustoimenpiteiden läpinäkyvyyteen liiketoimintaprosessien ja -verkostojen, kumppanuuksien ja muiden sidosryhmien osalta. Myös ICT- ja automaatiojärjestelmien teknillisen tason tilannetietoisuuksissa on kehittämistarvetta.

Organisaation kohtaamat kyberuhkat ja toimintaan liittyvät haavoittuvuudet mahdollistavat kyberhyökkäykset toimintaprosesseja vastaa. Prosessijohtamiseen ja systeemikäsitykseen liitettynä merkittävästi toimintaa häiritseviä kyberhyökkäyksiä voidaan pitää erityissyistä johtuvana prosessivaihteluna, joka heijastuu toiminnan jatkuvuuden varmistamiseen, organisaation toiminnan luotettavuuteen ja maineeseen. Nämä syyt eivät ole jatkuvasti läsnä prosessissa, eivätkä ole siten systeemistä itsestään johtuvia. Organisaation kybertoimintaympäristö aiheuttaa myös toimintaprosesseihin systeemistä itsestään johtuvaa vaihtelua muun muassa jatkuvina Internet-verkon kautta tapahtuvina tunkeutumisyrityksinä, ICT-laitteiden virheellisinä käyttötoimintoina tai laitevikoina. Organisaation johtamisessa onkin edellä mainitut syyt erotettava toisistaan.

Tapaustutkimuksissa 1 ja 2 on käsitelty yksityisen sektorin sähköyhtiön ja julkisen sektorin sairaalan ICT- ja automaatiojärjestelmiä ja niihin liittyvä kyberturvallisuuden näkökulmia. Tapaustutkimukset kuvaavat kriittiseen infrastruktuuriin organisaatioiden ja järjestelmien monialaisuutta. Väitöstutkimuksessa tuodaan esille, että laajoissa kybertoimintaympäristössä erityisistä syistä aiheutuvaan poikkeavaan toimintaan voidaan vaikuttaa kokonaisuudella, jossa kehitetään suojautumista, riskitarkastelua ja varautumista. Toimenpiteet pienentävät myös systeemistä itsestään johtuvaa vaihtelua. Organisaation käytännön toimenpiteet tuleekin pyrkiä kohdistamaan kattavasti kyberturvallisuuden kokonaisvaltaiseen tarkasteluun ja toteutukseen.

Väitöstyön keskeisimpään kysymykseen menettelyistä kriittisen infrastruktuurin organisaation kyberturvallisuuden johtamisessa ja kehittämisessä esitetään tavoitteeksi proaktiivista toimintaa, jonka avulla toiminnan jatkuvuutta, luottamusta ja mainetta voidaan ylläpitää. Toiminnan häiriöitä voidaan tunnistaa sekä niitä voidaan käsitellä tilannetietoisuutta ja kokonaisaltaista systeemiajattelua kehittämällä. Organisaatiossa ihmiset, prosessit ja käytettävät teknologiat muodostavat kyberturvallisuuden kyvykkyydet, mutta ne sisältävät myös haavoittuvuuksia. Väitöstyössä on esitetty kokonaisvaltainen systeemitarkastelu organisaation kyberturvallisuuden proaktiiviseen hallintaan. Se muodostuu viisikerroksisesta kyberrakenteesta ja strategisen, operatiivisen ja teknillisen/taktisen tason näkökulmista. Näkökulmat pitävät puolestaan sisällään kartoituksen organisaation luottamusta lisäävistä toimenpiteistä kybertoimintaympäristössä. Systeemitarkastelusta, näkökulmista ja toimenpiteistä on muodostettu organisaation kyberturvallisuuteen arkkitehtuurikehikko. Kehittämistoimenpiteitä voidaan edistää kattavasti arkkitehtuuria hyödyntämällä. Se tarkoittaa kyberturvallisuuden johtamis- ja kehittämistoimenpiteitä kaikilla organisaation päätöksentekotasoilla (strateginen, operatiivinen, teknillinen/taktinen). Kuvio 26 havainnollistaa vastausta keskeisimpään tutkimuskysymykseen (Lehto, 2019, muokattu). Kuvion mukaisesti organisaation päätöksentekotasoista voidaan käyttää nimityksinä C-taso, B-taso ja A-taso. D-tasoksi voidaan tarvittaessa nimetä organisaation kumppanit ja muut ulkopuoliset sidosryhmät. Organisaatio voi edellyttää D-tasolta myös kyberturvallisuutta edistäviä toimenpiteitä, jolloin voidaan myös parantaa näkymää toimintaverkostoon.




KUVIO 26 Organisaation kyberturvallisuuden kehittämisen kokonaisuus.

Väitöstyön tutkimuksellisen pääkysymyksen osalta organisaation proaktiivisen toiminnan kehittäminen koostuu seuraavista kohdista:

- ICT-infrastruktuurin vyöhykesuojaukseen integroiduilla uuden teknologian ratkaisuilla voidaan parantaa suojausta järjestelmätasoilla. Esimerkiksi tekoälyn kyvykkyyttä voidaan hyödyntää datan sekä tapahtumien analyyseissä ja havaintojen läpikäynnissä. Lohkoketjuteknologiaa voidaan hyödyntää tietojen ja sopimusten suojauksessa. Virtualisointitekniikka suojaustoimenpiteenä voi jatkossa mahdollistaa tietoteknisten prosessien aiempaa paremman suojaamisen. RFID-tekniikkaa puolestaan voidaan soveltaa laitevalvonnassa. Uuden teknologian ratkaisuehdotuksia on kohdistettu viitekehyksen viidelle eri kerroksille, jolloin niiden yhteisvaikutuksella voidaan tavoitella systeemitason integroitua suojauksen kehittämistä.
- Organisaation toiminnan ja järjestelmien kompleksisuus tekee mahdottomaksi kokonaan eliminoida uhkia ja haavoittuvuuksia sekä havaita ja jäljittää tunkeutumisia systeemin sisälle. Tilanteessa voidaan tunnistaa sekä uhkia ja haavoittuvuuksia, mutta niiden vaikutukset toiminnan jatkuvuuden hallintaa, luottamukseen ja maineeseen muodostavat riskejä. Tämän vuoksi toisena menettelynä edellä mainittuja suojaustoimenpiteitä täydentämään tarvitaan organisaatioon kattavasti laadittavia kyberturvallisuuden riskitarkasteluja ja niiden jatkuvaa ylläpitämistä.
- Organisaation kyberturvallisuuteen liittyy mahdollisuus tapahtumiin, jotka ovat edeltä ajateltuna tuntemattomia ja niiden vaikutukset voivat olla myös tuntemattomia. Kyberturvallisuuden tilanteeseen ja siten toiminnan jatkuvuuden varmistamiseen liittyy epämääräisyyttä ja epävarmuutta. Toiminnan jatkuvuuden varmistamiseen ja edellä mainittuja me-

nettelyjä täydentämään kolmantena menettelynä tarvitaan varautumissuunnitelmien laadintaa siten, että toiminnan resilienssiä voidaan parantaa. Toimenpiteillä edistetään prosessien jatkuvuuden varmistamista toimintaympäristön häiriötilanteissa koko kriittisen infrastruktuurin alueella.

- Organisaation tilannetietoisuuden kehittämiseen liittyvä tarve voidaan muodostaa tarkastelemalla tilannetietoisuuden edistämistä jokaisella päätöksentekotasolla. Strategisella ja operatiivisella tasolla voidaan hyödyntää organisaation kansallisia ja kansainvälisiä verkostoja. Erityistä huomiota tulee kiinnittää ratkaisuihin teknillisen tason tilannekuvan kehittämisessä. Kattavalla tilannetietoisuudella ja siihen liittyvällä organisaation tilannekohtaisella kyvykkyydellä tuetaan koko kriittisen infrastruktuurin toimintaa.

Kriittisen infrastruktuurin organisaatioiden tuottaessa yhteiskunnan toiminnan kannalta katsottuna keskeisiä palveluja, niin kehitystoimenpiteiden suorittamista edellyttää myös normipohja. Normien ja ohjeiden tarkoituksenmukainen hyödyntäminen laajassa mielessä edesauttaa kehitystoimenpiteitä. Normit voivat asettaa myös velvoitteita organisaatiolle. Tässä tarkoituksessa tulee esille EU-parlamentin verkko- ja informaatioturvallisuuden direktiivi eli NIS-direktiivi.

Väitöstyössä esitettävien organisaation kyberturvallisuuden kehittämistoimenpiteiden implementointiin voidaan soveltaa toiminnan kehittämisen PDCA-menetelmää. Laadunhallinnan näkökulmasta kehittäminen näyttäytyy osana laadukasta organisaation johtamista ja johtamisjärjestelmää. Tällöin kehitystoimenpiteiden edistymistä voidaan seurata toiminnan mittareilla, sisäisin auditoinnein ja katselmointien avulla. Tarvittaessa arviointi voi tapahtua organisaatiolle ulkopuolisen toimijan, auditoijan, todentamana käsityksenä kehitystoimien tilanteesta.

Tutkimustulokset osoittavat, että organisaatioiden eri kokoluokissa on huomattavia eroja kyberturvallisuuden kehittämiseen liittyvissä toimenpiteissä. Isojen yritysten osalta kyberturvallisuuden valmiudet ovat jo kehittyneet myönteiseen suuntaan. Osassa organisaatioita kattavat suojaustoimenpiteet ovat vasta käynnistymässä ja toimenpiteiden resursoinneissa on eroja. Väitöstyön kyberturvallisuuden johtamisen ja kehittämisen mallien ja toimenpiteiden avulla voidaan parantaa organisaatioiden kokoluokista riippumatta niiden proaktiivista toimintaa globaalissa kyberuhkaympäristössä. Niiden käyttöönotolla edistetään erityisesti toimintaprosessien jatkuvuuden hallintaa sekä luottamuksen ja maineen ylläpitämistä, joilla on merkittävää vaikutusta myös organisaatioiden kilpailuetuun markkinoilla. Toimivia tiedonvaihdon verkostomalleja hyödyntämällä ja jatkokehittämällä parannetaan kyberturvallisuustoimenpiteiden läpinäkyvyyttä koko verkostossa, kumppanuuksissa ja sidosryhmäyhteistyössä. Lisäksi kansallisesti on toiminnassa viranomaisten ja yksityisen sektorin välinen luottamusverkosto (Public Private Partnership, PPP-yhteistyö). Kehitystoimenpiteillä edistetään myös sekä kansallista kilpailuetua ja huoltovarmuutta että NIS-direktiivin tavoitteita. Organisaatioiden verkostorakenteen yhtyeteen on luontevaa

liittää muun muassa NIS-direktiivin edellyttämiä ilmoitus- ja tiedonvaihtorakenteita.

## 7.2 Pohdinta väitöstutkimuksen toteutuksesta

Väitöstutkimuksen attribuutit ovat kyberturvallisuus, kansallinen kriittinen infrastruktuuri, siihen liittyvä organisaatio, tietoteknillinen järjestelmä ja sen laitteet. Kokonaisuudesta muodostuu kompleksinen systeemien systeemi. Pehmeä systeemimetodologia on kehitetty kompleksisten organisaatiokokonaisuuksien tutkimiseen.

Suomalainen asiasanasto- ja ontologiapalvelu toteaa pehmeästä systeemimetodologiasta (SSM), että se on toimintatutkimukseen pohjautuva menetelmä. Tulevaisuudentutkimuksessa menetelmän avulla pyritään löytämään yhteydet päätöksentekoyksiköiden tavoitteiden asettelun, tulevaisuuden tutkimuksen tuottamien visioiden ja nykyisyyttä koskevan itseymmärryksen välille. Tiedoista voidaan synnyttään näkemys muutosprosessista, joka tarvitaan varauduttaessa mahdollisiin tulevaisuuden näkymiin. (Suomalainen asiasanasto- ja ontologiapalvelu, 2019)

SSM:n käytön valikoituminen väitöstyön tutkimusmenetelmäksi tapahtui jo tutkimuksen alussa, koska organisaation kyberturvallisuus, sekä sen kehittäminen ja johtaminen olivat lähtökohtaiset tutkimuksen näkökulmat. Myös käsitys tutkimusalueen kompleksisuudesta tuki valintaa. Väitöstutkimuksen muut attribuutit kuten kansallinen kriittinen infrastruktuuri, tietoteknillinen järjestelmä ja sen laitteet, ovat muodostaneet yhdessä organisaation kanssa kokonaisuuden, josta menetelmän alkuvaiheessa muodostettu nykytilan ymmärtäminen mahdollisti kehitys- ja muutosprosessin hahmottamisen. Kybertoimintaympäristö ja sen kehittymisen ominaispiirteet nostivat esille tutkimusprosessin aikana useita osakysymyksiä, joihin menetelmän eri vaiheissa on haettu vastuksia ja ratkaisujen dokumentoimalla ne tutkimusraporteiksi ja artikkeleiksi. Niissä korostuvat organisaatioiden kyberturvallisuuden haasteet ja mahdollisuudet. SSM on sopinut edellä kuvatulla tavalla, ontologian määritteen mukaisesti, väitöstyön tutkimusmenetelmäksi. Sen avulla tutkimustyö on edennyt loogisesti vaiheittain ja siten se on edistänyt tutkimusta tuomalla esiin sen eri vaiheissa uusia tutkimuskysymyksiä. Eteneminen on ollut myös tutkimuksen luotettavuuden näkökulmasta hyödyllistä. Tutkimuksen reliabiliteettia, eli tutkimusmenetelmän kykyä antaa toistettavia tuloksia, on pyritty edistämään taustatutkimusten haastattelumenetelmän sisällön kuvaamisella ja muun tutkimusaineiston liittämisellä väitöstyöhön. Validiteettikäsitettä eli sitä, että tutkimuksen aineiston analyysit ovat päteviä, tutkimuksen eri vaiheissa edustavat haastatteluaineistojen yhteismitallistaminen ja niiden esittäminen taulukoissa haastatteluteemoja vasten sekä tutkimusaineiston sisältöanalyysien referoiminen tutkimuskysymyksiä vastaaviin artikkeleihin.

Lisäksi, että SSM sopii tieteelliseksi tutkimusmenetelmäsi, organisaation on mahdollista muodostaa sen avulla oma kehitysprosessinsa. Väitöstyössä on esitetty CATWOE-analyysi muutosprosessin tueksi. SSM ei pidä sisällään muutosprosessin implementointia käytännön tasolla. Väitöstyössä on yhdistetty SSM-metodologia sekä organisaation PDCA-kehitysmenetelmä eli Demingin laatuympyrä. PDCA-kehitysmenetelmän avulla metodologiassa esitettyjä toimenpiteitä voidaan implementoida organisaatioissa käyttöön niiden omien resurssien ja toimenpiteiden tarpeellisuuden priorisoinnin perusteella. SSM-metodologia ja organisaatioiden PDCA-kehitysmenetelmä ovat hyvin tunnettuja menetelmiä, joten niiden yhdistämistä voi suositella väitöstutkimuksen perusteella yleiseen käyttöön, mikä kehittää metodologiaa ja mahdollistaa sen kokonaisvaltaisemman soveltamisen jatkossa tutkimustoiminnan konkretisointiin käytännön tasolla. Väitöstutkija pitää kokemukseensa perustuen organisaatiossa kehitystoimenpiteiden implementointia kehitystyön onnistumisen näkökulmasta avainkysymyksenä. Toimenpiteiden sijoittaminen organisaation jokapäiväisen operatiivisen toiminnan yhteyteen edellyttää erityisesti johdon vahvaa tukea, tavoitteiden levittämistä kaikille organisaatiotasoille, selkeitä toteuttamisvastuita, hyvää suunnittelua ja sidosryhmien informointia.

Väitöstutkimus korostaa suomalaisten kansallisten organisaatioiden kyberturvallisuutta edistäviä johtamis- ja kehittämistarpeita sekä niiden omien että koko yhteiskunnan turvallisuuden ja kilpailukyvyn näkökulmista. Tutkimuksen muut implikaatiot voidaan liittää EU-alueen kyberturvallisuuteen ja siten myös koko alueen kilpailukyvyn kehittämiseen. EU on tukemassa digitalisaatiota kilpailukykynsä parantamiseksi suunnittelemalla uutta Digitaalinen Eurooppa -rahoitusohjelman vuosiksi 2021–2027. Onkin nähtävissä, että kehittämisohjelman, jossa yhdistyy digitalisaation hyödyntäminen kilpailukykyä tukevalla tutkimuksella, uusilla ratkaisuilla ja niiden turvallisella soveltamisella käytäntöön, tulisi huomioida kyberturvallisuuden osaaminen ja yhdistäminen käytännön ratkaisuihin saumattomasti. Väitöstyö tulokset voisivat tällöin olla tukemassa kehitystä kyberturvallisuuden näkökulmasta. Lisäksi ne voisivat liittyä laajasti kyberturvallisuuden ratkaisujen edistämiseen esimerkiksi tulevissa EU:n HORISONTTI EUROOPPA 2021-2027 Pilari 2:n tutkimushankkeissa. Väitöstyössä on käsitelty EU:n Verkko- ja tietoturvadirektiiviä (NIS-direktiivi) ja sen velvoitteita jäsenvaltioille ja niiden väliseen yhteistyöhön. Implikaationa voisi olla myös kyseisen direktiivin jatkotoimien edistäminen ja direktiivin kehittäminen.

## 7.3 Väitöstutkimuksen rajoitteet

Väitöstutkimuksen rajoituksista voidaan mainita kolme pääasiallista huomiota. Ensimmäinen huomio liittyy yhteiskunnan elintärkeiden toimintojen uhkiin, jotka ovat fyysisiä, taloudellisia tai kyberturvallisuuden uhkia (Turvallisuuskomitea, 2017 b). Tyypillisiä fyysisiä uhkia ovat muun muassa luonnon katastrofit, ympäristökatastrofit, perinteinen sota ja terrorismi kineettisin asejärjestelmin (Lehto, 2019). Taloudellisia uhkia ovat muun muassa syvä kansantalouden tai

maailmantalouden lama, rahoitusmarkkinoiden toimintahäiriö tai globaalit logistiikkahäiriöt (Lehto, 2019). Yhteiskunnan turvallisuusstrategia vuodelta 2017 pitää edellä mainittuja kolmea uhka-aluetta merkittävimpinä uhkina yhteiskunnan elintärkeitä toimintoja turvattaessa. Väitöstutkimus rajautuu kyberuhkien käsittelyyn ja kriittisen infrastruktuurin organisaation toimenpiteisiin niitä vastaan.

Toinen huomio liittyy tutkimuksen tiedonhankintaan. Väitöstutkimuksessa ensimmäisessä haastatteluvaiheessa tutkimushankkeesta ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” hyödynnetyt haastatteluosiot kattoivat seitsemältä kriittisen infrastruktuurin osa-alueelta saadut yksityisten ja julkisen sektorin organisaatioiden tieto-/kyberturvallisuudesta vastaavien henkilöiden haastattelut (yhteensä 31 henkilöä). Tiedosta on muodostettu kyberturvallisuuden kokonaiskuvaa kriittisestä infrastruktuurista ja organisaation nykytila-analyysissä on hyödynnetty erityisesti energia-alan haastattelumateriaalia. Tutkimustietoja on täydennetty CyberTrust-tutkimushankeen työpajoissa sekä toisessa haastatteluvaiheessa tutkimushankeen ”Kyberturvallisuuden strateginen johtaminen Suomessa” haastattelutiedoilla. Hankkeessa haastateltiin yhteensä 40 yksityisen ja julkisen sektorin organisaatioiden johtohenkilöltä tai tieto-/kyberturvallisuudesta vastaavalta henkilöltä. Edellä kuvatulla tavalla muodostetut tutkimustiedot rajautuvat merkittävimpiin kriittisen infrastruktuurin organisaatioihin. Tutkimustiedot pienistä ja keskisuurista organisaatioista rajautuvat pois. Tutkimusvajetta on täydennetty viittaamalla muihin alan tutkimuksiin.

Kolmas huomio liittyy väitöstutkimuksen alan muita tutkimuksia käsittelevään kokonaisuuteen. Muiden tutkimusten katsauksen prosessi on muodostettu siten, että siihen valikoitunut aineisto sisältää kriteerit kriittinen infrastruktuuri, organisaatio ja kyberturvallisuus. Aineiston haku on toteutettu edellä mainittujen ehtojen mukaan viimeisimmistä kansainvälisistä kyberturvallisuuden konferenssien aineistoista. Näin muodostuneen aineiston analysoinnissa on käytetty kehikkona organisaatiota ja siihen liitettyä tutkimuksen viitekehystä sekä systeemiajattelua. Ainestoa on täydennetty suomalaisilla alan tutkimuksilla edellä mainituin ehdoin. Muuta alan tutkimustietoa sekä tietoturvallisuutta hakuehtona on käytetty tutkimustyön yhteydessä tapauskohtaisesti ja tarvittaessa täydentämään kyberturvallisuuden tutkimusaluetta.

## 7.4 Esitys jatkotutkimustarpeista

Väitöstyö ja sen tulokset pitävät sisällään tarpeita jatkotutkimuksille. Ensinnäkin, koska väitöstyö tuo esille organisaation tilannetietoisuuden merkityksen kyberturvallisuuden hallinnassa, olisi hyödyllistä tehdä jatkotutkimusta teknillisen tason tilannetietoisuuden kehittämiseksi. Tero Kokkonen on väitöstyössään ”Anomaly-Based Online Intrusion Detection System as a Senor for Cyber Security Situational Awareness System” (2016) kiinnittänyt huomiota samaan asiaan totea-

malla, että organisaation kyberturvallisuuden tilannetietoisuuden merkittävimmät haasteet liittyvät monimutkaisten teknillisten järjestelmäkokonaisuuksien haavoittuvuuksien ja toiminnan poikkeamien havainnointiin (Kokkonen, 2016). CyberTrust-tutkimushankkeen yhteydessä tehdyn selvityksen (RR4, P5) perusteella voidaan todeta organisaation ICT-varantojen reaaliaikaisen tilannekuvan aikaansaamisen ilmeinen tutkimustarve. Toinen vastaavan lainen tilannetietoisuuden haasteellinen alue liittyy teollisuusautomaatiojärjestelmien kyberturvallisuuden varmistamiseen myös reaaliaikaista tilannekuvaa hyödyntämällä. Asiaa on tukittu Jyväskylän yliopiston AaTi-hankkeessa, joka käsittelee auton automaatioväylän tietoturvaa (P3, P5). Autojen automaatioratkaisuissa käytetään laajasti CAN-automaatioväylää (Controller Area Network, CAN). Myös erilaisissa koneissa ja laitteissa sekä rakennus- ja teollisuusautomaatiossa on hyödynnetty CAN-väylärakennetta. Teollisuusautomaatiojärjestelmien tiedonsiirtoratkaisut ovat myöhemmin kehittyneet kohti pakettipohjaisia lähiverkkoratkaisuja. Väitöstutkimuksessa mainittu keksintöilmoitus pitää sisällään yhden ratkaisun CAN-väylän reaaliaikaisen tilannekuvan muodostamien osalta. Organisaation ICT-varantojen sekä teollisuusautomaatiojärjestelmien reaaliaikaisen tilannekuvan muodostamisen haasteita esitetään tutkittavaksi.

Toiseksi väitöstyö tuo esille organisaation ICT-infrastruktuurin vyöhykesuojaukseen integroituja uuden teknologian ratkaisuja, joilla pyritään parantamaan suojausta ja näkyvyyttä järjestelmätasoilla. Tähän liittyy toinen esitys jatkotutkimustarpeista, joka on väitöstyössä esitettyjen uusien teknillisten ratkaisujen toteutusmahdollisuuksia ja implementoimisia käsittävä tutkimustarve. Sen tavoitteena voidaan pitää perinteisiä suojautumisratkaisujen täydentäminen organisaation kyberrakenteen eri kerroksilla.

# SUMMARY


## Cyber security management and development as part of a critical infrastructure organization - System Thinking

The structure of the modern society is based on the cooperation of different parts of the critical infrastructure. Their mutual functional ability depends primarily on operationally reliable organizations that form systems, i.e. parts of the infrastructural whole. In cyberspace, the overall reliability of the society is constructed of the joint operation of these organizations. The developments in global digitalization bring forth new threats that increase security risks in this cyberspace.

More research is needed to ensure the safety of national critical infrastructure and its organizations. This doctoral dissertation was done in the Faculty of Information Technology in University of Jyväskylä and focuses on developing cybersecurity leadership in enterprises and other organizations in the network of national critical infrastructure. The research emphasizes controlling the continuity of their functional processes in all operational environments. The research method used was Soft Systems Methodology, SSM.

The dissertation presents different models of cybersecurity leadership and development for organizations. The focus is on proactiveness as well as creating trust, preserving reputation and managing the continuity of functional processes. These organization-specific measures advance the protection of national critical infrastructure and thus also cyber self-sufficiency, comprehensive security, security of supply and both national and organization-specific competitive advantage.

While the people, processes and technologies of an organization present its capabilities, they also contain vulnerabilities. The most central research question of the dissertation concentrates on cybersecurity leadership procedures in a national critical infrastructure organization. As a solution, a model of comprehensive system level view in cybersecurity management is presented. It consists of an organization's five-layer cyber structure and the strategic, operative and technical/tactical level approaches. These approaches include a survey of measures adding trust in the organization. An organization's architectural cybersecurity framework is constructed of these components and can be put to use in developing further steps in cybersecurity management on all levels of decision-making (strategic, operative and technical/tactical). Three practical measures for development are presented: first, embedding new technological solutions into the organization's piers cyber security structure, second, drafting comprehensive cyber security risk assessments and third, preparing contingency plans in order to improve an organization's resilience.

The need to develop an organization's situation awareness can be formulated by considering the need for it on every level of decision-making, utilizing the organization's national and international networks. Comprehensive situation awareness and related, situation-specific analytical capabilities of the organization support the functioning of critical infrastructure in its entirety.

In implementing the organizational cybersecurity development measures presented in the dissertation, the PDCA-method of process improvement can be applied. Carrying out these organization-specific measures in practice promotes the objectives of not only the national cybersecurity and competitiveness, but research results can also be applied for example in the European Union's future programs like Digital Europe etc.

# LÄHTEET


Aaltola, M., Fjäder C., Innola E., Käpylä J. & Mikkola H., 2016. Huoltovarmuus muutoksessa. Kansallisen varautumisen haasteet kansainvälisessä toimintaympäristössä. Ulkpoliittine Instituutti. FIIA REPORT 49.s. 47, 104.

Ahonen, P., 2017. Automaation kyberturvallisuuden kehitysprojektin tulokset (KYBER-TEO 2014-2016) ja tulevaisuus. ASAF-teemapäivä 10.5.2017: Turva-automaation uudet vaatimukset ja automaation tietoturva. VTT.

Airaksinen, T., 2003. Tekniikan suuret kertomukset, Filosofinen raportti, Otavan Kirjapaino Oy, Keuruu, 399 s.

Airaksinen, T., 2006. Ihmiskoneen tulevaisuus, WSOY, Helsinki, 326 s.

Alanen, J., 2000. CAN ajoneuvojen ja koneiden sisäinen paikallisväylä. VTT Automaatio, koneautomaatio. Tampere.

Arthur W. B., 2010. Teknologian luonne. Suomentanut Kimmo Pietiläinen. Hakapaino Helsinki, 229 s.

Australian Covernment, 2009. Cyber Security Strategy, Commonwealth of Australia, 2009, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf

Banathy, B., 2004. A Taste of Systemics. International Society for the Systems Sciences (ISSS), The Primer Project. www.isss.org/ taste.html.

Boyd J. R., 1995. The Essence of Winning and Losing.

Bowersox, D., Closs, D., Jessop, D. & Jones, D., 1986. Logistical Management, New York, John Wiley & Sons, Ltd., 392 s.

BusinessDictionary.com, 2019. Capability. http://www.businessdictionary.com/definition/capability.html

Carter, C., 2017. Critical Infrastructure and Cyber Security. imperva. Blogi. https://www.imperva.com/blog/critical-infrastructure-cyber-security/

Carsten, P., Yampolskiy, M., Andel, T.R. & McDonald, J.F., 2015. In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions. CISR '15 Proceedings of the 10th Annual Cyber and Information Security Research Conference (apr 2015), 477–482

Checkland, P. 1981. Systems Thinking, Systems Practice, John Wiley & Sons, Ltd., 330 s.

Checkland, P. 1985. Systems Thinking, Systems Practice. John Wiley & Sons, Pitman Press, Bath.

Checkland, P. & Scholes, J. 1990. Soft Systems Methodology in Action, John Wiley & Sons, Ltd., 329 s.

Checkland, P. & and Poulter, J., 2006. Learning for Action, London, John Wiley & Sons

Conner-Simons, A., 2016. System predicts 85 percent of cyber-attacks using input from human experts, MIT Techology Review, April 18, 2016

Csulak, E., Meadows, T., Corman, J., DeCesare, G., Fernando, A., Finn, D., Jarrett, M., Laybourn, L., McNeil, M., McWhorte, D., Mellinger, R., Monson, J., Radadoos, R., Rice, T., Sardanopoli, V., Suarez , R., Stine, K., Sublett, C., Thompson, L., Ting, D. & Trotter, F., 2017. Report on

improving cybersecurity in the health care industry. Health care industry cybersecurity task force-raportti. Saatavilla: 6.2.2019 https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

Cybersecurity and Infrastructure Security Agency, CISA, 2016. ICS Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS. https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B.

Cybersecurity and Infrastructure Security Agency, CISA, 2017. ICS Alert (ICS-ALERT-17-209-01), CAN Bus Standard Vulnerability.

Cybersecurity and Infrastructure Security Agency, CISA ICS-CERT, 2018. ICS Advisory (ICSA-10-272-01). Primary Stuxnet Advisory Original release date: September 29, 2010)

Dai, X., 2017. From model, signal to knowledge data-driven condition monitoring and attack detection in 4G Industrial Systems, SPS NATO PROJECT G5172. Northumbria University Newcastle, UK

Department of Defense (DoD) USA, 2008. Systems Engineering Guide for Systems of Systems. Versio 1, Elokuu 2008. https://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf)

Destre, E., 2017. Risks and Advantages in using Artificial Intelligence on Cyber Defence and Cyber Attack. SPS NATO PROJECT G5172. NATO Science and Technology Organization, Collaboration Support Office.

Dickerson C. & Mavris D. N., 2010. Architecture and Principles of Systems Engineering, CRC Press.

DIMECC, 2017. The Finnish Cyber Trust Program 2015-2017. Final report 7/2017. DIMECC PUBLICATIONS SERIES NO. 20.

Drivas G., Maglaras L., Janicke H. & Ioannidi S., 2019. Cybersecurity Assessment of the Public Sector in Greece. Proceedings of the 18th European Conference on Cyber Warfare and Security. ECCWS 201. s. 162-171

Dunn Cavelty, M., 2010. The Reality and Future of Cyberwar, Parliamentary Brief, 30th March 2010

Eduskunta, 2017. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta, HE 192/2017 vp

EECSP Expert Group, 2017. Cyber Security in the Energy Sector, Europe: Energy Expert Cyber Security Platform (EECSP).

EGA. e-Governance Academy, 2017. National Cyber Security Index (NCSI). https://ncsi.ega.ee/

Endsley, M. R., 1995. Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37.1: 32-64.

Energiateollisuus, 2019. Sähköntuotanto. https://energia.fi/perustietoa_energia-alasta/energiantuotanto/sahkontuotanto

ENISA, 2012. Threat Landscape, Responding to the Evolving Threat Environment, September 2012
ENISA, 2016. Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures.
ENISA, 2017. Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends.
ENISA, 2018 a. Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends.
ENISA, 2018 b. Cybersecurity – The Right Medicine for the eHealth Sector.
https://www.enisa.europa.eu/news/enisa-news/cybersecurity-2013-the-right-medicine-for-the-ehealth-sector
European Commission. CORDIS. European network of Cybersecurity centres and competence Hub for innovation and Operations. cordis.europa.eu/project/id/830943
Eurooppa-neuvosto, 2016. EU:n laajuiset kyberturvallisuussäännöt hyväksytty neuvostossa. http://www.consilium.europa.eu/fi/press/press-releases/2016/05/17/wide-cybersecurity-rule-adopted/
Euroopan unioni, 2013. Euroopan unionin kyberturvallisuusstrategia - Avoin, turvallinen ja vakaa verkkoympäristö, JOIN 1 final, 7.2.2013.
Euroopan unioni, 2016. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.
Euroopan yhteisöjen komissio, 2006. Tiedonanto elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta. Bryssel 12.12.2006 KOM(2006) 786 lopullinen.
Falco, C., 2016. Unleashing the Immune System: How to Boost Your Security Hygiene, IBM NEWS August 23, 2016.
Faber, S., 2015. Flow Analytics for Cyber Situational Awareness. SEI Blog.
https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html
Fimea, 2004. Terveydenhuollon laadunhallinta Lääkintälaitejärjestelmien turvallisuus. Lääkelaitoksen julkaisusarja 1/2004.
Fingrid Oyj., 2020. Voimajärjestelmän yleinen kuvaus. https://www.fingrid.fi/kantaverkko/sahkonsiirto/suomen-sahkojarjestelma/
FINLEX, 2014. Laki sähköisen viestinnän palveluista, 7.11.2014/917
Fjäder, C., 2014. The nation-state, national security and resilience in the age of globalisation, Resilience: International Policies, Practices and Discourses. 114-129.
Fjäder, C., 2018. Asiantuntijalausunto EDK-2018-AK-174875 HE 202/2017 vp HaV 06.03.2018.
Gao W., Morris T., Reaves B. & Richey D., 2010. On SCADA Control System Command and Response Injection and Intrusion Detection. Department of Electrical and Computer Engineering. Mississippi State University.

Grimes, S. T., 2016. Part 1 of 3: Best Practices for Medical Device Cybersecurity Management. CE-IT Collaboration Town Hall Series 23 - 24. https://docplayer.net/35473652-Part-1-of-3-best-practices-for-medical-device-cybersecurity-management.html

Halonen, P., 2016. Kyberturvallisuus terveydenhuollossa. Viestintäviraston kyberturvallisuuskeskuksen PowerPoint-esitys. https://docplayer.fi/25743256-Kyberturvallisuus-terveydenhuollossa-perttu-halonen-helsinki.html

Heitmann, B., 2017. Secure Multi-Party Computation (SMPC) on Secret Data. SPS NATO PROJECT G5172. Fraunhofer FIT, RWTH Aachen University, Germany.

Helsingin seudun kauppakamari, 2015. Yritysturvallisuus. Yrityksiin kohdistuvat kyberuhat 2015.

Helsingin seudun kauppakamari, 2016. Yritysturvallisuus. Yrityksiin kohdistuvat kyberuhat 2016.

Helsingin seudun kauppakamari, 2019. Yritysturvallisuus. Yrityksiin kohdistuvat kyberuhat 2019.

Hitt, M. A., Ireland, D. R. & Hoskisson, R. E., 1997. Strategic Management, 2th edison, St Paul, West Publishing Company, 438 s.

Hoppe, T., Kiltz, S. & Dittmann, J., 2009. "Applying Intrusion Detection to Automotive It-Early Insights and Remaining Challenges." Journal of Information Assurance and Security (JIAS) 4 (6): 226–235.

Horsmanheimo S., Kokkoniemi-Tarkkanen H., HKuusela P., Tuomimäki L., Puuska S. & Vankka J., 2017. Kriittisen infrastruktuurin tilannetietoisuus. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 19/2017.

Hundley, R. 0. & Anderson R. H., 1995. Emerging Challenge: Security - and Safety in Cyberspace, IEEE, Winter 1995/1996.

Huoltovarmuuskeskus, 2015. Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen vuonna 2014. KYBER-TEO 2014 hankkeen tuloksia.

Huoltovarmuuskeskus, 2019. KYBER-ENE Energia-alan kyberturvaaminen 1-2. Julkisten tulosten kooste. ISBN 978-952-5608-70-0 Energia-alan kyberturva (pdf).

IBM, 2019 a. Critical energy infrastructures targeted in cyber attacks. https://www.ibm.com/downloads/cas/RJG97ODA.

IBM, 2019 b. Cyber attacsks: the next healthcare epidemic. https://www.slideshare.net/ibmsecurity/cyberattacks-the-next-health-care-epidemic-84844472

Integrating the Healthcare Enterprise, 2015. IHE Patient Care Device (PCD) White Paper 10 Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide. Integrating the Healthcare Enterprisen raportti. http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf

International Standard, 2018: ISO 9004:2018. Quality management – Quality of an organization – Guidance to achieve sustained succes. https://www.sis.se/api/document/preview/80003425.

International Telecommunication Union, 1994. ITU-T Recommendation X.200

Izycki, E. & Colli, R., 2019. Protection of Critical Infrastructure in National Cyber Security. Proceedings of the 18th European Conference on Cyber Warfare and Security. ECCWS 201. s. 219-228

Jacobs, P. C., von Solms, S. H. & Grobler, M. M., 2016. Towards a framework for the development of business cybersecurity capabilities. International Conference on Business and Cyber Security (ICBCS), London, UK. The Business and Management Review, Volume 7 Number 4, 51–61.

Jacobs, P., von Solms, S. & Grobler, M. M, 2019. Towards a Framework for the Selection and Prioritisation of National Cybersecurity Functions. Proceedings of the 18th European Conference on Cyber Warfare and Security. ECCWS 201. s. 229-238

Jamshidi, M. 2008. SYSTEMS OF SYSTEMS ENGINEERING. Principles and Applications. CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742.

Johansson, K. H., Törngren, M. & Nielsen, L., 2005, Vehicle applications of controller area network, in Handbook of Networked and Embedded Control Systems, William S. Levine Dmiitris Hristu-Varsakelis, and ed., Birkhauser.

Juntunen, T., 2014. KOHTI VARAUTUMISEN JA SELVIYTYMISEN KULTTUURIA? Kriittisiä näkökulmia resilienssiin. https://www.researchgate.net/publication/283714641_Kohti_varautumisen_ja_selviytymisen_kulttuuria_-_Kriittisia_nakokulmia_resilienssiin

Juuti, P. & Luoma, M., 2009. Strateginen johtaminen. Miten vastata kompleksisen ja postmodernin ajan haasteisiin? Kustannusosakeyhtiö Otava. 296 s.

Kananen, I., 2013. Huoltovarmuuskeskus. Sähköjärjestelmä yhteiskunnan toimivuuden perustana. Käyttövarmuuspäivä 2.12.2013. http://wms.magneetto.com/webcasts/hd1/fingrid/2013_1202_kayttovarmuuspaiva_02_Kananen/Attachment/02_Kayttovarmuuspaiva_021213_Kananen.pdf

Kim, S. D., 2012. Characterizing unknown unknowns. Paper presented at PMI® Global Congress 2012—North America, Vancouver, British Columbia, Canada. Newtown Square, PA: Project.

Knowlesa, W., Princea, D., Hutchisona, D., Pagna Disso, J., F. & Jones, K., 2015. A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection. Volume 9, June 2015, Pages 52-80

Kokkonen, T., 2016. Anomaly-Based Online Intrusion Detection System as a Senor for Cyber Security Situational Awareness System. Jyväskylä studies in computing 251. University of Jyväskylä.

KPMG Finland, 2020. Teollsisuus 4.0. Kestävää kilpailuetua uusisita teknologioista. https://home.kpmg/fi/fi/home/Pinnalla/2018/02/teollisuus-4-0.html

Kuusisto, R., 2005. Tilannekuvasta täsmäjohtamiseen. Johtamisen tietovirrat kriisin hallinnan verkostossa. Liikenne- ja viestintäministeriön julkaisuja 81/2005.

Kuusisto, T., 2018. Jyväskylän yliopiston Julkisen hallinnon kyberturvallisuus KYBS7092-kurssi, 27.4.2018

Kuusisto, R. & Kuusisto, T., 2018. Cyber Security Strategy Implementation Architecture in a Value System. Springer. Cyber Security: Power and Technology pp 49-62.

Kyberturvallisuuskeskus, 2020. https://www.kyberturvallisuuskeskus.fi/

Laamanen, K. & Tinnilä, M., 2013. Prosessijohtamisen käsitteet. Teknologiateollisuus Oy. 5. uudistettu painos. 156 s.

Larson, U. E., Nilsson, D. K. & Jonsson, E., 2008. "An Approach to Specification-Based Attack Detection for in-Vehicle Networks." In 2008 IEEE Intelligent Vehicles Symposium, 220–25. doi:10.1109/IVS.2008.4621263.

Lazare, A., Controller Area Network (CAN) Communication. http://people.uwplatt.edu/~yangq/csse411/csse411-materials/s12/lazarea_CAN_communication_protocol.pptx

Lebrun, A. & Demay, J. C., 2016. Canspy: a platform for auditing can

devices. https://www.blackhat.com/docs/us-16/materials/us-16-Demay-CANSPY-A-Platorm-For-Auditing-CAN-Devices.pdf.

Lee, S. & Shon, T., 2016. Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures. 2016 Future Technologies Conference (FTC).

Lehto, M., 2008. The Finnish Defence Forces' C4ISR System from Systems Thinking Perspective, referee-artikkeli julkaistu: Proceedings of the ECIW 2008: The 7th European Conference on Information Warfare and Security, University of Plymouth, UK, 30.6–1.7.2008

Lehto, M., 2014. Kybertaistelu ilmavoimaympäristössä, Kybertaistelu 2020 (Tuija Kuusisto edit.) MPKK, Taktiikan laitos, julkaisusarja 2, n:o 1, s. 157-178.

Lehto, M., 2015. Phenomena in the Cyber World. Cyber Security: Analytics, Technology and Automation. Springer 2015, pages 3-29

Lehto, M. & Neittaanmäki P., 2016. Digitalisaatio muuttaa yhteiskunnan ja yksilöiden tapaa toimia. Tiedepolitiikka, 1/2016, 56–64

Lehto, M. & Limnéll, J., 2017. Kybersodankäynnin kehityksestä ja tulevaisuudesta, in M. Silvasti (Edith) Tiede ja Ase, s. 179-212.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M., 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, helmikuu 2017.

Lehto, M., Limnéll, J., Kokkomäki,, T., Pöyhönen, J. & Salminen, M., 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018.

Lehto M. & Neittaanmäki P. (Edit.), 2018. The modern strategies in the cyber warfare. Cyber Security: Cyber power and technology, Springer, Berlin, 2018, pages 3-20

Lehto, M. & Niemelä, J. 2019. Kyberalan tutkimus ja koulutus Suomessa 2019. Jyväskylän yliopisto. Informaatioteknologian tiedekunnan julkaisuja No. 83/2018.

Lehto, M., 2019. Kybermaailman ilmiöitä ja määrittelyjä. Kyber on kaikkialla. v 11.0. 1.9.2019.

Lemola, T., 2000. Näkökulmia teknologiaan. Gaudeamus Kirja, Helsinki, 284 s.

Lewis, T., 2015. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Second Edition

Liaropoulos, A., 2010. War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory. Proceedings of the 9th European Conference on Information Warfare and Security, the Department of Applied Informatics University of Macedonia Thessaloniki Greece, 1.-2.7.2010, pages 177 - 182.

Liao, K-H. & Huang, I-S., 2015. M a la ys iaImpact of Vision, Strategy, and Human Resource on Nonprofit Organization Service Performance. 6 th International Research Symposium in Service Management, IRSSM-6 2015, 11-15 August 2015, UiTM Sarawak, Kuching.

Libicki, M. C., 2007. Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York 2007.

Liikenne- ja viestintäministeriö, LVM, 2016. Maailman luotetuinta digitaalista liiketoimintaa Suomen tietoturvallisuusstrategia. Julkaisuja 7/2016.

Liikenne- ja viestintäministeriö, LVM, 2017. Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti, 20.4.2017.

Lillrank, P., (1998). Laatuajattelu. Laadun filosofia, tekniikka ja johtaminen tietoyhteiskunnassa. Otavan Kirjapaino Oy, Keuruu, 203 s.

Limnéll, J., Majewski, K. & Salminen, M., 2014. Kyberturvallisuus, Docendo Oy, Jyväskylä, 246 s.

Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. & Seager, T., 2013a. Measurable Resilience for Actionable Policy. Environmental Science & Technology.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen J. & Kott, A., 2013b. Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), pp. 471-476.

Mandiant Consulting, 2016. M-Trends 2016. https://content.fireeye.com/m-trends/rpt-m-trends-2016

Melkman, A. & Simmonds, K., 2016. Strategic Customer Planning: How to Develop and Implement a Strategic Account Plan. eBook Collection (EBSCOhost) - printed on 8/9/2016

National Institute of Standards and Technology (NIST). https://www.nist.gov/

National Institute of Standards and Technology, NIST, 2011. Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology . U.S. Department of Commerce.
National Institute of Standards and Technology, NIST, 2011. Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View. U.S. Department of Commerce
National Institute of Standards and Technology, NIST, 2012. Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments.
National Institute of Standards and Technology, NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018
Niiniluoto I., 2006. Tekniikan filosofia. Näkökulmia teknologiaan. Tarmo Leimola. Gaudeamus Kirja, Helsinki. 284 s.
Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Salonen, J., Savola, R., Savolainen, P., Suominen, A., Toivanen, H., Kyheröinen, J. & Remes, J., 2016. Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016.
Peltoniemi, M., Isoaho, S., Hämäläinen, T., Nurmi, P. & Nummela, E., 2004. KATSAUS SYSTEEMITEORIOIHIN – JÄRJESTELMÄAJATTELU. Materiaalivirtatutkimusryhmä. Bio- ja ympäristötekniikan laitos. Tampereen teknillinen yliopisto. [verkkojulkaisu]
Pirinen, R. & Rajamäki, J., 2015. Mechanism of critical and resilient digital services for design theory. 2015 Second International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM).
PricewaterhouseCoopersin (PwC), 2016. Industry 4.0: Building the digital enterprise. https://www.pwc.com/gx/en/industries/industrial-manufacturing/publications/assets/pwc-building-digital-enterprise.pdf
Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K., 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Independencies. IEEE Control Systems Magazine. December 2001.
Rubin, A. 2014. PEHMEÄ SYSTEEMIMETODOLOGIA (SSM). www.innokyla.fi.
Saaranen-Kauppinen, A. & Puusniekka, A., 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. http://www.fsd.uta.fi/menetelmaopetus/
Sadeghi, A. R., Wachsmann, C., & Waidner, M., 2015. Security and privacy challenges in industrial internet of things. Proceedings of the 52nd Annual Design Automation Conference. ACM.er P:
Sartonen, M., Huhtinen, A-M., & Lehto, M., 2016. Rhizomatic Target Audiences of the Cyber Domain. Journal of Information Warfare, 15(4), 1-13. 2016 ISSN 1445-3312 print/ISSN 1445-3347 online
Seeck, H., 2008. Johtamisopit Suomessa, taylorismista innovaatioihin. Gaudeamus Helsinki University Press Oy Yliopistokustasnnus, HYY htymä. 397 s.

Selkälä J., 2016. CIO decision making: Issues and a process view. JYVÄSKYLÄ STUDIES IN COMPUTING 232. ISBN 978-951-39-6548-8 (PDF). Jyväskylä University Printing House, Jyväskylä 2016.

Shein, E. H., 2009. YRITYSKULTTUURI – selviytymisopas. 2. suomenkielinen painos. Suomen Laatukeskus Oy. 220 s.

Siponen, M., Mahmood, M. A. & Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.

Siukonen T. & Neittaanmäki P., 2019. Mitä tulisi tietää tekoälystä. Docendo Oy. Jyväskylä. 344 s.

Siwicki, B., 2016. Healthcare staff lacking in basic security awareness, putting medical infrastructure at risk. HIMSS Median internetsivusto. https://www.healthcareitnews.com/news/study-healthcare-staff-lacking-basic-security-awareness-putting-medical-infrastructure-risk

Snell, E., 2016. Cybersecurity Attacks Leading 2016 Data Breach Cause. Xtelligent Healthcare Media, LLC:n internetsivusto. https://healthitsecurity.com/news/cybersecurity-attacks-leading-2016-data-breach-cause

Stouffer, K., Falco, J. & Scarfone, K., 2011. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology . U.S. Department of Commerce.

Strategy&, 2012. What is a capability? http://www.strategyand.pwc.com/global/home/what-we-think/multimedia/video/mm-video_display/what-is-a-capability

Suomalainen asiasanasto- ja ontologiapalvelu, 2019. YSO - Yleinen suomalainen ontologia. http://finto.fi/yso/fi/page/p7508

Suomen Automaatioseura ry., 2010. Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. 1. verkkopainos. Suomen Automaatioseura ry. Turvallisuusjaosto. SAS julkaisusarja nro 29.

Suomen Standardisoimisliitto SFS ry. Julkaisut ja palvelut. Standardi tutuksi. https://www.sfs.fi

Suomen Standardisoimisliitto SFS ry. Julkaisut ja palvelut. Standardi tutuksi. Standardit direktiivit ja ce-merkintä. https://www.sfs.fi

Suomen Standardisoimisliitto SFS ry., 2012. SFS-käsikirja 327. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. SFS ry, Helsinki, s. 361.

Suomen Standardisoimisliitto SFS ry., 2016. Johdanto laadunhallinnan ISO 9000 – standardeihin. slideplayer.fi/slide/11133323/

SUPO, 2017, Vuosikirja 2017. https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/75374_Supo_2017_FIN_www.pdf?57559a3bf3fad688

Taylor, A., Japkowicz, N. & Leblanc, S., 2015. "Frequency-Based anomaly detection for the automotive CAN bus," in Proc. of WCICSS, 2015, pp. 45–49.

Taylor, A., Leblanc, S. & Japkowicz, N., 2016. "Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks". IEEE DSAA (2016).

Ten, C-W., Manimaran, G., & Liu, C-C., 2010. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 40, NO. 4, JULY 2010

Terveyden ja hyvinvoinnin laitos, 2014. Terveys- ja sosiaalipalvelujen henkilöstö 2014.

Traficom, 2020. https://www.traficom.fi/fi/traficom/tietoa-traficomista/organisaatio?toggle=Kyberturvallisuuskeskus%20

Turvallisuuskomitea, 2010. Yhteiskunnan turvallisuusstrategia, YTS, Valtioneuvoston periaatepäätös 16.12.2010

Turvallisuuskomitea, 2013. Suomen kyberturvallisuusstrategia 2013. Valtioneuvoston periaatepäätös 24.1.2013.

Turvallisuuskomitea, 2017 a. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020.

Turvallisuuskomitea, 2017 b. Yhteiskunnan turvallisuusstrategia, YTS, Yhteiskunnan turvallisuusstrategia ja sen liitteet. Valtioneuvoston periaatepäätös, 2.11.2017.

Turvallisuuskomitea, 2018. Kyberturvallisuuden sanasto.

Turvallisuuskomitea, 2019. Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019.

Valtioneuvosto, 2013. Valtioneuvoston päätös huoltovarmuuden tavoitteista, 857/2013, Helsinki 5.12.2013.

Valtiontalouden tarkastusvirasto, VTV. 2017. Kybersuojauksen järjestäminen. Tuloksellisuustarkastuskertomus, Valtiontalouden tarkastusviraston tarkastuskertomukset, 16/2017. https://www.vtv.fi/files/5862/16_2017_Kybersuojauksen_jarjestaminen.pdf

Valtiovarainministeriö, 2009. 5 Kuinka välttää tartunta. Varainministeriön internetsivusto. www.vahtiohje.fi/web/guest/kuinka-valttaa-tartunta

Velev, T. & Dobrinkova, N., 2019. The Logical Model of Unified, Innovative Platform for Automation and Management of Standards (PAMS). Information & Security: An International Journal, Volume 43, Issue 1, p.113-120 (2019)

Weed, S. A., 2019. US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure. AIR UNIVERSITY. Air Force Research Institute. Perspectives on Cyber Power.

Veeramachaneni, K., Arnaldo, I., Cuesta-Infante, A., Korrapati, V., Bassias, C. & Li, K., 2016. AI2: Training a big data machine to defend, Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High

Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference, 9-10 April 2016

Viestintävirasto, Terveydenhuoltoalan kyberuhkia, 2016, https://www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf

Viestintävirasto (2018). https://www.viestintavirasto.fi/kyberturvallisuus/ncsa-fi.html

Von Solms, R. & van Niekerk, J., 2013. From information security to cyber security. Computers & Security 38: 97-102. doi: http://dx.doi.org/10.1016/j.cose.2013.04.004

Voss, W, & Comprehensible, A., 2005. Guide to Controller Area Network. Massachusetts, USA: Copperhill Media Corporation.

Willison, R. & Siponen, M., 2007. A Critical assesment if IS Security Research Between 1990-2004, Copenhagen Business Scholl, Department of Informatics, WORKING PAPER NO. 01-2007

Wolf, M., Weimerskirch, A. & Paar, C., 2004. Security in automotive bus systems. In Proceedings of the Workshop on Embedded Security in Cars 2004.

World Economic Forum, 2019. The Global Risks Report 2019.

Zhang, Y., Qiu, M., Tsai, C-W., Hassan, M. M, & Alamri, A., 2017. Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data, IEEE Systems Journal, Vol 11 , Issue 1 , March 2017, pages 88 – 95

Zaidenberg, N. J., 2017. Hardware rooted security in Industry 4.0 systems. SPS NATO PROJECT G5172.

9001 quality., 2020. The Plan Do Check Act (PDCA) cycle. Saatavana 27. Tammikuuta 2020 osoitteesta: http://9001quality.com/plan-do-check-act-pcda-iso-9001/

# LIITE 1 KÄSITTEET

**Attribuutio -** hyökkäyksellisen kyberoperaation toteuttajan tunnistaminen, paikantaminen ja tarvittaessa oikeudelliseen vastuuseen saattaminen.

**CERT-FI-ryhmä (Computer Emergency Response Team) –** Traficomin Kyberturvallisuuskeskuksessa toimivan CERT-FI:n tehtäviin kuuluu verkko-, viestintä- ja lisäarvopalveluihin kohdistuvien tietoturvaloukkausten ennaltaehkäisy, havainnointi ja ratkaiseminen, tietoturvauhkista ja -asioista tiedottaminen sekä tiedon kerääminen. (Kybertruvallisuuskesksu.fi)

**Haavoittuvuus –** alttius tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.

**Haittaohjelma** - tietokoneohjelma, joka tarkoituksellisesti aiheuttaa tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa.

**Havainnointi- ja varoitusjärjestelmä HAVARO; HAVARO** - erityisesti huoltovarmuuskriittisille organisaatioille suunnattu järjestelmä, joka havainnoi tietoturvauhkia ja varoittaa toteutuneista tietoturvaloukkauksista ja niiden yrityksistä.

**Henkilötietosuoja –** järjestelyt, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.

**HORIZON 2020** - Euroopan unionin tutkimuksen ja innovoinnin puiteohjelma. (Euroopan komissio, 2014)

**Hybridivaikuttaminen –** poliittisesti motivoitunut suunnitelmallinen toiminta, jolla pyritään saavuttamaan omat tavoitteet erilaisia, toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen. Hybridivaikuttamisen keinot voivat olla esimerkiksi taloudellisia, poliittisia tai sotilaallisia. Keinoja voidaan käyttää samanaikaisesti tai siten, että ne seuraavat toisiaan.

**Hypervisor** - tai virtuaalikonemonitori (Virtual Machine Monitor VMM) on tietokoneohjelmisto, laiteohjelmisto tai laitteisto, joka luo ja käyttää virtuaalikoneita. (https://www.ssh.com/cloud/virtualization/hypervisor)

**Häiriötilanne –** uhka tai tapahtuma, joka vaarantaa yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä ja jonka hallinta edellyttää viranomaisten ja

muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää.

**Informaatiovaikuttaminen -** toiminta, jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla muutetaan kohteen käsityksiä tai toimintaa informaatio- ja mielipideympäristön kautta.

**Informaatio-operaatio** - suunnitelmallinen sarja toimintoja, joilla tuetaan ja koordinoidaan vaikuttamista informaatioon ja informaatiojärjestelmiin määritetyn tavoitteen saavuttamiseksi

**Jatkuvuudenhallinta** – organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa.

**Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI** – valtionhallinnon elin, joka käsittelee ja sovittaa yhteen valtionhallinnon keskeiset tietoturvan ja kyberturvallisuuden linjaukset (VAHTI-ohjeet).

**Kansallinen turvallisuusauditointikriteeristö (Katakri)** – viranomaisten käyttöön tarkoitettu arviointityökalu, jonka avulla voidaan arvioida kohdeorganisaation kykyä suojata viranomaisen turvallisuusluokiteltua tietoa.

**Kiristyshaittaohjelma** – haittaohjelma, joka salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta.

**Kriittinen infrastruktuuri** – perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi.

**Kriittinen tietoinfrastruktuuri** - kriittisen infrastruktuurin yhteydessä käytetään usein englanninkielisiä ilmauksia "critical infrastructure protection" (CIP), joka tarkoittaa kriittisen infrastruktuurin suojaamista, ja "critical information infrastructure protection" (CIIP), joka tarkoittaa kriittisen tietoinfrastruktuurin suojaamista.

**Kohdistettu haittaohjelmahyökkäys; kohdistettu hyökkäys; APT-hyökkäys -** monivaiheinen tietoverkkohyökkäys, joka kohdistuu tiettyyn rajattuun kohteeseen ja joka tehdään haittaohjelmien sekä muiden toimintojen avulla.

**Koneoppiminen –** tekoälyn osa-alue, jonka tarkoituksena on saada ohjelmisto toimimaan entistä paremmin pohjatiedon ja mahdollisesti käyttäjän toiminnan perusteella. (Siukonen & Neittaanmäki, 2019)

**KRIVAT-palvelu** - häiriötilanteiden hallinnan palvelukokonaisuus, joka helpottaa yhteiskunnan kriittisten toimintojen parissa työskentelevien tahojen varautumista häiriötilanteisiin ja mahdollistaa keskinäistä viestintää ja tilannekuvan muodostamista kaikissa olosuhteissa, myös vakavissa häiriötilanteissa. (erillisverkot.fi)

**Kyberavaruus** - bittien muodostama dynaaminen ja verkottunut artefaktinen tila.

**Kyberdomain** - määritellyillä rajoilla varustettu ja jonkun hallinnassa oleva toiminta-alue.

**Kyberekosysteemi** - kybersysteemien, -toimijoiden ja -toimintaympäristön muodostama kokonaisuus.

**Kyberfyysinen järjestelmä -** Kyberfyysinen järjestelmä on järjestelmä, jossa verkon avulla yhteen liitetyt ohjelmistot kontrolloivat fyysisiä laitteita. (teknologiateollisuus.fi)

**Kyberhäiriötilanne, kyberturvallisuuden häiriötilanne, kyberhäiriö** – toteutunut kyberuhka, joka haittaa organisaation tai järjestelmän toimintaa.

**Kyberkulttuuri** - yhteisön tai koko ihmiskunnan henkisten ja aineellisten kybermaailman saavutusten kokonaisuus.

**Kybermaailma** - inhimillisen postmodernin olemassaolon oleminen maapallolla.

**Kyberpuolustus** - kyberturvallisuuden maanpuolustuksellinen osa-alue, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä

**Kybertoimintaympäristö** - ihmisten, organisaatioiden ja fyysisten systeemien muodostama vaikutusympäristö.

**Kybertoimintaympäristö; kyberympäristö** – yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö.

**Kyberturvallisuus** – tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, ky-

berturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Keskeiset tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden, määritellään Suomen kyberturvallisuusstrategiassa (Valtioneuvoston periaatepäätös 24.1.2013).

**Kyberturvallisuuden tilannekuva; kybertilannekuva -** koottu kuvaus tietojärjestelmien tietyllä hetkellä vallitsevasta käytettävyys- ja turvallisuustilanteesta sekä kybertoimintaympäristön vallitsevasta tilasta.

**Kyberturvallisuuskeskus** – Traficomin Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Se tuottaa tilannekuvaa tietoturvallisuuden ilmiöistä ja tiedottaa niistä sekä toimii tietoliikenneturvallisuusviranomaisena. (https://www.traficom.fi/fi/viestinta/kyberturvallisuus)

**Kyberuhka** – mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon.

**Kybervakoilu; tietoverkkovakoilu** - vakoilu, jossa hyödynnetään tietoverkkoja, niihin liitettyjä laitteita ja ohjelmistoja.

**Käyttöoikeuksien hallinta** – menettelyt, joilla myönnetään, evätään tai muilla tavoin käsitellään käyttöoikeuksia palveluihin ja järjestelmäresursseihin.

**Lohkoketju –** hajautettu tietokanta, joka koostuu muuttumattomista, järjestyksessä toisiinsa linkitetyistä datalohkoista ja joka on kryptografisesti suojattu. (Siukonen & Neittaanmäki, 2019)

**Normaaliolot** – yhteiskunnan pääsääntöinen tila, jossa yhteiskunnan elintärkeät toiminnot voidaan turvata ilman, että on tarpeen mahdollistaa viranomaisten tavanomaisesta poikkeava toimivaltuuksien käyttö.

**Palomuuri -** laite tai ohjelmisto, jolla rajoitetaan tietokoneelta tai sisäverkosta lähtevää tai Internetistä tietokoneelle tai sisäverkkoon tulevaa liikennettä ennalta määrättyjen sääntöjen mukaisesti. (digivinkit.fi/palomuuri)

**Palvelunestohyökkäys** – tietoverkkohyökkäys, jolla pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai tietojärjestelmä.

**Poikkeusolot** – valmiuslaissa (1552/2011) tarkoitettu yhteiskunnan tila, jossa on niin paljon tai niin vakavia häiriöitä tai uhkia, että on tarpeen mahdollistaa viranomaisten tavanomaisesta poikkeava toimivaltuuksien käyttö.

**Resilienssi –** yksilöiden ja yhteisöjen kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä.

**Riskianalyysi –** toiminta, jossa tunnistetaan riskit ja arvioidaan vahinkotapahtuman todennäköisyys sekä odotettavissa olevat vahingot.

**Riskienhallinta –** järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet.

**Tekoäly –** viittaa yksinkertaisimmillaan sellaisiin tietokoneen toimintoihin, joihin normaalisti tarvitaan ihmisälyä. (Siukonen & Neittaanmäki, 2019)

T**eollisuus 4.0 (Industry 4.0)** - termi, jota käytetään maailmanlaajuisesti kuvaamaan sitä yhä tiivistyvää kokonaisuutta, jonka esineiden internetiin (Internet of Things, IoT) pohjautuvat teknologiat, tekoäly, lisätyn todellisuuden hyödyntäminen, edistynyt analytiikka sekä edistyksellinen automaatio yhdessä muodostavat. (KPMG Finland, 2020)

**Tietoturva, tietoturvallisuus –** järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa.

**Tietoturvahäiriö; tietoturvapoikkeama –** yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti.

**Tietoturvahäiriön hallinta; tietoturvapoikkeaman hallinta –** toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi.

**Tietoturvaloukkaus –** oikeudeton puuttuminen tietoon tai tietojärjestelmään. Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.

**Tietoturvavalvomo; (security operations centre, SOC) –** organisaatio tai sen osa, jossa muodostetaan, seurataan ja analysoidaan tietoturvan tilannekuvaa, ehkäistään, tunnistetaan ja analysoidaan tietoturvahäiriöitä, dokumentoidaan niitä sekä reagoidaan niihin ohjeistuksen mukaisesti. Organisaatiolla voi olla oma tietoturvavalvomo tai valvomon palvelut voidaan ostaa ulkopuoliselta palveluntarjoajalta.

**Tietoverkkohyökkäys; verkkohyökkäys; < kyberhyökkäys** - tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön.

**Tunnistus, tunnistaminen** – menettely, jolla varmistetaan henkilön identiteetti tai esineen tai asian tunniste.

**Valmiussuunnittelu** – normaalioloissa tapahtuva varautumisen suunnittelu. Valmiuslain (1552/2011) 12 § velvoittaa viranomaiset varautumaan muun muassa valmiussuunnittelun avulla. Valmiussuunnitteluprosessissa selvitetään muun muassa häiriötilanteiden ja poikkeusolojen vaikutukset organisaation tehtäviin ja toimintaan, toiminnassa ja tehtävissä tapahtuvat muutokset, toiminnan jatkuvuuden turvaaminen ja toimenpiteet normaalioloihin palaamiseksi. Valmiussuunnittelun yksi tärkeä osa on valmiussuunnitelman teko.

**Varautuminen** – toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa. Varautumistoimenpiteitä ovat muun muassa valmiussuunnittelu, jatkuvuudenhallinta, etukäteisvalmistelut, koulutus sekä valmiusharjoitukset.

**Virushyökkäys -** haitallinen ohjelmakoodi tai ohjelman tyyppi, joka on kirjoitettu muuttamaan tietokoneen toimintatapaa, ja on suunniteltu leviämään tietokoneesta toiseen. (us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html)

**Virtualisointi -** tekniikka, joka simuloi laitteisto-ominaisuuksia ohjelmistopohjaisten IT-palveluiden, kuten sovellusten, palvelimien, tallennusvälineiden ja verkkojen, luomiseksi. (citrix.fi/glossary/what-is-virtualization.html)

**Yhteiskunnan elintärkeä toiminto** – toiminto, joka on välttämätön yhteiskunnan toimivuuden kannalta.

Lähteet, jollei ole erikseen käsitteen kohdalla tarkennettu:
Turvallisuuskomitea: Kyberturvallisuuden sanasto 2018.
Sanastokeskus TSK 50: Kokonaisturvallisuuden sanasto 2017.

# LIITE 2 STANDARDIT, OHJEET JA SUOSITUKSET OSANA ORGANISAATIOIDEN KYBERTURVALLISUUDEN HALLINTAA

Mitä standardeja, ohjeita ja suosituksia voidaan hyödyntää organisaation kyberturvallisuuden hallinnan kehittämisessä?

RR1. Pöyhönen J. (2018). Standardit, ohjeet ja suositukset osana teollisuusyrityksen kyberturvallisuuden hallintaa. Jyväskylä yliopisto, Informaatioteknologian tiedekunnan julkaisuja No. 55/2018.

Julkaisu "A survey of cyber security management in industrial control systems" (Knowlesa ym. 2015) käsittelee ICS-alueen standardeja. Ne ovat pääosin vapaasti saatavilla olevia yhdysvaltalaisia kansallisia standardeja tai suosituksia ja ovat siten helposti käytettävissä. Ohessa taulukossa on ota artikkelissa olevasata ICS-alueen standardiluettelosta. Liitteessä on kuvattu tiivistetysti luettelon standardisarjojen sisältöjä tutkimusalueeseen liittyen. Lisäksi liite pitää sisällään tiedot kansallisesta turvallisuusauditointikriteeristöstä (KATAKRI) ja valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän ohjeistosta, (VAHTI-ohjeet).

| | | |
|---|---|---|
| **Country** | **Publication** | **Paid or public** |
| International | ISO/IEC27000Series | Paid |
| United States | DoDDirective8500.1:InformationAssurance | Public |
| United States | DoD Instruction8500.2:InformationAssuranceImplementation | Public |
| United States | DoD Instruction8510.01:DIACAP | Public |
| United States | FIPS 199 | Public |
| United States | FIPS 200 | Public |
| United States | NIST 800 Series | Public |

## 1. Termistö

**Federal Information Processing Standards, FIPS PUB 199 (2004)**
**Standards for Security Categorization of Federal Information and Information Systems**

Standardi tiedon luokittelemiseksi ja suojaamiseksi siihen liittyvien attribuuttien mukaan jaoteltuna tarkoittaa seuraavaa:

- Standardia voidaan käyttää tiedon ja tietojärjestelmien luokitteluun määritettäessä niiden riskitasoja. Luokittelu on ensimmäinen askel riskienhallinnan prosessissa.
- Tieto tai tietojärjestelmä voidaan sisällyttää eri riskitasoille kunkin suojattavan attribuutin mukaan.

- Ohje sisältää tietoturvallisuuden minimivaatimukset kussakin attribuuttiluokassa.

Suojattavan tiedon kolme attribuuttia ovat:

- TIEDON LUOTETTAVUUS (CONFIDENTIALITY
- TIEDON EHEYS (INTEGRITY)
- TIEDON SAATAVUUS (AVAILABILITY)

| **TURVALLISUUSTASO** | **MATALATASO** | **KESKITASO** | **KORKEATASO** |
|---|---|---|---|
| **Luottamuksellisuus** Sisältää rajoituksia tietojen saantiin ja tietojen paljastumiseen. Mukaan lukien keinot yksityisyyden ja omistusoikeuden suojaamiseksi. | Tietojen luvattomalla paljastumisella voidaan olettaa olevan rajallisen kielteinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. | Tietojen luvattomalla paljastamisella voidaan olettaa olevan vakava haitallinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. | Tietojen luvattomalla paljastamisella voidaan olettaa olevan vakava tai katastrofaalisen haitallinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. |
| **Eheys** Informaation muuttamisen tai tuhoamisen estäminen. Informaation aitouden varmistaminen. | Tietojen luvattomalla muokkauksella tai tuhoamisella voidaan olettaa olevan rajallisen kielteinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. | Tietojen luvattomalla muokkauksella tai tuhoamisella voidaan olettaa olevan vakava haitallinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. | Tietojen luvattomalla muokkauksella tai tuhoamisella voidaan olettaa olevan vakava tai katastrofaalisen kielteinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. |
| **Saatavuus** Ajankohtaisen ja luotettavan tiedonsaannin ja käytön varmistus. | Tietojen tai tietojärjestelmän käytöllä tai käyttötietojen häiriintymisellä odotetaan olevan rajallisesti haitallisia vaikutuksia organisaation toimintaan, varallisuuteen tai yksilöihin. | Tietojen tai tietojärjestelmän käyttöoikeuksien katoamisella tai käytön estymisellä voi odottaa olevan vakava kielteinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. | Tietojen tai tietojärjestelmän käytön tai käytön katoamisella voi odottaa olevan vakava tai katastrofaalisen kielteinen vaikutus organisaation toimintaan, varallisuuteen tai yksilöihin. |

## 2. Minimivaatimukset

### Federal Information Processing Standards, FIPS 200 (2006) Minimum Security Requirements for Federal Information and Information Systems

Tämä standardi edistää tietoturvallisten tietojärjestelmien kehittämistä, käyttöönottoa ja toimintaa määrittämällä tietoturvallisuuden vähimmäisvaatimukset sekä helpottamalla johdonmukaisempaa, vertailukelpoista ja toistuvaa lähestymistapaa määritettäessä tietojärjestelmien turvatarkastusten valintaa niille asetettavissa olevia minimivaatimuksia vasten.

Standardi antaa ohjeita yhdysvaltalaisen julkisen hallinnon, sen verkosto-organisaatioiden ja yksityisen sektorin yritysten, tiedon ja tietojärjestelmien turvallisuuden minimitasojen määrittämiseksi seuraavasti:

- Standardi perustuu riskitasojen mukaan määritetyille tarkoituksenmukaisille turvallisuustasoille.
- Ohjeistaa tiedon ja tietojärjestelmän sisällyttämisen kuhunkin luokitteluryhmään.
- Antaa turvallisuusluokittelun minimivaatimukset tiedolle ja tietojärjestelmälle kussakin luokitteluryhmässä.

Tiedon turvallisuuden luokittelussa sen luotettavuus, eheys tai saatavuus vaihtelevat tietojärjestelmästä toiseen järjestelmään asetetun turvallisuusvaatimuksen mukaisesti. Tällöin uhkan matala vaikutustaso toteutuu, kun sen tiedon jokaiseen attribuuttiin kohdistuvan uhkan vaikutus arvioidaan matalaksi. Järjestelmän keskimmäinen vaikutustaso määrittyy silloin, kun vähintään yksi sen tiedon attribuuteista arvioidaan tälle tasolle eikä yksikään attribuuteista saavuta keskimmäistä tasoa korkeampaa statusta. Korkein taso määrittyy silloin, kun yksikin sen attribuuteista arvioidaan tälle tasolle.

Ohjeessa tietoturvallisuuden minimivaatimukset edellytetään seuraavilta osa-alueilta: pääsyn hallinta, tilannetietoisuus ja koulutus, tarkastustoiminta ja eri vastuut, sertifiointi, akkreditointi ja turvallisuusarvioinnit, kokoonpanonhallinta, valmiussuunnittelu, tunnistaminen ja todentaminen, tapahtumavastuut, ylläpito, laitesuojaus, fyysinen- ja ympäristösuojaus, suunnittelu, henkilöstöturvallisuus, riskiarviointi, järjestelmä- ja palveluhankinta, järjestelmä- ja laitesuojaus, tietoturva.

### Kansallinen turvallisuusauditointikriteeristö, KATAKRI (2015)

Kriteeristön tavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa organisaatiossa kohteen turvallisuustason todentavan tarkastuksen eli turvallisuusauditoinnin. Kriteeristö toimii kansallisesti velvoittavana asiakirjana silloin, kun suomalaisten yritysten turval-

lisuustaso varmennetaan kansallisen turvallisuusviranomaisen toimesta kansalliseen tarpeeseen tai kansainväliseen viranomaispyyntöön pohjautuen tai yritysturvallisuustodistuksen myöntämiseen tähdäten.

KATAKRI on siten viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Auditointityökaluna voidaan käyttää erityisesti arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä.

Mikäli suomalainen yritys tarvitsee yritysturvallisuustodistuksen esimerkiksi valtionhallinnon salassa pidettävää tietoa sisältäviin hankkeisiin liittyen tai osallistuakseen kansainväliseen tarjouskilpailuun, niin toimivaltaiset viranomaiset toteuttavat yritysten turvallisuustason tarkastamisen. Vaatimukset täyttävälle yritykselle toimivaltainen viranomainen voi myöntää tästä erillisen todistuksen (kansainvälisessä yhteydessä Facility Security Clearance, FSC). Ohjeistoa sovelletaan myös alihankintaketjuun silloin, kuin organisaatiolla siirtää sopimuksellista työtä alihankintaan.

KATAKRI:iin kirjatut vaatimukset on jaettu kolmeen osa-alueeseen, jotka ovat

- Turvallisuusjohtaminen (T) – organisaation turvallisuusjohtamisen valmiudet sekä kyvykkyys.
- Fyysinen turvallisuus (F) - salassa pidettävien tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset.
- Teknillinen tietoturvallisuus (I) - tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset.

**Kansallinen valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, VAHTI-ohjeet**

> ”Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) toimii julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä.”

VAHTI-ohjeiston avulla on tavoitteena kehittää tieto- ja kyberturvallisuutta, valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tavoite pitää sisällään tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa ja käyttöä.

Valtionhallinnon näkökulmasta katsottuna siihen liittyy kansallista ja kansainvälistä tietoturvallisuutta kehittävien yhteistyöryhmien toiminta sekä mahdollisesti valtionhallinnolle annettavien linjausten valmistelu. Suomen kyberturvallisuusstrategian mukaisesti VAHTI käsittelee ja sovittaa yhteen valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset.

## 3. Informaatioturvallisuuden hallinta

Kansainvälinen ISO/IEC 27000- standardisarja ohjeistaa organisaatioiden informaatioturvallisuuden kokonaishallinnan. Se on laadittu malliksi hallinnan kehittämiselle, toteuttamiselle, käyttämiselle, valvonnalle, katselmoinnille, katselmoinnille, ylläpitämiselle ja parantamiselle. Standardi on maksullinen, mutta siitä on vapaasti saatavana opetusmateriaali SFS:n verkkosivuilla.

ISO/IEC 27000- standardisarjan koulutusmateriaalissa on todettu informaatioturvallisuuden hallintajärjestelmän tarpeesta ja luonteesta seuraavasti: (SFS 2012 b)

1. Tietoturvallisuuden hallintajärjestelmä tukee eri kokoisia ja tyyppisiä organisaatioita silloin, kun ne:

- keräävät, käsittelevät, säilyttävät ja välittävät suuria määriä informaatiota,
- pitävät informaatiota sekä siihen liittyviä prosesseja, järjestelmiä, verkkoja ja ihmisiä tärkeinä turvattavina kohteina, joiden avulla organisaation tavoitteet saavutetaan,
- kohtaavat monia erilaisia riskejä, jotka voivat vaikuttaa turvattavien kohteiden toimintaan, ja
- muokkaavat riskejä toteuttamalla tietoturvamekanismeja.

2. Tietoturvallisuuden hallintajärjestelmää voidaan kuvata siten, että:

- se on osa yleistä hallintajärjestelmää, joka liiketoimintariskien arviointiin perustuen luodaan ja toteutetaan ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus,
- se on tarkoitettu yritysjohdon tietoturvatyön organisoimiseksi ja helpottamiseksi,
- sen tulisi kattaa kaikki tietoturvan johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat menettelyt ja toimenpiteet,
- se ei ole yksittäinen dokumentti, vaan moniosainen prosessi, jota on kehitettävä jatkuvasti,
- sen osia ovat mm. riskianalyysi, tietoturvapolitiikka, tietoturva-, jatkuvuus- ja toipumissuunnitelmat.

Tietoturvallisuuden hallintajärjestelmästandardien sarja koostuu toisiinsa liittyvistä standardeista. Tietoturvallisuuden hallintajärjestelmästandardien sarja liittyy moniin muihin ISO- ja ISO/IEC -standardeihin. Standardit luokitellaan tarkemmin johonkin seuraavista tyypeistä: (SFS 2012 a)

> ”Yleiskatsauksen ja termit sisältävät standardit (27000).”

> ”Vaatimuksia määrittelevät standardit (27001, 27006).”

”Yleisiä ohjeita antavat standardit (27002, 27003, 27004, 27005, 27007).”

”Sektorikohtaisia ohjeita antavat standardit (27011, 27799).”

## 4. Teollisuusautomaation kyberturvallisuus

### NIST Special Publication 800-82 Revision 2, (2015) Guide to Industrial Control Systems (ICS) Security

Teollisuusautomaatiojärjestelmien (Industrial Control Systems, ICS) kyberturvallisuuden ohjeistamiseksi on käytettävissä NIST-ohjeperheen julkaisu 800-82 Revision 2, joka käsittelee laajasti koko tekniikka-alueen turvallisuusratkaisuja, kuten SCADA-käytönvalvontajärjestelmät (Supervisory Control and Data Acquisition Systems), hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS) ja ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC). Se sisältää järjestelmien tyypilliset rakenteet keskinäisine riippuvuuksineen, niiden haavoittuvuudet tyypillisine uhkineen ja suositukset toimenpiteistä uhkien aiheuttamien riskien pienentämiseksi. Julkaisu linkittää myös muita NIST-perheen ohjeita alueen turvallisuuden hallitsemiseksi.

Ohjeen alkuosassa on myös selostettu eri teollisuusautomaatiojärjestelmien rakenteita ja esitetty niistä tyypillisimpiä esimerkkejä. Teollisuusautomaatiojärjestelmät on jaettu niiden ohjausjärjestelmien ja verkkorakenteen perusteella seuraaviin ryhmiin:

1. SCADA-käytönvalvontajärjestelmät (Supervisory Cotrol and Data Acquisition Systems, SCADA)
2. Hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS).
3. Ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC).

Ohje painottaa riskitarkastelun tärkeyttä läpi organisaation ns. kolmitasoisena tarkasteluna. Tasot ovat organisaatiotason tarkastelu, liiketoimintaprosessitaso ja IT-/ICS- järjestelmätasot (tietojärjestelmät). Tavoitteena tulee olla jatkuvan parantamisen periaate riskiriippuvaisissa toimenpiteissä läpi organisaatioketjun, jossa on sen ulkoisia omistajia ja sisäisiä toimijoita. Riskien arviointiprosessiin kuuluu neljä komponenttia, jota ovat rajaaminen, arvioiminen, reagointi ja valvonta. Ne ovat keskenään riippuvuussuhteessa siten, että esimerkiksi valvonta voi johtaa muutokseen riskien rajaamisessa ja sitä kautta koko prosessiketjuun.

Ohjeen mukainen toiminta pitää sisällään informaatioturvallisuuden kokemusten, ohjelmien ja toimintatapojen yhdistämisen ICS-järjestelmien tekniikoiden ja toimintaympäristön vaatimiin erityispiirteisiin. ICS-järjestelmiä käyttävien organisaatioiden tulee jatkuvasti päivittää turvallisuussuunnitelmiaan vastaamaan muutoksia teknologioissa, toimintatavoissa, toimintaa ohjaavissa standardeissa ja säädöksissä yhtä hyvin kuin muissakin turvavaatimuksissa. Onnistunut turvallisuusohjelman laadinta perustuu turvattavan liiketoiminnan huomioimiseen, organisaatiorajat ylittävien ohjelman laadintatiimien kokoamiseen,

ICS-spesifiseen politiikkaan ja toimintatapoihin, riskienhallinnan toteuttamiseen ja henkilöstön kouluttamiseen. Henkilöstön sitouttaminen ohjelman laadintaa ja toteutukseen tulee lähteä organisaation johdosta ja sen tulee ulottua koko henkilöstöön läpi organisaation.

ICS:n turvallisuusarkkitehtuuri on sidoksissa yrityksen yleiseen ICT-arkkitehtuuriin. ICS:n kyberturvallisuuteen kohdistuu kuitenkin omia erityisvaatimuksiaan. Esimerkiksi yrityksen tiedonsiirron verkkoarkkitehtuuria suunniteltaessa on suositeltavaa erottaa ICS-verkko sen yleisestä verkosta - yritysverkosta. Internet, sähköposti ja muu vastaava liikenne ovat yritysverkon liikennettä, mutta ne eivät ole sallittuja ICS-verkossa. Verkkolaitteisiin, niiden konfiguraatioihin ja ohjelmistopäivityksiin kohdistuvat ICS-järjestelmissä tiukat kontrollit. Yritysverkoissa tilanne ei saata aina olla näin. Mikäli ICS-verkkoliikenne sallittaisiin yritysverkossa, niin se olisi siepattavissa tai siihen kohdistuisivat yleiset DoS- ja ”Man-in-the-Middle” hyökkäykset. Toisin sanoen verkkojen erottamisella estetään yritysverkojen turvallisuus- ja toimintaongelmien siirtymiset ICS-verkkoihin. Erottamistekniikkoina ovat palomuurit ja DNZ-tekniikan avulla suoritettava verkon segmentointi.

Tiedonsiirtoverkon segmentointi ja erottaminen tulee perustua ICS-järjestelmien operatiivisten riskein analysointiin. Myös ison ICS-tiedonsiirtoverkon osittaminen pienempiin osaverkkoihin voi olla tarkoituksenmukaista. Tarkoituksenmukaisuus riippuu sellaisista tekijöitä, kuin hallinnan valtuutuksista, luottamustekijöistä, toiminnan kriittisyydestä ja siirrettävän liikenteen määrästä erotettuun verkkoon. Nämä tietoverkkoon kohdistettavat toimenpiteet ovat organisaation näkökulmasta katsottuna kaikista tehokkaimpia ICS:n suojaustoimenpiteitä kyberuhkia vastaan.

- Ohjeen mukaan tiedonsiirtoverkon segmentointi- ja erottamistekniikoista riippumatta toimenpiteisiin pätee seuraavat teemat:
- Jokainen järjestelmä ja verkko tulee segmentoida ja erottaa aina datalinkkitasolta sovellustasolle asti.
- Käyttöoikeudet myönnetään ainoastaan tarvittavilta osiltaan.
- Erota informaatioon ja infrastruktuuriin liittyvät turvallisuusjärjestelyt toisistaan.
- Sovella käyttöoikeuksissa ns. white-listoja; ne sopivat ICS-järjestelmiin, koska niiden sovellukset ovat vakioituja. Toimenpide helpottaa myös järjestelmien loki-analyysejä.

Ohjeen viimeisessä luvussa, joka käsittelee tietoturvamenettelyjen soveltamista ICS-järjestelmiin, on viittauksia alueen muihin standardeihin, ohjeisiin ja suosituksiin. Mm. riskienhallinnasta ohjeistuksen mukaiset vaiheet ovat kuvattuina ICS-järjestelmiin sovellettuna. Vaiheet ovat järjestelmäluokittelu, tietoturva-asetusten valinta, tietoturvavalvontatoimenpiteet, suojausasetusten arviointi, järjestelmähyväksyntä ja valvontatoimenpiteiden seuranta. Lisäksi luku käsittää laajasti eri turvatoimenpiteiden soveltamisia ICS-ympäristöön. Niihin liittyen yksi ohjeen liitteistä pitää sisällään selvitykset uhkalähteistä, haavoittuvuuksista ja tavanomaisimmista haitallisista tapahtumista.

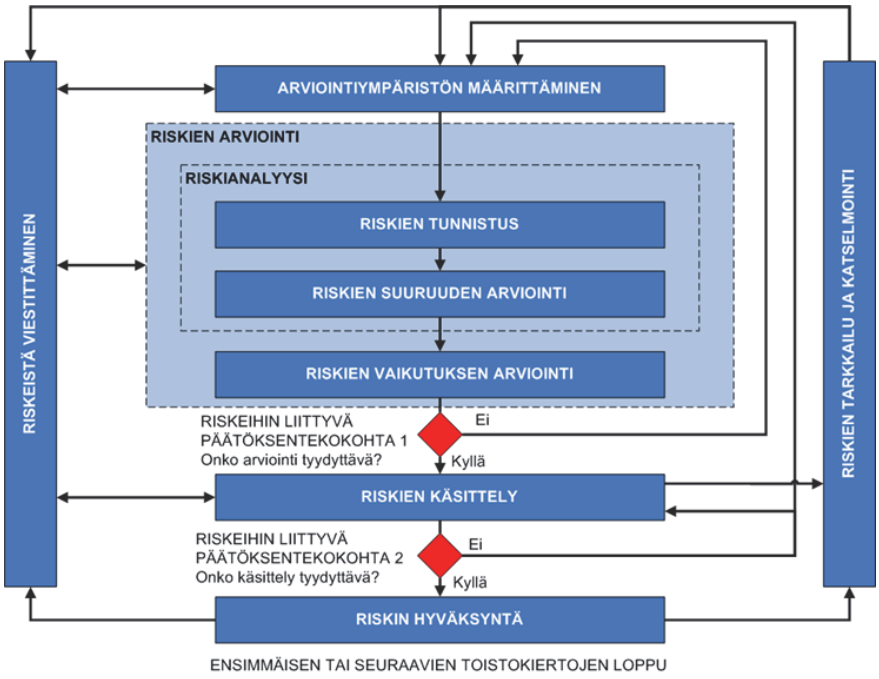
## 5. Riskien hallinta

### ISO/IEC 27005 Riskien hallinta

Tämä ohje käsittelee organisaation tietoturvallisuusriskien hallintaa. Sen ohjeisto tukee standardin ISO/IEC 27001 mukaisia tietoturvallisuuden hallintajärjestelmän vaatimuksia, mutta se ei pidä sisällään mitään tiettyä riskien hallinnan menettelytapaa. Organisaatio itse määrittelee riskien hallintaan liittyvät toimintatapansa. Toimintatavan valintaan vaikuttavat esimerkiksi hallintajärjestelmän kattavuusvaatimukset, arviointiympäristö ja toimiala. Standardin menettelyjä voidaan soveltaa kaiken tyyppisissä organisaatioissa.

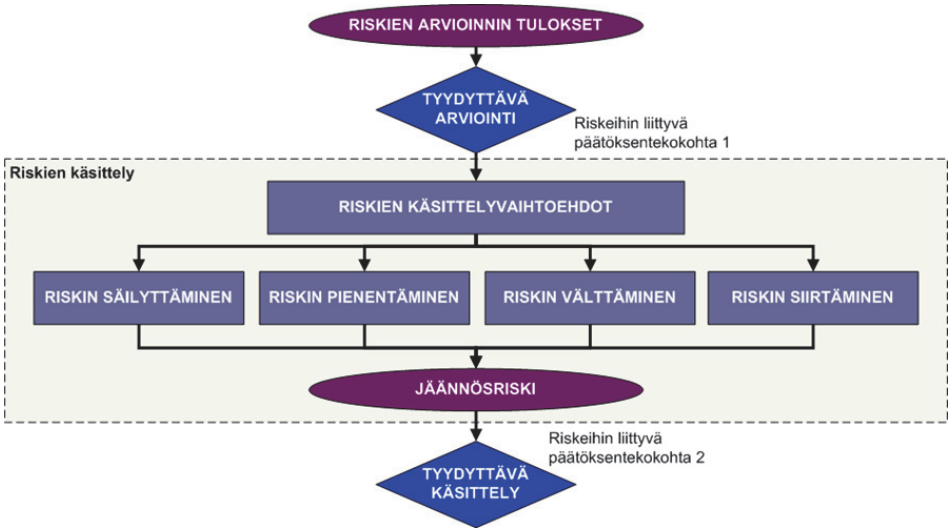
Ohjeessa ISO/IEC 27005 riskeihin liittyvät menettelyt on kiteytetty seuraaviin kuviin. Ohessa on myös ohjeen kuvaus standardin mukisesta tietoturvallisuuden hallintaprosessista, joka koostuu seuraavista vaiheista: (SFS, 2012 b)

1. ”Arviointiympäristön määrittämisestä.”
2. ”Riskien arvioinnista.”
3. ”Riskien käsittelystä.”
4. ”Riskin hyväksynnästä.”
5. ”Riskeistä viestimisestä.”
6. ”Riskien tarkkailusta ja katselmoinnista.”



Arviointiympäristön määrittämisen jälkeen tehdään riskien arviointi, jonka jälkeen voidaan siirtyä riskien käsittelyyn alla olevan kuvauksen mukaisesti. Riskien käsittelyvaihtoehdot ovat niiden säilyttäminen, pienentäminen, välttäminen ja siirtäminen.

Ohje painottaa, että riskien käsittelyn tehokkuus riippuu riskien arvioinnin tuloksista. On myös mahdollista, että esimerkiksi jäännösriskiä ei saada välttämättä heti hyväksyttävälle tasolle, jolloin sen vaatimia toimenpiteitä on edelleen tehostettava. Koko tietoturvariskien hallintaprosessin ajan on tärkeää viestiä riskeistä ja niiden käsittelystä organisaatiossa tarkoituksenmukaisella tavalla.




**Department of Defense, INSTRUCTION NUMBER 8510.01 (2017) Risk Management Framework (RMF) for DoD Information Technology (IT)**

ICS-järjestelmien elinkaaret ovat pitkiä ja niitä jatketaan yleensä kustannustehokkaasti eritasoisilla elinkaaripäivityksillä. Kyberturvallisuuden riskien hallitseminen ja turvallisuutta parantavat toimenpiteet onkin suoritettava huomioiden tarkasteltavan järjestelmän koko elinkaari. Niiden liittäminen elinkaaren alkuvaiheen järjestelmäsuunnitteluun, jatkossa tapahtuviin elinkaaripäivitysten suunnitteluun ja käytännön implementointeihin sopii ICS-järjestelmien elinkaarien eri vaiheissa suoritettaviin toimenpiteisiin kehitetyt standardit ja ohjeet. Yhdysvalloissa on puolustusvälineteollisuus ohjeistettu dokumentilla “The U.S. Department of Defense (DoD), DoD Instruction 8510.01:DIACAP” toteuttamaan järjestelmähankintojen riskiperusteista hallintaa. Yritystasolla ohjeiston toimivuuden todentaminen käytännössä on edellytyksenä järjestelmätoimittajan hyväksyn-

nälle puolustusvälinetoimittajaksi, joten sitä voidaan pitää käyttökelpoisena ohjeena myös muihin kohteisiin. Sen avulla voi muodostaa suuntaa antavan käsityksen kyberturvallisuuden suunnitteluun tarvittavista eri toimenpiteistä ja niiden vaiheista, jotka ovat seuraavat:

1. Järjestelmäluokittelu
2. Tietoturva-asetusten valinta
3. Tietoturvavalvontatoimenpiteet
4. Suojausasetusten arviointi
5. Järjestelmähyväksyntä
6. Valvontatoimenpiteiden seuranta

**NIST Special Publication 800-37 Revision 1, (2010)**
**Guide for Applying the Risk Management Framework to Federal Information Systems Security. Life Cycle Approach**

Tämän ohjeen mukaisen riskienhallinnan viitekehyksen (Risk Management Framework, RMF) soveltaminen on tarkoitettu ICT-järjestelmien elinkaarien aikaiseen riskien tarkasteluun. Viitekehyksen mukainen toiminta korostaa riskien hallintatyön merkitystä osana yrityksen johtamista ja kokonaisvaltaista riskien hallintaa. Se painottaa riskien hallinnan toimenpiteistä saatujen kokemuksen ja organisaation kaikkien kyberturvallisuuskykyjen hyödyntämistä sovellettaessa toimenpiteitä ICT-toimintaan, alueen tilannetietoisuuden ylläpitämiseen ja johdon päätöksenteon pohjaksi. Ohjeet tarkoitus on kohdistaa käytännön riskien arviointitoimenpiteet ICT-järjestelmien turvallisuusluokitteluun, ohjaustoimenpiteiden valintaa, käyttöönottoon ja valvontaan.

Ohjeen mukaan koko organisaation osallistumista riskien arviointityöhön pidetään ensiarvoisen tärkeänä, koska tällöin riskit tulee huomioitua kaikilta osiltaan ja laaja-alaisesti koko organisaation toimintakentässä. Se tarkoittaa operatiivisten ICT-järjestelmätason riskien lisäksi sitä, että mukaan tulevat myös taktisen tason ja strategisen tason riskitarkastelut. Näin toteutettuna operaatioympäristöön ja liiketoimintaympäristöön kohdistettuna riskitarkastelu kattaa niin prosessitason toteutusvastuut kuin organisaation kokonaisvastuut. Toimenpiteiden tulee olla johdonmukaisia, hyvin informoituja ja jatkuvasti ylläpidettäviä. Riskien hallinnan viitekehyksen mukaiset vaiheet ja vastuut on lueteltu ohjeessa.

Kuhunkin hallintaprosessin vaiheista on ohjeessa kuvattu sen eri osavaiheet ja niiden vaatimat toimenpiteet, ensisijaiset vastuut, toiminnan edellyttämät tukevat roolit, valtuutukset, toimenpiteen järjestelmän eri elinkaarivaiheissa ja tehtävän suorittamiseen liittyvät täydentävät ohjeet. Myös jokaiseen vaiheeseen liittyvät muut ohjeet ja tietolähteet on luetteloitu.

Ohjeen loppuosan liitteissä on mm. lueteltu ja kuvattu toimintaan liittyvät organisatoriset vastuut ja esitetty taulukkomuodossa jokaisen vaiheen tehtävät ja niihin liittyvät vastuutahot roolituksineen. Lisäksi liitteissä ovat kuvaukset turvallisuuteen liittyvistä valtuutuksista, niiden jatkuvan valvonnan toteutuksesta ja kuvaukset riskien hallintaan liittyvistä mahdollisista toimintaympäristöistä.

Vaiheessa 1 ICT-järjestelmät luokitellaan tiedon attribuuttien mukaan eli luokittelu tapahtuu tiedon luotettavuuden, eheyden ja saatavuuden mukaisesti. Oheiset attribuutit ovat ohjeen FISP 199 mukaisia. Tiedon saatavuuden varmistaminen ja siten järjestelmätason korkean käytettävyyden ylläpitäminen on merkittävin ICS-järjestelmien tapauksessa. SCADA- järjestelmään annetut suositukset ja ohjaukset liittyvät järjestelmän kulloiseenkin tehtävään, mutta esimerkiksi sähkön jakelun ja tuotannon ohjauksessa vaatimustasot ovat seuraavat: luotettavuusvaatimus on keskitasoa, eheysvaatimus on korkea ja käytettävyysvaatimus on korkea. Lisäksi ohje antaa esimerkkejä erilaisten haittavaikutusten luokittelusta asteikolla matala, keskinkertainen ja korkea sovellettuna taloudellisiin menetyksiin, ympäristövaikutuksiin, häiriön kestoon ja julkisuuskuvaan.

Vaiheessa 2 suoritetaan varmenteiden valintatoimenpiteet vaiheessa 1 suoritetun luokittelun mukaisesti. Ohje FISP 200 määrittää minimivaatimukset kahdeksalletoista turvallisuusalueelle tiedon luotettavuuden, eheyden ja satavuuden näkökulmista, kun tietoa käsitellään, varastoidaan tai välitetään ICT-järjestelmissä. Varmenteen tulee olla koko työyhteisöä käsittävä, tarkoituksenmukainen, organisaatiota ja ICT-järjestelmiä päällekkäisesti kattava lajitelma niitä. Näin varmenteet voidaan kohdistaa parhaiten vastaamaan kunkin kohteen tarpeita. Niiden ”räätälöinnillä” saavutetaan organisaation sisällä olevat erillistarpeet ja -vaatimukset. Esimerkiksi ICS-järjestelmissä varmenteiden ”räätälöinti” on suoritettava kohdassa 1 esitettyjen haittavaikutusten luokittelun mukaisesti.

Prosessin vaiheessa 3 suoritettavilla toimenpiteillä huolehditaan, että varmenteet tulevat käyttöön niin vanhoissa kuin uusissakin kohteissa. Kun varmenteita otetaan käyttöön, niin samalla on syytä tarkistaa, että niiden kattavuus on riittävä eikä turvallisuuteen jää aukkoja miltään osin.

Prosessin vaihe 4 pitää sisällään varmenteiden arviointimenettelyn, joka tarkoituksena on varmistaa niiden käyttöönotto, toiminta ja vaikuttavuus niin, että asetetut vaatimukset täyttyvät.

Prosessin vaihe 5 liittyy ICT-järjestelmään siten, että sen tuloksena on hallinnollinen päätös auktorisoida IT-järjestelmän toiminta ja hyväksyttää siihen liittyvät toiminnat, laitteet tai henkilöt valtuutuksineen ja riskeineen.

Prosessin viimeisen vaiheen (kohta 6) toimenpiteiden tarkoituksena on pitää yllä jatkuvaa ICT-järjestelmien muutosseurantaa, jotta niistä aiheutuvat vaikutukset varmenteisiin voidaan hallita tehokkaasti.

### NIST Special Publication 800-30 Revision 1, (2012) Guide for Conducting Risk Assessments

Riskien arviointi on yksi organisaation riskienhallinnan peruskomponenteista, josta on laadittu julkaisu nimeltä ”Guide for Conducting Risk Assessments” NIST-sarjaan tunnuksella 800-39. Toimenpiteitä käytetään organisaation toiminnallisten riskien tunnistamiseen, arviointiin ja priorisointiin huomioiden organisaation järjestelmät, henkilöstö, sidosryhmät ja yhteiskunnalliset velvoitteen. Arvioinnin tarkoituksena on tunnistaa ja kartoittaa päätöksentekijöille riskit seuraavasti: organisaatioille aiheutuvat merkittävät uhat, toimintaverkoston välityk-

sellä uhkaavat toimet omaan ja muihin organisaatioihin nähden, sisäiset haavoittuvuudet organisaation ulkopuolelle ja organisaatioiden keskinäisvaikutuksiin. Lisäksi toimenpiteisiin kuluu riskien toteutumisen todennäköisyyksien ja niistä aiheutuvien vahinkojen arviointi. Lopputuloksena tulee olla riskien määrittämisen kuvaus. Tyypillisesti se esitetään riskien haitta-asteena ja tapahtumatodennäköisyytenä, josta lopullinen luokittelu esitetään näiden matemaattisena tulona.

Ohjeen mukaan riskienhallinnassa toimenpiteet tulee suorittaa kolmella hierarkiatasolla:

- Taso 1, organisaation taso
- Taso 2, tehtävä / liiketoimintaprosessitaso
- Taso 3, tietojärjestelmätaso

Tasoilla 2 ja 2 organisaatiot käyttävät riskinarviointeja arvioidakseen kartoittaa sellaisia järjestelmällisiä tietoturvaan liittyviä riskejä, jotka liittyvät organisaation hallintoon ja johtamiseen, liiketoimintaprosesseihin, yritysarkkitehtuuriin tai rahoitukseen. Tasolla 3 organisaatiot käyttävät riskinarviointeja kartoittaakseen riskejä, jota kohdistuvat tehokkaammin tietoturvaluokitukseen sekä tietoturvallisuuden valvonnan valinta-, toteutus- ja arviointitoimenpiteisiin.

Tämä julkaisu keskittyy riskienhallintaan, joka pitää sisällään seuraavat vaiheet:

- miten valmistaudutaan riskinarviointeihin,
- miten suoritetaan riskinarviointeja,
- miten riskinarviointitulokset voidaan kommunikoida tärkeimpien organisaatioiden kanssa, henkilöstö mukaan lukien,
- miten riskinarviointien pitäminen ajan tasalla tapahtuu ja miten sitä mittaan.

Organisaatioiden tulee arvioida riskejään jatkuvasti huomioiden järjestelmiensä elinkaaret ja edellä mainitut hierarkiatasot. Riskien arviointi on olennainen osa kokonaisvaltaista, koko organisaation laajuista riskienhallintaprosessia, joka on määritelty NIST: n erikoisjulkaisussa 800-39; Riskienhallintaprosesseihin kuuluvat: riskien määrittäminen, riskien arviointi, riskiin vastaaminen ja seurata.
Riskienarviointimenetelmään kuuluvat tyypillisesti:

- riskienarviointiprosessi, selkeä riskimalli, jossa määritellään keskeiset käsitteet ja arvioitavat riskitekijät ja niiden suhteet,
- arviointimenetelmä, jossa määritellään ne riskitekijät, jotka voivat olettaa toteutuvan,
- miten riskitekijöiden yhdistelmät tunnistetaan / analysoidaan ja arvioidaan (julkaisu NIST 800-30 opas arvioinnin suorittamiseksi) ja
- analysointimenetelmä (esim. vaikutus tai haavoittuvuus), jossa kuvataan riskien yhdistelmiä ja eri tekijät tunnistetaan/analysoidaan ongelmatilan riittävän kattavuuden varmistamiseksi.

Ohje pitää sisällään nelivaiheisen riskien käsittelyprosessin ohjeistuksen. Vaiheet ovat: valmistautuminen, arvioinnin suorittaminen, tulosten ilmoittaminen ja ylläpitäminen. Jokainen vaihe on jaettu joukkoon tehtäviä, jotka ovat kuvattu. Kutakin tehtävää varten on käytössä täydentävät ohjeet. Riskitaulut ja esimerkinomaiset arviointiasteikot luetellaan asiakohtaisissa tehtävissä.

**NIST Special Publication 800-39, (2011)**
**Managing Information Security Risk, Organization, Mission, and Information System View**

Organisaation toiminta voi sisältää monenlaisia riskejä. Tietojärjestelmien käyttöön liittyvät turvallisuusriskit ovat vain yksi monista organisaation riskeistä, joita johtajien on syytä käsitellä osana kokonaisvastuutaan. Tehokas riskienhallinta edellyttää, että organisaatiot tunnistavat toimivansa monimutkaisissa, toisiinsa yhteydessä olevissa tietotekniikkaympäristöissä, joissa käytetään huipputeknisiä, mutta myös vanhoja tietojärjestelmiä.

Tämä julkaisu sijoittaa tietoturvan ja sen riskitarkastelun laajempaan organisaatiokehykseen, jossa yrityksen tavoitteena on pitää yllä hyvää mainettaan ja saavuttaa menestystä liiketoiminnassaan. Ohjeen tavoitteena on:

- varmistaa, että johtajat tunnustavat tietoturvariskit ja luovat asianmukaiset hallintorakenteet tällaisen riskin tunnistamiseksi ja hallitsemiseksi,
- varmistaa, että organisaation riskienhallintaprosessi toteutetaan tehokkaasti kaikkialla kolmella hierarkiatasolla; organisaatio (taso 1), liiketoimintaprosessit (taso 2) ja tietojärjestelmät (taso 3),
- edistetään organisaation ilmapiiriä, jossa tietoturvariskit otetaan huomioon koko toiminnassa, liiketoimintaprosessien suunnittelussa, yrityksen tietojärjestelmien arkkitehtuurissa ja järjestelmäkehityksessä, ja
- auttaa henkilöstöä vastaamaan tietojärjestelmien käytöstä tai toiminnasta ja ymmärtämään aiempaa paremmin mistä tietojärjestelmien turvallisuusriskit muodostuvat.

Jotta riskienhallintaprosessi voidaan integroida koko organisaatiossa, on ohjeessa kuvattu kolmiportainen lähestymistapa välttämätön. Toimenpiteet tulee kohdentua riskeihin organisaatiotasolla, operaatio-/ liiketoimintaprosessitasolla ja tietojärjestelmätasolla. Ohjeessa riskienhallintaprosessi toteutetaan saumattomasti kaikille kolmelle tasolle, jolloin toimenpiteiden yleistavoitteena on organisaation toiminnan jatkuva parantaminen organisaation tietoturvaan liittyvissä riskeissä. Tarkoituksenmukaiset toimenpiteet ja niiden viestintä kaikkien sidosryhmien kesken ovat merkittävä osa koko prosessia. Niillä on merkitys eri tahojen sitoutumisessa organisaation toimintaan ja liiketoiminnan menestyksessä.

Taso 1 (TIER 1) käsittelee riskit organisaation näkökulmasta katsottuna. Se muodostaa ensimmäisen riskienhallinnan osa-alueen, joka tarjoaa perussisällön kaikille muillekin riskienhallintatoimille. Organisaatiotasolla toteutettavat ensisijaiset riskienhallinnan toimenpiteet vaikuttavat suoraan toimenpiteisiin tasoilla 2 ja 3. Esimerkiksi tasolla 1 määritellyt tehtävät vaatimuksineen vaikuttavat ta-

solla 2 suoritettavien liiketoimintaprosessien suunnitteluun, kehittämiseen ja niiden toteuttamiseen. Taso 1 asettaa etusijan tehtäviin ja liiketoimintamalleihin, jotka puolestaan ohjaavat mm. sijoitusstrategioita ja rahoituspäätöksiä, ja siten vaikuttavat koko yrityksen tietotekniseen arkkitehtuuriin (mukaan lukien sulautettu tietojärjestelmät). Näistä seuraavat järjestelmien käyttöönotot ja operatiiviset ja tekniset turvatarkastukset tasolla 3. Muita esimerkkejä tason 1 toiminnoista, jotka vaikuttavat seuraaville tasoilla tehtäviin toimenpiteisiin, ovat mm. yhteinen tietoturvavalvonta, ohjauksen antaminen riskinhallinnassa, lupajärjestelyt eri toimijoille tietojärjestelmissä ja varautumiseen liittyvät toimenpiteet, kuten järjestelmien palauttamisjärjestyksen määrittäminen ja toteuttamiseen liiketoiminnan kriittisissä tehtävissä.

Määrittämistaso 2 (TIER 2) käsittelee riskejä liiketoimintaprosessin näkökulmasta katsottuna. Tason riskienhallintaan kuuluvat toimenpiteet, joilla:

- määritellään liiketoimintaprosessit, joita tarvitaan organisaatiossa koko toiminnan tukemiseen,
- priorisoidaan liiketoimintaprosessit strategisten tavoitteiden suhteen,
- määritellään tarvittavat tiedot menestyksekkääseen toimintaan ja määritellään tietojen kriittisyys/herkkyys sekä sisäiset ja ulkoiset tiedotusorganisaatiot,
- määritetään tietojen sisällyttäminen turvaluokitusvaatimusten mukaisesti ja luodaan tietotekninen yritysarkkitehtuuri, jossa on mukana sulautettu tietoturva-arkkitehtuuri ja joka edistää kustannustehokaita tietotekniikkaratkaisuja ja on johdonmukainen organisaation strategisten tavoitteiden ja suorituskyvyn kanssa.

Tason toimenpiteet vaikuttavat suoraan tasolla 3 toteutettaviin toimintoihin, joista esimerkkinä on yrityksen tietoturva-arkkitehtuuri, joka ohjaa tietosuojatarpeita, jotka vuorostaan vaikuttavat ja ohjaavat turvatarkastuksiin ja tietojärjestelmien osiin. Taso 2 vaikuttaa myös tietojärjestelmien suunnitteluun mukaan lukien spesifikaatiot, jotka ovat hyväksyttäviä näiden järjestelmien kehittämiseen. Taso 2: n toimet voivat myös tarjota hyödyllistä palautetta tasolle 1, mistä saattaa aiheutua riskitarkasteluun muutoksia tai, jotka vaikuttavat suoranaisesti meneillään oleviin riskienhallintatoimiin.

Taso 3 (TIER 3) käsittelee riskiä tietojärjestelmien näkökulmista tarkasteltuna ja ohjaa riskien ja riskialttiiden toimintojen liittymiset tasoille 1 ja 2. Tason riskienhallintatoimiin kuuluvat:

- tietojärjestelmien luokittelu,
- tietoturvatarkastukset tietojärjestelmittäin ja niiden toimintaympäristön suhteen huomioiden, että kyseiset järjestelmät toimivat yhdenmukaisesti organisaation tietoarkkitehtuurin kanssa ja
- tietoturvatarkastusten valinta, toteutus, arviointi, hyväksyntä, joka on jatkuvaa toimintaa osana järjestelmien elinkaariprosessin toteutusta koko organisaatiossa.

Tasolla 3 tietojärjestelmien omistajat, tietoturvatarkastajat, järjestelmä- ja turvallisuusinsinöörit tekevät riskiin perustuvia päätöksiä tarvittavien turvatoimenpiteiden toteuttamisesta ja valvonnasta. Päivittäisten toiminnan riskien perusteella laaditut päätökset mahdollistavat ja valtuuttavat luvan tehdä riskiin perustuvia päätöksiä siitä riippumatta ovatko kyseessä olevat tietojärjestelmät alun perin sallittuja toimimaan tietyissä ympäristöissä tai voivatko ne saada edelleen jatkuvan toimiluvan. Jatkuvat riskiperusteiset toimenpiteet auttavat johdon päätöksen teossa turvattaessa toimivat liiketoimintaprosessit. Lisäksi taso 3:n toiminnot tarjoavat olennaisen palautteen tasoille 1 ja 2. Esimerkkinä näistä palautteista ovat tietojärjestelmissä havaitut haavoittuvuudet, jotka ulottuvat koko organisaatioon. Nämä samat haavoittuvuudet voivat laukaista muutoksia yrityksen tietoturva-arkkitehtuuriin tai voivat edellyttää organisaation riskitoleranssin muuttamista.

Ohje palvelee monipuolisesti riskienhallinnan johtotehtäviä, organisaatioiden kokonaistehtävien suorittamisesta, tietojärjestelmien, tietotekniikkatuotteiden ja -palveluja hankkijoita sekä tietoturvallisuuden valvonta-, hallinta- ja toteutustahoja.

## 6. Turvallisuustekniikat

### NIST Special Publication 800-177, (2016)
### Trustworthy Email, 2. DRAFT

Sähköposti on organisaation viestinnässä erittäin merkittävä kanava. Samalla, kun sähköposti mahdollistaa tehokkaan viestinnän, sen avulla hyvin yleisesti yritetään huijata viestin saajia tai murtautua yrityksen tietovarantoihin ja -järjestelmiin. Tämä luonnosasteella oleva NIST-organisaation dokumentti antaa ohjeita ja suosituksia turvalliseen sähköpostitoimintaan. Toimenpiteillä voidaan pienentää riskejä huijatuksi tulemiseksi, viestien päätymiseksi jakeluun kuulumattomille ja niiden käyttöä tietojärjestelmiin kohdistuvana hyökkäysmuotona. Ohje soveltuu käytettäväksi eri kokoisissa julkisissa ja yksityisissä organisaatioissa niin omin toimin hallituissa kuin ulkoistetuissa sähköpostipaleluissa ja virtuaaliympäristössä.

Ohjeessa on kuvattu sähköpostijärjestelmään kuuluvat osat ja niistä muodostuva tyypillinen järjestelmäkokonaisuus sekä järjestelmän tiedonsiirtoprotokollat ja sanomaformaatit.

Se sisältää myös kuvaukset sähköpostipalvelujen merkittävimmistä uhkatekijöistä tiedon eheyteen, luotettavuuteen ja saatavuuteen liittyen. Uhkatekijät liittyvät erityisesti luvattomiin pääsyihin organisaation sähköpostijärjestelmään ja sen luottamuksellisiin viesteihin, huijausviesteihin ja sähköpostipalvelujen käytön estämiseen.

Ohje sisältää turvallisuussuosituksia em. uhkien osalta, joilla vähennetään luvattoman lähettäjän riskiä ja luvattomien vastaanottimien riskiä sekä estetään yrityksen ICT-infrastruktuuriin kuulumattomien laitteiden kytkeytymiset sähköpostijärjestelmään.

Ohje sisältä turvalliseen viestien lähettämiseen ja vastaanottamiseen liittyviä menettelyjä, jota on kuvattu teknillisiä yksityiskohtia myöten. Esimerkiksi liikenteen suodattaminen, salaaminen ja eri todennukset ovat laajasti kuvattuina ohjeessa. Kukin osa-alue sisältää turvallisuussuosituksia.

**NIST Special Publication 800-147, (2011), BIOS Protection Guidelines**
**NIST Special Publication 800-147B, BIOS Protection Guidelines for Servers (Draft)**

Tietokoneiden systeemitason perusohjelmisto on nimeltään Basic Input/Output System (BIOS), joka toimii laitetason prosessien käynnistäjänä ja alustajana käyttöjärjestelmälle. Se on tyypillisesti kehitetty alkuperäisen laitevalmistajan tai alihankkijan toimesta ja otettu käyttöön vasta lopullisessa tietokoneen valmistumisvaiheessa valmistajan toimesta, jolloin BIOS:n sisältämät haavoittuvuudet ovat voineet jäädä korjaamatta. Lisäksi luvaton BIOS:n modifiointi haittaohjelman avulla on merkittävä uhka tietokoneiden toiminalle, koska BIOS ohjaa tietokoneen käynnistysprosesseja ja on siten ainutlaatuinen ja ohittamaton osa tietokonearkkitehtuurissa. BIOS:iin kohdistuvien haittaohjelmahyökkäysten onnistuminen vaatii erikoisosaamista. Onnistuessaan ne ovat vaikeasti havaittavissa ja voivat täten aiheuttaa vakavaa vahinkoa tietojärjestelmissä.

Ohjeisto pitää sisällään suojaustoimenpiteitä, joilla pyritään ehkäisemään hallitsemattomien ja haitallisten BIOS-ohjelmien päätyminen tietokoneisiin. Ohjeisto käsittää turvallisen BIOS-päivitysprosessin ohjeet tahoille, jotka suunnittelevat, valitsevat tai toteuttavat järjestelmän BIOS-päivityksen ja varmistavat sen aitouden ja eheyden. Lisäksi ohje käsittelee BIOS:n suojausta ulkopuolisilta muutoksilta. Suositusten tarkoituksena on estää luvaton BIOS:n muuttaminen.

Toinen ohje (NIST-800147B) käsittelee palvelimia. Palvelinjärjestelmän arkkitehtuurin, toiminnan monimutkaisuus ja prosessoreiden määrä edellyttävät palvelimien etähallintaa, mistä johtuu, että niiden BIOS:n suojaustoimenpiteet eroavat muista tietokoneiden vastaavista toimenpiteistä. Tästä johtuen BIOS-päivitykset edellyttävät useiden eri päivitysmenetelmien hallintaa. Palvelinten BIOS:n suojaamiseen tähtäävä ohje sisältää kolme keskeistä periaatetta, joita voidaan soveltaa niin pääteasemiin kuin palvelin tason laitteisiinkin. Periaatteet liittyvät hyväksyttyyn ohjelmistopäivitykseen, tiedon eheyden suojaamiseen ja ohittamattomiin suojausmenetelmiin. Ohje sisältää palvelimien BIOS-päivitysten vaatimuksia, joiden avulla pyritään ehkäisemään BIOS-ohjelmien vahingoittuminen tai korruptoituminen.

**NIST Special Publication 800-41 (2009)**
**Guidelines on Firewalls and Firewall Policy**

Palomuurit ovat laitteita tai ohjelmia, jotka ohjaavat verkkoliikennettä erilaisia turvallisuusasetuksia hyväksi käyttäen. Ohjeella pyritään auttamaan organisaatioita ymmärtämään palomuuritekniikan ominaisuuksia ja käyttöä ohjaavaa palomuuripolitiikkaa. Se tarjoaa käytännön ohjeita palomuurisääntöjen kehittämiseen ja valintaan, palomuurien testaaminen, käyttöönotto ja hallinta.

Ohje sisältää yleiskatsauksen useisiin verkon palomuuritekniikkoihin ja suosituksia niiden toteutukseen. Näitä ovat mm. paketti- suodatus-, tilatarkastus-, proxy-yhdyskäytävä-/palvelintekniikat ja VPN-tekniikka sekä henkilökohtaiset palomuuriratkaisut.

Lisäksi ohje käsittelee palomuurien sijoittamista verkkoarkkitehtuureihin, palomuurisääntöjä ja antaa ohjeita toimintapolitiikkaan ja käytettäviin liikennetyyppeihin ja pitää sisällään suosituksia em. alueisiin.

Ohje sisältää yleiskatsauksen palomuurin suunnitteluun ja toteutukseen. Siinä luetellaan tekijöitä, jotka on otettava huomioon palomuuriratkaisuja valittaessa ja antaa suosituksia palomuurien määrittämiselle, testaamiseksi, käyttöönottoon ja hallintaan.

**NIST Special Publication 800-48 Revision 1**
**Guide to Securing Legacy IEEE 802.11 Wireless Networks**

Langattomat paikallisverkkoja (Wireless Local Area Networks, WLAN) käytetään yleensä laajentamaan langallisten verkkojen alueellista kattavuutta rajoitetulla toiminta-alueella. Tyypilliset käyttökohteet ovat rakennukset tai alueelliset toiminnalliset kokonaisuudet, joissa on mahdollista toteuttaa radioyhteyden muodostuminen. Perinteisesti käytetty WLAN-tekniikka perustuu IEEE802.11 standardiin. Tämä dokumentti kiinnittää huomion perinteisesti käytetyn tekniikan ja uudemman IEEE802.11i turvallisuusstandardin välisiin eroihin. IEE801.11 standardin mukaisesti toimivat WLAN-yhteydet ovat alttiita tiedon saatavuuden, luotettavuuden ja eheyden menetyksille. Turvallisuuden rajoittuneisuus voi johtaa luvattomiin kirjautumisiin organisaation tietojärjestelmiin ja –varantoihin, josta voi puolestaan aiheutua tietojen korruptoituminen, tietoverkon kaistalevеyden pieneneminen ja verkon toiminnan rajoittuminen tai estyminen. Ongelmat voivat heijastua laajalle myös muihin järjestelmiin verkkoihin yhteyksien kautta.

Organisaatioille, joilla on käytössään perinteisen tekniikan langattomia yhteyksiä, standardi suosittelee siirtymistä IEEE801.11i:n mukaisten ratkaisujen käyttöönottamista.

Suositukset pitävät sisällään teknillisiä termejä ja niiden kuvauksia. Keskeisimmät termit ovat Robust Security Networks (RSN) ja Robust Security Network Associations (RSNA). Kuvaukset käsittelevät termeihin liittyviä teknillisiä ominaisuuksia, kuten sanomarakenteita, sanomakättelymenettelyjä, avaimiston hallintaa sekä salauksen ja todentamisen keinoja.

Ohjeen lopussa on 57-kohtainen tarkistuslista WLAN-yhteyden elinkaaren eri vaiheissa huomioonotettavista turvallisuusseikoista. Lista on hyödyllinen myös organisaatioille, joilla on jo operatiivisessa käytössä WLAN-yhteyksiä ja joiden tavoitteena parantaa niiden turvallisuutta RSN:n periaatteiden mukaisesti.

**NIST Special Publication 800-125B**
**Secure Virtual Network Configuration for Virtual Machine (VM) Protection**

Virtualisointi on yleistymässä teollisissa sovelluksissa sen mahdollistavien hyötyjen, kuten kustannussäästöjen, järjestelmän käytettävyyden varmistamisen ja joustavuutta lisäävien vaikutusten vuoksi. Nykytietotekniikka mahdollistaa virtuaalisoinnin käytön myös teollisuuden prosessiohjausjärjestelmissä ainakin osittain. Virtuaaliympäristöistä ja niiden virtuaalikoneista (Virtual Machines, VMs) on siten muodostumassa avainresursseja useisiin eri palveluihin, joten niiden kyberturvallisuuden huomioiminen on ensiarvoisen tärkeää.

NIST 800-125B ohjaistus kuvaa virtuaaliympäristön tietoteknillisiä ratkaisuja, niiden etuja ja haittoja. Ohjeen keskeisiä termejä ovat verkon segmentointi, verkkoyhteyksien redundanssi, VM:n suojaaminen käyttäen palomuuriliikenteen valvontaa ja VM-liikenteen monitorointi. Näiltä osin dokumentti antaa suosituksia turvallisuuskäytänteiden kehittämiseen.

Verkon segmentoinnin osalta ohjeessa on käsitelty viittä eri lähestymistapaa toteutuksen aikaansaamiseksi. Ensimmäisenä on eri suojaustason vaatimien virtuaalipalvelimien erottaminen toisistaan kytkimillä ja säätämällä verkkoliikennettä palomuurisäännöillä. Tämän jälkeen ohje pitää sisällään virtuaalikytkimien ja –palomuurien teknilliset ratkaisut. Segmentointia käsittelevässä osiossa on lisäksi kuvattu VLAN (Virtual Local Area Network, VLAN) tekniikkaa ja limittelyä virtuaaliverkkoratkaisuiksi. Ohje sisältää edellä mainittuihin asioihin liittyen viisi toimintasuositusta.

Verkkoyhteyksien redundanssia voidaan parantaa rakentamalla verkkokorteista ryhmiä, joissa on vähintään kaksi fyysistä liityntää. Tällöin toinen on toiminnassa toinen varmistaa yhteyden toimivuuden häiriötilanteessa. Yhteyksien hallintaperiaatteet ja –politiikat antavat lisämahdollisuuksia ryhmien laatimiseen ja sitä kautta suojauksen parantamiseen. Tähän liittyy ohjeessa kolme suositusta.

VM:n suojaaminen käyttäen palomuuriliikenteen valvontaa perustuu liikenteen valvontaan eri segmenttien väleillä tai segmenttien sisältämiin aliverkkoihin ja VM:stä sisään ja ulos suuntautuvaan liikenteeseen. Ohje pitää sisällään sekä fyysiset palomuuriratkaisut että virtuaalipalomuuriratkaisut etuineen ja haittoineen. Tähän osioon ohjeessa liittyy neljä suositusta.

VM-liikenteen monitorointi on tarkoitettu organisaation tiedon suojaamiseen tunnistamalla vahingollinen tai haitallinen liikenne, joka suuntautuu VM:iin tai sieltä ulos aiheuttaen hälytyksen tai suojaustoimenpiteet. Tarvittaessa monitorointi voi käynnistää liikenteen tallentamisen porttipeilauksella analysointitarpeisiin. Ohje suosittelee liikenteen molempien suuntien monitoroinnin. Toteutukseen liittyy kaksi muuta teknillistä suositusta.

## 7. Muu ohjeisto

### NIST Special Publication 800-34 Rev. 1 (2010)
### Contingency Planning Guide for Federal Information Systems

Tämä tietojärjestelmien valmiussuunnittelua käsittelevä dokumentti antaa ohjeita, suosituksia ja näkökohtia tietojärjestelmän ennakoimattoman toiminnan ar-

viointiin ja siitä johtuvien toimenpiteiden suunnitteluun häiriöalttiissa kybertoimintaympäristössä. Organisaation selviytymiskykyä ennakoimattomissa häiriötilanteissa kutsutaan sen resilienssiksi. Se on nopea ja joustava kyky sopeutua ja toipua kaikista tunnetuista tai tuntemattomista muutoksista toimintaympäristössä. Suunnittelun tavoitteena on toiminta, jonka mahdollistaa keskeisten tehtävien suorittamisen häiriöiden aikana. Resilienssit organisaatiot pyrkivät sopeutumaan muutoksiin ja riskeihin, jotka voivat vaikuttaa heidän kykyynsä jatkaa toimintojaan. Ohje painottaa riskienhallinnan ja jatkuvuussuunnittelun yhteisvaikutusten tarpeellisuutta osana hätätilanteiden hallintaan valmistautumista.

Valmiussuunnitelmassa viitataan väliaikaisiin toimenpiteisiin tietojärjestelmäpalvelujen palauttamiseksi häiriötilanteista. Väliaikaisiin toimenpiteisiin voi sisältyä tietojärjestelmien ja toimintojen siirtäminen johonkin vaihtoehtoiseen sijaintipaikkaan, tietojärjestelmätoimintojen hyödyntäminen vaihtoehtoisella laitteella tai suorituskyvyn ylläpitämiseen manuaalisilla menetelmillä.

Ohjeessa käsitellään erityistä varasuunnittelua koskevia suosituksia kolmelle alustatyypille ja tarjoaa näille kaikille järjestelmille yhteiset strategiat ja tekniikat. Näitä ovat serverijärjestelmät, tietoliikennejärjestelmät ja tietokonejärjestelmät.

Ohje määrittää seitsemän vaiheisen valmiussuunnitteluprosessin, jonka avulla organisaatio voi kehittää ja ylläpitää elinkelpoista valmiussuunnitteluohjelmaa toimintaansa. Nämä seitsemän vaihetta on tarkoitettu integroitavaksi em. ICT-järjestelmien elinkaaren jokaiseen vaiheeseen. Vaiheet ovat:

1. Kehitä valmiussuunnitelmaperiaatteet. Tällöin toimintapolitiikka tarjoaa viranomaisten ohjeet ja muut ohjeet tehokkaan valmiussuunnitelman kehittämiseksi.
2. Suorita liiketoiminnan vaikutusten arviointi. Se auttaa tunnistamaan ja priorisoimaan tietoja, jotka ovat tärkeitä organisaation liiketoimintaprosessien tukemisessa. Toimenpiteet tarjoavat perustan jatkotoimenpiteille.
3. Tunnista häiriöitä ehkäisevä valvonta. Järjestelmähäiriöiden vähentämiseen tähtäävät toimenpiteet lisäävät kohdejärjestelmän toimivuutta ja siten vähentää katkoskustannuksia.
4. Luo varasuunnitelmia. Perusteelliset häiriöitä varten laaditut toipumisstrategiat varmistavat järjestelmän nopean ja tehokkaan toipumisen häiriötapahtuman jälkeen.
5. Kehitä tietojärjestelmän valmiussuunnitelma. Suunnitelmassa olisi oltava yksityiskohtaiset ohjeet ja menettelyt turvallisuuden kannalta ainutlaatuisen tiedon ja järjestelmähäiriön palauttamiseksi.
6. Varmista suunnitelman testaamalla, kouluttamalla ja harjoittelemalla. Testaus vahvistaa palautumisominaisuudet, kun taas koulutus valmistelee henkilöstöä suunnitelman aktivoimiseksi ja suunnitelman käyttämiseksi. Harjoitustoiminta parantaa suunnitelman tehokkuutta ja koko organisaation varautumista.

7. Varmista suunnitelman ylläpito. Suunnitelman tulisi olla jatkuvasti ylläpidettävä asiakirja. Sitä tulee päivittää säännöllisesti huomioiden tapahtuneet järjestelmäkehitykset ja organisaatiomuutokset.

Asiakirja on perusteellinen ja loogisesti etenevä ohje hyödynnettäväksi organisaation valmiussuunnitelman kehittämisessä. Siinä on erityisesti huomioitu organisaation tarpeiden arviointi ja sen resilienssin kehittäminen. Ohjeessa on aluksi taustoitettu valmiussuunnittelua mukaan lukien erilaisten turvallisuus- ja hätätilanteiden hallintaan liittyvien suunnitelmien vaikutus organisaation kokonaisresilienssiin, riskienhallintakehyksen (RMF) hyödyntäminen ja ohjeen FIPS199 vaikutustasojen huomioiminen. Tietojärjestelmän ennakoimattoman toiminnan suunnitteluprosessi pitää sisällään perussuunnitelmat, jotka ovat välttämättömiä tehokkaan valmiusominaisuuden kehittämiseksi. Tällä on vaikutuksia kaikkiin suunnittelujaksoihin, mukaan lukien liiketoiminnan vaikutusten arviointi, vaihtoehtoinen ratkaisujen valinta ja niiden hyödyntämisstrategiat. Suunnitelmassa käsitellään myös henkilökunnan yhteisiä tehtäviä ja vastuita. Tietojärjestelmän varasuunnitelman kehittäminen, yläpito, testaus, koulutusta ja harjoittelu ovat myös kuvattuina. Tekniset varautumissuunnitteluun liittyvät näkökohdat on käsitelty edellä lueteltuja kolmea järjestelmätyyppiä koskien. Se auttaa valmiussuunnittelijoita tunnistamaan, valitsemaan ja toteuttamaan asianmukaiset tekniset valmiudet.

**NIST Special Publication 800-150 (Draft) (2016)**
**Guide to Cyber Threat Information Sharing**

Kyberturvallisuuden ylläpitämisessä organisaatioiden välinen ja organisaation sisäinen uhkatiedon vaihto on eräs keskeisimmistä toimenpiteistä. Erityisesti yritysten keskinäinen yhteistyö esimerkiksi oman toimialansa sisällä on hyödyllinen toimintamalli kyberturvallisuuden kehittämiseksi kussakin toimintaan osallistuvassa yrityksessä ja koko toimialan sisällä. Yhteistyö mahdollistaa resurssien jakamisen sekä alueen yleisen tietotason kehittymisen kokemusten ja erilaisten kyvykkyyksien hyödyntämisen kautta. Yrityksen proaktiivinen toimintakyky kehittyy yhteistoiminnan seurauksena. Lisäksi yhteistoimintamallit kyberturvallisuuden eri toimijoiden kanssa, kuten erityisesti kansallisen CERT-organisaation kanssa, tuovat merkittäviä etuja yrityksille turvallisuustilannetietoisuuden parantamiseksi ja toimintansa hallitsemiseksi toimintaympäristönsä kyberturvallisuusriskien osalta. Yleisesti ottaen yhteistyö auttaa kehittämään turvallista, vastuullista ja tehokasta tiedonvaihtoa siihen osallistuvien tahojen kesken.

Kyseessä olevaa ohjeluonnosta voi pitää peruskonseptina ja sisältöluettelona kehitettäessä em. yhteistoimintaa. Ohje pitää sisällään tietoa kyberuhkatyypeistä ja teknologioista huomioiden tiedon jakamisen hyödyt ja haasteet. Organisaatiot voivat hyödyntää ohjetta suunnitellessaan ja toteuttaessaan yhteistoimintaa eri tahojen kanssa.

Yhteistoiminnassa käsiteltäviksi aiheiksi ja tiedonvaihtoalueiksi ohje suosittelee uhkiin liittyvistä toimijoista saatavat indikaatiot, havaitut toimintataktii-

kat, käytetyt tekniikat ja proseduurit sekä CERT-organisaation turvallisuushälytystiedot. Indikaatiot voivat muodostua epäilyttävistä IP-osoitteista ja nimipalvelimista tai web-osoitteista, jotka viittaavat haitallisiin sisältöihin. Organisaatioiden yhteistoiminta voi olla erityisen hyödyllistä vaihdettaessa kokemustietoja erilaisten työkalujen ja mekanismien käytöstä, kun on jouduttu ratkomaan kohdalle sattuneita haastavia kyberturvallisuuden uhkatilanteita.

Ohje auttaa asettamaan yhteistyölle tavoitteita, niiden priorisointia, kehittää uhkatietolähteiden hyödyntämistä, tiedonjakokäytänteitä ja yhteistyöosaamista.

Ohjeesta löytyvät seuraavat neljä aihekokonaisuutta:

1. Yleiskuvaus organisaation kyberturvallisuutta uhkaavien haitallisten tapahtumien koordinoinnista ja niihin liittyvistä tiedonvaihtotarpeista sekä organisaation haasteista käynnistäessään tiedonvaihtoon liittyviä prosesseja. Lisäksi osio pitää sisällään kuvaukset tiedonvaihdon ja haitallisten tapahtumien koordinoinnin peruskonsepteista, kuten kyberhyökkäyksen elinkaari, uhkatiedustelu, tiedon vaihdon rakenne sekä viralliset ja epäviralliset tiedonvaihdon yhteisöt.
2. Välittömien kyberturvallisuuskykyjen tarpeellisuuden tunnistaminen. Kyvykäs organisaatio kykenee tehokkaasti osallistumaan yhteistyöhön muiden organisaatioiden kanssa haitallisten tapahtumien selvittämisessä tarvittavaan koordinaatioon ja uhkatiedon jakamiseen. Lisäksi yksittäisen organisaation tulee kyetä toteuttamaan toimintansa itsearviointia, havaitsemaan puutteita toiminnassaan ja kehittämään kyberturvallisuuttaan toiminnan jatkuvan parantamisen kainoja hyväksi käyttäen.
3. Avainkykyjen tunnistaminen toteutettaessa haitallisten tapahtumien koordinointi- ja tiedonjakokykyjä. Toimenpiteet voidaan ryhmitellä seuraavasti: tiedonvaihdon suhteiden luonti, toimintaan osallistuminen ja toiminnan ylläpitäminen. Lisäksi aihekokonaisuus pitää sisällän ohjeistuksen siitä, miten varmistetaan tiedonjakoprosessin jatkuvuus ja elinkaari.
4. Viimeinen asiakokonaisuus pitää sisällään yleiset suositukset toiminnan toteutuksesta.

Ohjeen liitteessä A on kuvattu useita tyypillisiä skenaarioita, joilla voidaan parantaa organisaation kyberturvallisuutta uhkaavien haitallisten tapahtumien käsittelyä hyödyntäen erilaisia tiedonvaihtomekanismeja. Näitä skenaarioita ovat: kansallinen tiedonvaihto haittaohjelmahyökkäyksistä tiettyyn teollisuussektoriin, kampanja-analyysit, palvelunestohyökkäykset tiettyyn teollisuussektoriin, sähköpostikalastelun torjunta yhteistyöllä, palvelinongelmien ratkaisu liikekumppanien yhteistyöllä, CERT-yhteistyö ja luottokorttivarkaudet.

### NIST Special Publication 800-160 (Second Public Draft) (2016) Systems Security Engineering

Tietoteknisten järjestelmien kyberturvallisuuden luominen lähtee järjestelmäsuunnittelusta, jonka jälkeen turvallisuuteen tähtääviä toimenpiteitä tulee toteuttaa koko järjestelmän elinkaaren ajan.

Tämä järjestelmäsuunnittelun turvallisuutta käsittelevä ohje on tarkoitettu käytettäväksi yhdessä kansainvälisen ohjelmistosuunnittelua koskevan ISO/IEC/IEEE 15288 standardin kanssa. Ohjetta suositellaan käytettäväksi sellaisenaan tai sovellettuna kyberturvallisuuden suunnitteluprosessiin niin, että sen suosittelemat toimenpiteet ulottuvat kaikilta osiltaan järjestelmän koko elinkaaren kattavaan suunnitteluun.

Ohje antaa järjestelmäsuunnittelun perustiedot tavoiteltaessa mahdollisimman korkeaa toiminnan luotettavuutta tämän päivän kybertoimintaympäristössä. Luotettavuuden varmistaminen tässä yhteydessä tarkoittaa kaikkia niitä toimenpiteitä, jotka täyttävät kattavat kriittiset vaatimukset järjestelmän sisältämille komponenteille, alijärjestelmille, pääjärjestelmille, tiedonsiirtoverkoille, ohjelmistosovelluksille ja koko käyttöorganisaatiolle. Vaatimukset voivat pitää sisällään esimerkiksi turvallisuus- ja luotettavuusvaatimuksia, riippuvuussuhteita, toimintaan liittyviä vaatimuksia, sietokyky- ja selviytymiskykyvaatimuksia laajassa mitassa potentiaalisia häiriöitä ja uhkia vastaan. Luotettavuuden varmistukseen liittyvät tehokkaat toimenpiteet edellyttävät vaatimusten riittävää täyttämistä ja hyvin suunniteltuja toimenpiteitä. Järjestelmän kyberturvallisuuden suunnittelussa on tällöin kyse seuraavien toimenpiteiden yhdistelmästä: hyvä perussuunnittelu ja siihen liitetyt turvallisuusperiaatteet, konseptit ja tekniikat järjestelmän elinkaaren jokaisessa vaiheessa konseptisuunnittelusta aina käytöstä poistoon asti.

Mikään suunnitteluprosessi ei mahdollista järjestelmän ehdottoman turvallisuuden saavuttamista, vaan epävarmuutta joudutaan jokaisessa suunnittelukohteessa olevassa järjestelmässä sietämään. Järjestelmähankinnan yhteydessä onkin syytä huomioida epävarmuus, joka välttämättä jää tavoitteiden ja toteutuksen väliseksi ristiriidaksi. Turvallisuussuunnittelun tavoite tuleekin määritellä siten, että erilaiset rajoitteet ja välttämättömät suunnitteluperusteet ohjaavat turvallisuuden näkökulmasta tarkasteltuna tarkoituksen mukaisen järjestelmäkokonaisuuden aikaansaamiseen. Tällöin se on optimissaan sekä aktiivisen että passiivisen suojautumisen muodostama yhdistelmä, joka pitää sisällään järjestelmän elinkaaren kaikki vaiheet ja kaikki kyberturvallisuuden asteet (normaalitilanne, epävarmuus, vajaatoiminta ja palautuminen). Tarkoituksenmukaisuus voidaan määritellä kompromissiksi seuraavien ominaisuuksien välillä: suunniteltavan järjestelmän turvallisuuden varmistaminen, sen suorituskyisyys ja tehokkuus estää suunnittelemattomien toimintojen ja toimintarajoitteiden esiintyminen järjestelmässä. Tarkoituksenmukaisuutta ohjaa lopulta hankintaspesifikaatio, jonka kohteista ja niiden priorisoinnista vastaavat hankevastuussa olevat sidosryhmät turvallisuuteen liittyvien tavoitteiden ja vaatimusten kautta.

Aktiivinen suojautuminen pitää sisällään systeemiominaisuuden/toiminnallisuuden ja suorituskyvyn määrittelyt. Tällöin korostuvat ehdottomat vaatimukset järjestelmän käytölle, hyödyntämiselle ja vuorovaikutukselle teknologioiden/laitteiden, toimintaympäristön, ihmisten ja fyysisten systeemielementtien muodostamassa kokonaisuudessa.

Passiivinen suojautuminen puolestaan mahdollistaa sekä aktiivisen suojauksen että järjestelmän yleisen toiminnallisuuden niin toteutukseltaan kuin rakenteeltaankin. Se pitää sisällään järjestelmäarkkitehtuurin ja -suunnittelun sekä säännöt, jotka ohjaavat järjestelmän käyttöä, vuorovaikutussuhteita ja toiminnallista hyödyntämistä.

Ohjeen tarkoitus on

- luoda pohja IT-järjestelmän käyttöönotolle sisältäen periaatteet, käsitteet ja toiminnot,
- edistetään yhteistä ajattelutapaa järjestelmän turvallisuuden takaamiseksi riippumatta sen laajuudesta, koosta, monimutkaisuudesta tai järjestelmän elinkaaren vaiheesta,
- tarjota näkökulmia ja osoittaa, miten järjestelmätekniikan turvallisuusperiaatteita, konsepteja ja toimintoja voidaan tehokkaasti soveltaa järjestelmien suunnitteluprosesseihin,
- edistää järjestelmien turvallisuustekniikkaa julkaisemalla sen soveltamiseksi toimenpiteitä, tutkimustietoa ja
- antaa perusteita henkilöstön koulutukseen ja koulutusohjelmien kehittämiseen, mukaan lukien yksittäisten sertifikaattien ja muiden ammatillisten arviointiperusteiden kehittäminen.

Järjestelmien turvallisuustekniikan voidaan soveltaa jokaisen järjestelmän elinkaaren eri vaiheessa. Turvallisuussuunnittelussa järjestelmätyypit tai elinkaarivaiheet voivat olla seuraavat:

- uudet järjestelmät
- toiminnalliset muutokset järjestelmiin
- suunnitellut päivitykset toimiville järjestelmille samalla kun ylläpidetään päivittäisiä toimintoja
- suunnitellut päivitykset järjestelmiin, jotka johtavat uusiin järjestelmiin
- ketterät järjestelmät
- System-of-Systems (SOS)
- käytöstä poistuvat järjestelmät

Järjestelmäsuunnitteluprosessit puolestaan voivat olla seuraavat:

- sopimuksellinen prosessi
- organisaationallinen projektin mahdollistava prosessi
- teknillinen hallintaprosessi
- teknillinen prosessi

Ohjeessa on oman lukunaan kuvattu turvallisuustekniikan ja suojaustarpeiden näkökulmista katsottuna järjestelmien perusrakenteet, järjestelmäelementit niiden toimintaympäristössä huomioiden turvallisuuden merkitys, turvallisuusarkkitehtuuri, luotettavuus ja varmuus. Ohjeessa kuvataan myös laajasti järjestelmien turvallisuustekniset näkökohdat yleisesti määriteltyihin järjestelmien suunnitteluprosesseihin ja standardeihin sidottuina. Ohjeistuksessa on esitetty tietoturvaparannuksia, jotka lisäävät tai laajentavat tarkasteluprosessin tuloksia,

toimintoja ja tehtäviä. Parannetut suunnitteluprosessit koskevat toimenpiteitä koko järjestelmän elinkaaren ajan.

Ohje sisältää laajan liitekokonaisuuden muun sisällön käytännön soveltamisen tueksi.

**NIST Special Publication 800-115 (2008)**
**Technical Guide to Information Security Testing and Assessment**

Organisaation oman informaatioturvallisuutensa tilannekuvan muodostamisen erä ulottuvuus on käyttöön soveltuvien testaus ja arviointimenetelmien hyödyntäminen. Se on useiden eri prosessien kokonaisuus, joiden avulla pyritään määrittämään organisaation resurssien (järjestelmät, verkot, toimintaproseduurit, henkilöstö) kyky täyttää niille asetetut turvallisuustavoitteet. Prosessit koostuvat tyypillisesti kolmesta eri menetelmästä, jotka ovat testaaminen, tutkiminen ja haastattelu. Testaaminen on kohteiden toiminnan spesifikaatioiden täyttymisen todentamista. Tutkiminen koostuu kohteen havainnoinnista, tarkastuksista, katselmoinneista tai analysoinneista. Toimenpiteillä pyritään ymmärtämään tai selkeyttämään kohteen toimintaa tai saaman todisteita jostakin sen toiminnasta. Haastattelu puolestaan voi kohdistua yksittäisiin henkilöihin tai toiminallisiin ryhmiin. Haastatteluihin liittyvien keskustelujen avulla pyritään muodostamaan käsitys turvallisuustilanteesta, selkeyttämään sitä ja paikallistamaan kehitystarpeita. Jokainen prosessikokonaisuus palvelee organisaation mahdollisuuksia toteuttaa tehokasta ja tarkoituksenmukaista turvallisuusvarmistusta.

Informaatioturvallisuuden arvioinnin perusteena olevien testaus- ja tutkimusmenetelmien onnistumiseksi ohje suosittaa organisaatiolle seuraavia toimenpiteitä:

- informaatioturvallisuuden arviointipolitiikan luominen
- toistettavan ja dokumentoitavan arviointimenetelmän käyttöönotto
- arviointitapahtuman kohteiden määrittäminen
- tulosten analysointi, heikkouksien osoittamien riskien pienentäminen

Ohje pitää sisällään seuraavat kolme arvioinnin pääperiaatetta ja niihin liittyviä testaus- ja tarkastustekniikoita. Pääperiaatteet ovat:

- katselmointi ja siihen liittyvät tekniikat
  - järjestelmien, sovellusten, verkkojen, toimintapolitiikkojen ja –menetelmien arvioiti
- kohteen identifiointi ja analysointi ja niihin liittyvät tekniikat
  - järjestelmien, porttien ja palvelujen haavoittuvuuksien testaaminen
- kohteen haavoittuvuuden validointi ja siihen liittyvät tekniikat
  - haavoittuvuuksien paikallistaminen

Ohje pitää sisällään myös seuraavat käytännön ohjeet onnistuneen informaatioturvallisuuden arvioinnin suorittamiseksi:

- Toteutuksen suunnittelun osa-alueet, kuten arviointipolitiikka, toimenpiteiden priorisointi, aikataulutus, valinta ja looginen käsittely. Lisäksi se

pitää sisällään hahmotelman arviointiin liittyvistä oikeudellista näkökohdista, jotka organisaation tulee tarvittaessa huomioida.
- Toteutukseen liittyvät seikat, kuten toimenpiteiden koordinointi, itse toimenpiteiden suorittaminen organisaatioympäristössä, tulosten analysointi ja erilaiset datan käsittelyyn liittyvät huomiot.
- Toteutuksen jälkeiset toimenpiteet, kuten havaittuja ongelmia lieventävät suositukset ja tulosten raportointi.

Liitteissä ovat esimerkit testaus- ja tutkimusmenetelmistä, jotka auttavat organisaatioita sovellusohjelmistojen ja etäkäyttöjen haavoittuvuuksien selvittämisissä.

Sovellusohjelmistojen testaustoimenpiteet ovat tehokkainta suorittaa heti tuotteen ohjelmiston kehitysvaiheessa. Niihin kohdistuvista hyökkäysvektoreista ovat esimerkkeinä mm. eri muotoiset tietovarkaudet, luvattomat hallintamenettelyt ja palvelunestohyökkäykset. Sovellusohjelmistojen turvatestaamiseen voidaan käyttää useita menetelmiä, joista esimerkkeinä ohjeessa ovat white ja black box testit, niiden yhdistelmä gray box testi ja testeihin liittyvät yleiset ominaisuudet.

Etäkäytön toimivuuden testimetodit liittyvät haavoittuvuuksiin, jotka esiintyvät päätepalvelimissa, VPN-tekniikassa, SSH-tunneloinnissa, erillistietokoneissa ja modemeissa. Etäkäytön testaaminen voidaan suoritta osana tunkeutumien eston testausta, mutta erikseen toteutettuna testi voidaan keskittää osatestausta paremmin etäkäyttötoteutuksiin. Yleisesti käytetyt testaustekniikat ovat: luvattomien etäpalvelujen tunnistaminen porttiskannauksella, sääntöjen katselmointi luvattomien etäyhteyksien estämiseksi (konfiguraation katselmointi), etäyhteyksien pääsyoikeuksien testaaminen salasanatestauksella ja etäyhteyksien kommunikoinnin monitorointi verkkohaistelulla.

Lisäksi liitteenä on työkalusuosituksia katselmointiin, kohteen identifiointiin ja analysointiin sekä kohteen haavoittuvuuden validointiin.

**Lähteet:**

Gilsinn J. (2008). Establishing an Industrial Automation and Control Systems Security Program – An Overview of ISA-99.02.01 ISA EXPO 2008. [verkkodokumentti]. ____ http://www.controlglobal.com/assets/Media/0811/Gilsinn_ISA-99.02.01.pdf

Huoltovarmuuskeskus. (2015). KYBERTURVALLISUUDEN KEHITTÄMINEN JA JALKAUTTAMINEN TEOLLISUUTEEN VUONNA 2014. KYBER-TEO 2014 -hankkeen tuloksia. [verkkodokumentti].

International Organization for Standardization. https://www.iso.org/home.html

Knowlesa, W., Princea, D., Hutchisona, D., Ferdinand, J., Dissob, Jones, K. (2015). International journal of critical infrastructure protection 9. A, survey of cyber security management in industrial control systems.

National Institute of Standards and Technology (NIST), U.S. Department of Commerce

- NIST Special Publication 800-30 Revision 1, (2012), Guide for Conducting Risk Assessments
- NIST Special Publication 800-39, (2011), Managing Information Security Risk, Organization, Mission, and Information System View
- NIST Special Publication 800-37 Revision 1, (2010), Guide for Applying the Risk Management Framework to Federal Information Systems Security Life Cycle Approach
- NIST Special Publication 800-41 (2009), Guidelines on Firewalls and Firewall Policy
- NIST Special Publication 800-48 Revision 1 (2008), Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST Special Publication 800-82 Revision 2, (2015), Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-115 (2008), Technical Guide to Information Security Testing and Assessment
- NIST Special Publication 800-147, (2011), BIOS Protection Guidelines
- NIST Special Publication 800-147B, (2014), BIOS Protection Guidelines for Servers (Draft)
- NIST Special Publication 800-160 (Second Public Draft) (2016), Systems Security Engineering
- NIST Special Publication 800-177, (2016), Trustworthy Email, 2. DRAFT

Puolustusministeriö, KATAKRI 2015, http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Suomen Standardisoimisliitto SFS ry. http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi

Suomen Standardisoimisliitto SFS ry. (2012 a). SFS-käsikirja 327. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. SFS ry, Helsinki, 361 s.

Suomen Standardisoimisliitto SFS ry. (2012 b). Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 -standardiperhe Kalvosarja oppilaitoksille https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta

Suomen Standardisoimisliitto SFS ry. (2013). SFS Käsikirja 631-3: Automaatio. Osa 3: Tietoturvallisuus.

USA Department of Defense INSTRUCTION NUMBER 8510.01 (2017). http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf?ver=2017-07-28-134447-703

USA, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems (2004)
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems (2006)

Valtionvarainministeriö, VAHTI-ohjeet: https://www.vahtiohje.fi/web/guest/home

# ALKUPERÄISET TUTKIMUSARTIKKELIT

**Artikkeli P1:**



# Cyber security creation as part of the management of an energy company

2017
Jouni Pöyhönen, University of Jyväskylä, Jyväskylä Finland,
Martti Lehto, University of Jyväskylä, Jyväskylä, Finland

Originally published in the proceedings of the 16th European Conference on Cyber Warfare and Security ECCWS2017, 29-30th June 2017, University College Dublin, Dublin, Ireland, pages 332-340

# Cyber security creation as part of the management of an energy company

Jouni Pöyhönen, Martti Lehto
University of Jyväskylä, Finland
jouni.a.poyhonen@jyu.fi
martti.lehto@jyu.fi

**Abstract**

The functioning of a modern society is based on the cooperation of several critical infrastructures, whose joint efficiency depends increasingly on a reliable national electric power system. Crucial in the cyber environment are functional data transmission networks and the usability, reliability and integrity of system data in the operating environment, whose cyber security risks are continuously augmented by threatening scenarios of the digital world. A modern society depends entirely on a cyber environment that provides dynamic services. Trust in the operation of organizations and its continuous maintenance with effective measures are central factors affecting cyber security. Security is based on trust. It is also good to be conscious of the fact that perfect safety is in general hardly achievable, and this also applies to the cyber world, which is a dynamic environment difficult to anticipate. Therefore, it is particularly important to understand the great significance of trust in the cyber world and its security. The role of proactive measures enhancing trust is emphasized. When we build operations in the cyber world on a foundation that is as sustainable as possible, we can utilize the diverse opportunities it offers. This paper focuses on the cyber trust issues and the procedures applied to cyber security management in the processes of critical infrastructure energy companies, whereby research experiences from the latest Finnish cyber security situation research programme have been utilized. The focus is on electricity companies. The major contribution of this paper is the review of an individual energy company's cyber security management and of the actions that are needed in the structure of its business processes to gain trust. Based on the results of the research, the company needs a programme to develop its measures on all decision-making levels – strategy, operations and tactics – as well as in the area of technology and capability solutions in the cyber environment. A SWOT analysis is a useful tool for determining the current cyber situation awareness in a company's cyber security and for specifying all features that are important in the procedures of its security management. To implement the measures that are needed for the creation of cyber trust, the energy company's top leaders should consider confidence-building measures relating to cyber security as part of the company's strategic goals. Furthermore, they should maintain high performance processes and communicate their strategy to the implementation of the affirmative action policy.

Keywords: critical infrastructure, Electricity Company, cyber security management, trust, SWOT analysis

## 1. Introduction

The functioning of a modern society is based on the cooperation of several critical infrastructures, whose joint functioning depends on the reliability of the national electric power system. In addition, reliability consists of functional data transmission networks between organizations and the usability, reliability and integrity of service-level system data in the cyber environment, the security risks of which are continuously heightened by the threatening scenarios of the digital world.

In the cyber environment, the availability of electric energy provides a basis for the entity consisting of data transmission networks and related services. That is why this paper focuses on the results related to electricity companies in the latest research programme on Finland's cyber security for the energy sector.

Finland's electric power system – comprising power plants, a nationwide transmission grid, regional networks, distribution networks and electricity consumers – is part of an inter-Nordic power system together with the systems of Sweden, Norway and Eastern Denmark. In addition, there are direct current transmission links to Finland from Russia and Estonia in order to connect the Nordic system to the power systems of Russia and the Baltic countries. (Fingrid, 2016)

Electricity is produced at Finnish power plants in various ways, using several energy sources and production methods. The major sources of energy include nuclear power, water-power, coal, natural gas, wood fuels and peat. In addition to the sources of energy, production can be classified according to the production method. In Finland there are about 120 enterprises that produce electricity as well as around 400 power plants, over half of them hydroelectric power plants. Nearly a third of electricity is produced in connection with heat production. Compared with many other European countries, Finland's electricity production is decentralized. A diverse and decentralized electricity production structure increases the security of the national energy supply. (Finnish Energy, 2015)

The national significance of an electric power system is very similar irrespective of the country. For example, in the USA the power system is considered to be a critical infrastructure and a key resource for the functioning of the entire society. The basic structures of the power system are similar to those in Finland. In the USA, it can be seen that the grid represents a technologically highly advanced system entity and that its solutions call for the use of the most demanding technologies. Grid technology and its control procedures constitute the principal areas in examining cyber security. (Lewis, 2015)

In autumn 2016, the Finnish Prime Minister's Office implemented a research project focusing on the current state of Finland's cyber security. The aim was to compare the current state with the targets of the national Cyber Security Strategy and to map further actions needed to achieve the targets. One of the work packages in the research project focused on the private sector. The work package aimed at analysing the situation of national cyber security performance in the private sector and at providing information on how the goals of the Cyber Security Strategy have been achieved. The organizations chosen for the study were critical infrastructure companies from seven branches, including energy supply. This paper focuses on the research results of the work package obtained through a SWOT analysis. The research method was applied in order to identify the company specific data and factors affecting national cyber security that are relevant for answering the research questions.

In addition to an introductory section, the paper includes an overview of a typical cyber environment in an electricity company. It also describes the principles and interview themes of a SWOT analysis, which was chosen as the qualitative research method, and provides the research results with conclusions as well as a final summary with development proposals.

## 2. An electricity company's typical cyber environment

The general networks and working processes involved in the operation of an electricity company can be illustrated with a logistics framework that comprises a supplier network, a production process, a client network, and information and material flows that connect them. Information technology (IT) systems are part of a company's infrastructure and thus constitute a significant part of the operations that support a company's core processes. Corporate-level IT systems are related to administration and to the management of information and material flows in the network. The production level includes industrial automation systems (industrial control systems, ICS). Figure 1 presents the structure of a company's logistics framework and common IT and industrial automation systems.

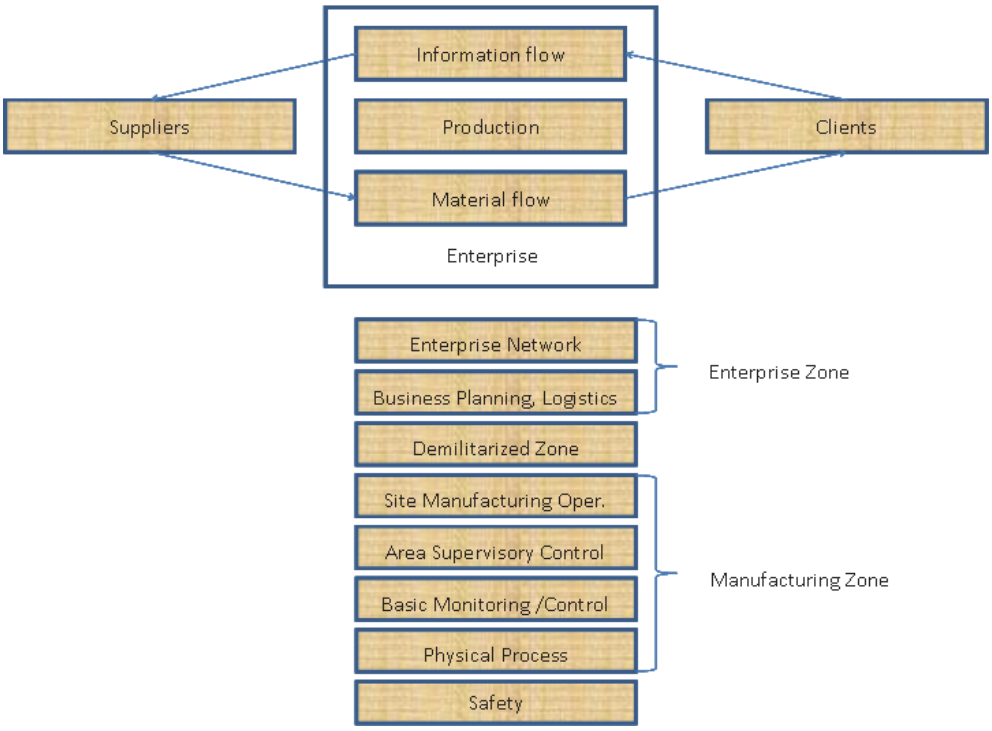



Figure 1. The logistics framework of an electricity company (adapted) and common IT and industrial automation systems (Bowersox et al., 1986, adapted; Knowles et al., 2015)

The highest levels of IT system hierarchy include the general information systems of administration and the enterprise resource planning (ERP) system. The top level of a typical ERP system includes overall process management by, for example, guiding the production volume. It also covers the restocking of raw materials, storing, distribution, payment traffic and human resources. If needed, between ERP software and control rooms there may be a manufacturing execution system (MES), which makes it possible to transfer the information obtained from the control room to the ERP system.

The industrial automation systems of production within an electricity company comprise their own hierarchy levels. Topmost of them is the control room, from which the operation of the entire process is presented to the supervisors in graphic form. Based on the information, process alarms are handled and the operation of the process is monitored and controlled. The next level consists of process stations, which house devices for process control, measuring and regulation. The same level also includes the actions taken to monitor faults and interferences in devices. The lowest level comprises the field equipment used to control and monitor process actuators and to gather measurement data.

Harmful measures to the systems of an electricity company can be implemented by foisting mal- and spyware into the systems through the staff, or they can include intruding or network attacks via wireless connections or the internet. The intruders' goals may be related to the prevention of network services, the complete paralysation of operations, data theft or distortion, and the use of spyware. Components pre-infected with so called backdoors or the programming of components intentionally for the purposes of attackers is also increasingly common in today's cyber world. (Lehto, 2015)

In the USA, the security threats to the electric power system also concern power plant logistics. They involve interfering with and harming raw material supply routes, doing physical damage to transmission and distribution networks as well as to the transformer and switching substations between them, or carrying out cyberattacks on the control and regulation systems of the power grid. (Lewis, 2015)

Trust in the operation of organizations and its continuous maintenance with effective measures are central factors affecting cyber security. Security is based on trust. Without trust there is no security, and vice versa. It is also good to be conscious of the fact that perfect safety is in general hardly achievable, and this applies to the cyber world as well, which is a dynamic environment difficult to anticipate. Therefore, it is particularly important to understand the great significance of trust in the cyber world and its security. The role of measures enhancing trust is emphasized. When we build operations in the cyber world on a foundation that is as sustainable as possible, we can utilize the diverse opportunities it offers. (Limnell et. al., 2014)

The ISO 9000 standard states that an organization achieves success by acquiring and maintaining the trust of clients and other relevant interest groups. Understanding their present and future needs contributes to the organization's continuous success. The standard includes the central concepts of quality management and the principles for building trust. It can be applied by organizations that pursue ongoing success in their operation by utilizing a quality management system of their own. The quality of an organization's products and services is determined by how its clients experience that their needs and expectations are met. Clients also look for guarantees of the organization's ability to systematically produce products and services that correspond to their requirements. The ISO 9000 standard comprises seven quality management principles, which constitute a commonly accepted basis for applying the standard series. The standard also specifies the benefits to an organization that has adopted the principles in its operation. The seven basic quality management principles are related to customer focus, leadership, the engagement of staff, a process approach, continuous improvement, evidence-based decision-making, and relationship management. (ISO, 2017)

Establishing measures that increase cyber world security and trust in a company is primarily the responsibility of corporate leadership. Integrating the necessary measures with the idea of ensured business activities increases their significance and benefits through better processes for the entire organization, interest groups and society. If security is not considered, risk analysis reveals potential damage as well as its costs and social consequences. The leadership's views and requirements brought out in the analysis play a central role in developing security planning for the operating process. The costs and other resources allocated to the activities are simultaneously specified. (Stouffer et. al., 2011)

An organization has a management system generally suitable for its business environment when it is managed systematically and at a high level, taking into account customers, the significance of staff, the efficiency and guidance of processes, continuous development of activities, and interest group communication. The management system can also be utilized in managing the processes of the cyber environment.

In order to build corporate cyber security comprehensively, corporate leadership must define and guide actions at the strategic, operational and technological-tactical levels. The strategic level provides answers to 'why' and 'what' questions. The operational and tactical levels answer the 'how' question. The approach guided by questions ensures that the right things are done and that they are done in line with the set goal. The technological-tactical level must implement the goal-oriented activities defined at the strategic level, not create it. The company's organizational capability in implementing the cyber security measures required by the technological-tactical level ultimately determines how the company manages potential disturbance situations. (Limnell et. al., 2014)

Building corporate cyber security management begins from the level of vision and strategy work. The visions created by corporate leadership to enhance cyber trust are translated into strategic goals, operational-level actions, guidelines and a policy. The practical measures derived from the strategy are realized at the technological-tactical level. Organizational capability factors enable the success of the measures.

In this paper, creating a vision of cyber security in an electricity company is presented in the context of continuous development and maintenance of cyber trust as part of national critical infrastructure. The strategic choices supporting the creation of visions are primarily related to

corporate social responsibility, company reputation, and ensuring business and its economic efficiency. The leadership is expected to make concrete strategic choices as well as support and guide the execution of the chosen measures throughout the organization. It is also important that the leadership ensure sufficient resource allocation to the measures. The chosen measures should be comprehensively communicated to the company's interest groups. (Stouffer et. al., 2011; ISO, 2017)

The measures at the operational level promote the strategic goals. Comprehensive measures that increase security and trust call for holistic cyber security management. It must be based on risk assessment and analyses of the measures based on the assessment. It is also important that the company declares and communicates the policy with which the leadership commits to the measures required to develop cyber security management. The declaration of a policy that ensures cyber security and the development of related procedures must be integrated with the organization's general policies. The highest organizational level is responsible for creating a policy that defines acceptable risk levels and the measures used in the reduction of risks (Stouffer et. al., 2011). The concrete measures at the operational level must be targeted at ensuring data security solutions and at creating business continuity and recovery plans. The maintenance of situational awareness regarding the cyber environment of the electricity company's processes, furthermore, makes it possible to monitor the effects of the operational measures and, when needed, to react efficiently to events that constitute a threat within the company's operating environment. The aim must be to monitor the availability of processes continuously and to support decision-making in disturbance situations that require analyses and decisions (Faber, 2015).

The tactical corporate level encompasses the systems and processes that comply with the logistics framework. Consistent and predictable results are achieved more efficiently when operations are handled and managed as interrelated processes that function as a coherent system (ISO, 2017). Cyber security threats set special requirements for these processes in addition to other operational requirements. At a general level, the performance of processes is determined according to their client-based demands. In an electricity company, uninterrupted production of electricity can be regarded as the most important requirement, and it is achieved through a high availability level of the processes. In the cyber environment, the target can be achieved by defining the processes to be protected, choosing process control mechanisms successfully, and by using expedient technological solutions and services to protect the processes (Stouffer et.al. 2011). Successful operation also calls for the adoption of security-oriented values to guide the activities of staff (Lillrank, 1998). The aforementioned solutions suitable for the cyber environment constitute an entity that can be called a technological-tactical level.

### 3. Applying SWOT analysis to a company's cyber environment

The term SWOT is an acronym of the words Strengths, Weaknesses, Opportunities and Threats. A SWOT analysis is an important tool for analysing an organization's performance and operating environment as a whole. It is a fourfold method commonly applied to create business strategies, to identify learning or problems, to assess and to develop operating processes. A SWOT analysis can be targeted at a specific function of a company, an organization as a whole, the status and competitive ability of a product or service or, for example, a competitor's operation and competitive edge.

In this study, a company's cyber security was analysed from the perspectives of organizational strategy, operative measures, technological-tactical-level solutions and ability factors, with the company's cyber structure and operation considered as part of a networked society. Taking into account these perspectives, the cyber security strengths and weaknesses can be analysed by evaluating their mutual relationship. The most central factor in analysing opportunities and threats is change in the operating environment of a company – in this study, the cyber environment. The analysis of opportunities is then connected to the company's possibility to utilize measures supporting change in order to improve its opportunities to function. The assessment of threats comprises operating environment analyses and threat analyses, based on which measures can be taken to reduce threats.

The interview themes of our SWOT analysis were derived from the strategic guidelines of Finland's Cyber Security Strategy, utilising the seven basic principles of the ISO 9000 quality standard and the key points of the ISO 27000 information security standard. The themes encompass perspectives linked to the cyber structure of a typical electricity company (Table 1), which have been derived from the logistics framework of an electricity company and common IT and industrial automation systems (Figure 1). (SFS, 2012; ISO, 2017; Secretariat of the Security Committee, 2013)

Table 1. The SWOT analysis interview themes

| Strengths and weaknesses | Opportunities and threats |
|---|---|
| • Management<br>• Staff competence<br>• Cyber security products and services<br>• Situation awareness<br>• Stakeholder approach<br>• Ensuring continuity of operation<br>• Expert services | • Acquisition of advanced technology<br>• New cooperation partners<br>• New opportunities for development<br>• Analysing the operating environment<br>• Analysing cyber threats<br>• Analysing the operating network |

## 4. Research results

Based on the interviews, the research results can be summarized according to the SWOT themes (Table 1).

*Strengths and weaknesses*

The strategy-level strengths of electricity companies in management consist of organisation leaders who consider cyber security issues as a strategic goal, a published cyber security policy and risk-based management as part of overall security and business activity. Nationwide clean networks are one of the main strengths for the electric power systems that provide a foundation for the entire critical infrastructure and its services. The weaknesses in management include the challenges of implementing policies throughout the entire organization and identifying severe threats. The corrective actions against vulnerabilities are often reactive rather than proactive. Companies do not have cyber security representation in the management group.

From an operational point of view, the strength of the stakeholder approach is based on the use of the best partners in outsourcing, clustering, public–private partnerships (PPP) and international cooperation. The electricity companies rely on a good reputation among stakeholders. The weakness in the stakeholder approach may be the conflict between a company's business activity and the national supply security requirements (resourcing) for critical infrastructure.

The strength of companies' situation awareness is the possibility to learn about threats often directly from the operating network or partners and the use of announcements of the National Cyber Security Centre Finland. On the other hand, overall situation awareness is often based on scattered data, and obtaining situation awareness of the entire operating network is challenging. Real-time situation awareness of IT assets and industrial automation (ICS) is also challenging.

The strength of electricity companies is based on ensuring continuity of operations through training, planning exercises and preparedness plans.

Electricity companies can leverage expert services as a strength in different audits and in solving problem situations also by utilizing best practices and national research programmes. Weaknesses in this area include the inability of auditing coverage to cover overall operations and software operation/services as well as the reduction in spontaneous research in companies.

The technological-tactical level implementation focus is on staff competence, security products and services. First, the electricity companies emphasize good IT staff competence, e-learning training for other staff groups and the importance of competence verification. These are important strengths despite the challenges of training the entire staff in large organizations. Companies are worried about national in-depth competence because it is in the hands of few people. That means a lack of competence in cases of extensive failures. The electricity companies have a large amount of IT/ICS technology in their assets. It is a challenge to create cyber security competence for both IT and ICS systems at the same time. Second, the electricity companies emphasise good cyber security products and services as strengths. The best possible products worldwide are used. Good competence in services has been achieved through outsourced services. Outsourcing is partly decentralized based on risks. These measures are suitable for ordinary threats. Cyber security products and services have weaknesses that contribute to challenges in evaluating the activities and the cyber security capabilities of the partner network. An insufficient view on the protection of new services (e.g. cloud services) is a real problem for the main business activity of electricity companies.

*Opportunities and threats*

The opportunities of electricity companies are based on the possibility to invest in new advanced technology and find new partners. Competitive advantages include PPP activity and the possibility to create consistent situation awareness by using branch collaboration. New opportunities are also based on the development of national inquiries legislation and on the official support that it provides. Extending benchmarking and developing processes through auditing can also be viewed as future opportunities.

From the perspective of threats, a continuous analysis of the operating environment is important. Unknown threats and security breaches are the most challenging to identify in the large cyber environments of electricity companies. New business models require new technologies (e.g. IoT, robotics), the threats of which are not known. The analyses of cyber threats such as industrial espionage and the ability of governmental actors are the most challenging measures. Electricity companies consider terrorism, cyber-physical influencing of the electrical network, staff risks and threats to key personnel as the most likely threats. Analysis of the operating network is challenging because there is no comprehensive idea of its interdependencies. Outsourced services include the threat that supranational enterprises often restructure operations for financial reasons. These changes could lead to the disappearance of key competence, which means the disappearance of the electricity company's competence.

*Analyse of results*

The protection measures against threats caused by common malware are administratively and technically at a reasonably high level in the entire research area. The operation of the power system is monitored continuously, and people trust in the cleanliness of data transmission networks. The technical protection measures are also at a high level as regards this area. The national power system provides a foundation for the entire critical infrastructure and its services.

As regards cyber threats caused by advanced malware, the situation in the companies is more challenging than with the common malware. Preparedness in this context requires particularly close cooperation between authorities and enterprises. To succeed in this task, the authorities should be granted more rights to take action. The starting point is favourable because the enterprises regard Finland as a pioneer in public–private partnerships (PPP), which significantly contributes to the resilience of the entire society in a cyber environment.

This study extensively identified such measures implemented in companies that promote the guidelines of the national strategy. These measures include, for example, risk-based management, staff training programmes, utilization of the best available products and services for protection, partner networks, expert services (such as auditing services), and practical exercises. Moreover, some organizations possess alarm procedures for quick response to disturbances.

Based on the interviews, there is still reactiveness in the operation of the analysed enterprises, but they have made significant progress toward proactive operation at all decision-making levels. Management is based broadly on strategies and risks, and related issues get relatively wide attention in the policy guidelines of the enterprises. Situation awareness is promoted, and operations are developed through network cooperation and clustering. Preparedness plans have been created and rehearsed. Risk analysis and preparedness planning are increasingly being transferred to the business units, which will improve the link between operations and related threats. The enterprises find that training on risk-based cyber threat prevention is important and a good opportunity to develop operations.

From various perspectives, the maintenance of national research activities is regarded as important. The companies participating in this study expect concrete results from research for developing their activities, particularly in the present situation in which their own research activity has been reduced from previous years. The companies are thus relatively committed to research activities.

Even small enterprises that provide services for electricity companies can play a significant role in the operating networks of larger enterprises. Some of these enterprises are only now launching more comprehensive protection measures than traditional data security. The resourcing of the measures also varies. The most advanced electricity companies may find these chained services challenging. The various parts of the chain are not easily visible, which arouses questions about the cyber security ability of the parts. This point of view is supported by earlier research, such as the study conducted by the Helsinki Region Chamber of Commerce in 2015. According to it, the preparedness of large companies differs clearly from that of smaller ones. The responses indicated that large companies could much better identify intrusions themselves, which is a crucial ability in protection. (Helsingin seudun kauppakamari, 2015)

The level of cyber security management and expertise in the research subjects is good. They utilize the best available products and services to ensure their usability. In addition, the companies cooperate nationally and internationally to establish situation awareness, which is regarded as a definite prerequisite for proactive operation. Several electricity companies that are central to the critical infrastructure have outsourced their data communications, IT services and, consequently, part of their own cyber security management. This network includes both domestic and foreign enterprises. Data security enterprises have high-level expertise in common malware threats, but research has questioned whether the resources are sufficient for potential disturbances that require extensive investigations.

**Conclusions**

Digitalization is an increasingly important element in the interaction between electricity companies and their customers. Digital services are part of this development. Different applications and services are thus more and more often offered on the internet and as cloud services. Enterprises have created deeper real-time relationships with their partners, customers, suppliers of services and goods, and public administration. These procedures in the cyber environment have made overall operations more efficient, but they have simultaneously increased different vulnerabilities. Because of the consequent broadening of threats, special attention must be paid to business risk analysis in all sectors of an enterprise.

Success in developing the operation of an enterprise, or part of it, ultimately depends on how committed its leadership is to the task and how the actions are resourced. It is often necessary to use external developers also because the company's own staff is mainly engaged in their daily operational tasks. Using external development resources is also recommended from the perspective of obtaining extra knowhow. Moreover, cost-effective solutions are invariably worth pursuing.

A SWOT analysis is regarded as a functional tool in creating business strategies, identifying learning or problems, assessment, and developing operating processes. In addition to strategy work in enterprises, the analysis can be applied to survey the other aforementioned areas, comparing them consciously with a chosen scenario and thus creating situation awareness on the

area. Situation awareness and consequent conclusions can be achieved in compliance with a theory developed by Endsley: perception of the analysed situation, comprehension of the situation, and projection of the future status (Endsley, 1995). This situation awareness provides a basis for conclusions and decision-making. The scenario chosen for this study is a company's cyber security and the situation awareness established on it. In order to create situation awareness with an eye on research aims and questions, interview themes were formed based on the framework of the research area and the initial data. At the final stage of the study, the company-specific interviews were compiled into a theme-specific synthesis, which provided a basis for situation awareness, conclusions and development proposals.

Based on the results of the research entity, the concept of national critical infrastructure can be simplified in accordance with Figure 2. An electricity company can position its own strategic role and identify its operation as part of an entity whose other parts depend on a reliably functioning electrical network. This also facilitates the identification of cyber dependencies within the services of the service layer so that they can be secured with the most efficient and practical measures.

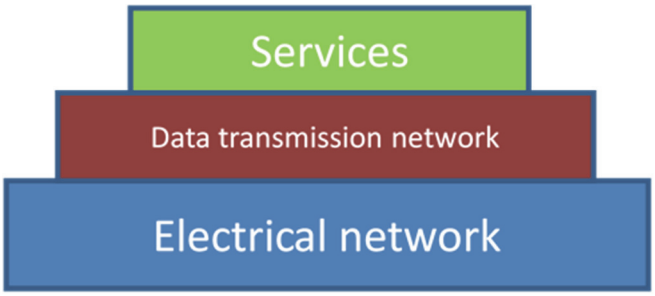



Figure 2. Simplified composition of critical infrastructure

We can conclude based on the study that an energy company's strategic prerequisites for operating in the cyber environment are promoted by active collaboration in different international forums and national public–private partnerships. This enhances general cyber security situation awareness and supports the measures taken to detect and prevent, in particular, the most advanced malware. In addition, branch-specific networking and other networking with the business world is further promoted.

Management at the operational level must be developed toward a more proactive approach. It can be promoted by developing company-specific cyber security systems thinking, in which the processes are in the network and data protection plays a key role. It is ensured that all parts of the network take care of their own protection and that the network nodes continuously maintain themselves as functional parts of the network. The network members' motivation is based on joint cyber security interests and the aim to establish resilience in the core areas. Continuous, active information exchange is of key importance.

At the tactical level, it is important to develop the use of a real-time tactical-level situation awareness system in each enterprise and to utilize the best products and services of partners. The company's procedures of continuous improvement are developed by making technical-level protection methods and auditing more comprehensive, in compliance with the principle of taking into account overall operations, products and services.

The development of measures at all decision-making levels is an investment in the strengthening of competence that promotes cyber security in a company, covering its entire cyber structure. The strength of a company's operations in the cyber environment consists of the following elements: strategy, tools (policy, networks, products and services, preparedness plans), training and assurance.

The results of the study also highlight needs for further research focusing on different dimensions of the cyber environment. These dimensions include the structures and interdependencies of energy companies' networks, development of tactical-level situation awareness, and

the effects of new products and services (e.g. the Internet of Things and cloud services) on the business processes of electricity companies.

## References


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

Endsley M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37.1: 32-64.

Faber S. F. (2015). Analytics for Cyber Situational Awareness. SEI Blog. https://insights.sei.cmu.edu/sei_blog/2015/12/flowanalytics-for-cyber-situational-awareness.html

Fingrid Oyj, (2016). Voimajärjestelmän yleinen kuvaus. Retrieved on 6 August 2016 from http://www.fingrid.fi/fi/voimajarjestelma

Finnish Energy, (2015). Retrieved on 25 October 2015 from http://energia.fi/energia-ja-ymparisto/sahkontuotanto

Finnish Standards Association SFS, (2012). SFS-käsikirja 327. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. SFS ry, Helsinki.

Helsingin seudun kauppakamari, (2015). Yrityksiin kohdistuvat kyberuhat 2015. [online document]. http://helsinki.chamber.fi/media/filer_public/36/0f/360fddcd-4cfe-41a6-ab89c028aa0bf15c/kyberturvallisuus_2015.pdf

International Organization for Standardization, ISO, (2017). ISO9000- Standards. Quality management principles. [online document].http://www.iso.org/iso/pub100080.pdf

Knowles W., Prince D., Hutchison D., Ferdinand J., Disso P., Jones K. (2015). International journal of critical infrastructure protection 9. A survey of cyber security management in industrial control systems.

Lehto M. (2015). Cyber Security: Analytics, Technology and Automation. Springer.

Lewis T. (2015). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Second Edition.

Lillrank P. (1998). Laatuajattelu. Laadun filosofia, tekniikka ja johtaminen tietoyhteiskunnassa. Otavan Kirjapaino Oy, Keuruu.

Limnell J., Majewski K., Salminen M. (2014). Kyberturvallisuus, Docendo Oy, Jyväskylä.

Secretariat of the Security Committee, (2013). Finland's Cyber Security Strategy. [online document]. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Stouffer K., Falco J., Scarfone K. (2011). NIST Special Publication 800-82. Guide to Industrial Control

Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce. [online document]. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

**Artikkeli P2:**



# Application of Cyber Resilience Review to an Electricity Company

2018
Jouni Pöyhönen, University of Jyväskylä, Jyväskylä Finland,
Viivi Nuojua, University of Jyväskylä, Jyväskylä Finland,
Martti Lehto, University of Jyväskylä, Jyväskylä, Finland
Jyri Rajamäki, Laurea University of Applied Sciences, Espoo, Finland

Originally published in the proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS2018, 28 - 29 June 2018, Oslo, Norway, pages 380-389

# Application of Cyber Resilience Review to an Electricity Company

Jouni Pöyhönen[1], Viivi Nuojua[1], Martti Lehto[1], Jyri Rajamäki[1,2]
[1]University of Jyväskylä, Jyväskylä, Finland
[2]Laurea University of Applied Sciences, Espoo, Finland
jouni.a.poyhonen@jyu.fi
viivi.nuojua@jyu.fi
martti.j.lehto@jyu.fi
jyri.rajamaki@laurea.fi

**Abstract**

The functioning of a modern society is based on the cooperation of several critical infrastructures, whose joint efficiency depends increasingly on a reliable national electric power system. Reliability is based on the functional data transmission networks of the organizations belonging to the electric power system. Furthermore, reliability is linked to the confidentiality, integrity and availability of system data in the operational environment, whose cyber security risks are continuously augmented by the threatening scenarios of the digital world. In Finland, the electricity generation is in various ways distributed, which contributes to the reliability of the electric power system. There are about 120 electricity generation companies and about 400 power plants nationally, in which the electricity is produced using various production methods. The control of electric power system's operational processes is highly automated and networked. The major contribution of the paper is to apply the cyber resilience review to a single electricity company. The basis is in SWOT analysis, which is used for analyzing and that way for bettering the cyber security level of an organization. However, there is not such as perfect security. Security is based on trust, which can be developed with the help of preparedness planning. Resilience review can be seen as preparedness planning that also enables contingency planning. Resilience metrics framework proposed by Linkov et al. is utilized by applying the resilience measures to the organization's operational processes. In addition, open source intelligence and organization's operating networks are used for collecting significant security information and that way for updating the preparedness plan, i.e. resilience plan. In order to put the resilience plan into practice, the leadership of an organization must regard resilience measures related to cyber security as a strategic goal and communicate to their staff the importance of contingency planning in achieving the goals. As a result, the cyber security management of an electricity company is improved.

Keywords: Critical infrastructure, cyber security management, electricity company, resilience, trust.

## 1. Introduction

Electricity is produced at Finnish power plants in various ways, by using several energy sources and production methods. The major sources of energy include nuclear power, hydropower, coal, natural gas, wood fuels and peat. In addition to the sources of energy, production can be classified according to the production method. In Finland there are about 120 enterprises that produce electricity as well as around 400 power plants, over half of them hydroelectric power plants. Nearly a third of electricity is produced in connection with heat production. Compared with many other European countries, Finland's electricity production is distributed. A diverse and distributed electricity production structure increases the security of the national energy supply (Finnish Energy, 2015).

The global threats within the cyber environment have remained at a high level over the past few years, as stated in the annual international business world surveys by the World Economic Forum. Cyber threats are seen to be among the major global threats based on their likelihood and impact (World Economic Forum, 2018).

The electric power system with all its components belongs to critical national infrastructure: it is vital for the operations of a country, and its outage or destruction would weaken national security, economy, public health and safety as well as make the operations of state administration less effective. The criticality of a power system is expressed clearly in the seminar presentation "The power system as a basis for a functioning society" (in Finnish: "Sähköjärjestelmä yhteiskun-

nan toimivuuden perustana") given by the former chief executive officer of the National Emergency Supply Agency. Table 1 is an extract from the presentation. It describes the effects of power failure on the operations of society as a function of the duration of the failure. Endangered cyber security has been regarded as one of the most significant threats to the functioning of energy supply and energy networks (Kananen, 2013).

A diversified and distributed power production structure increases the national security of power supply. Considering cyber security in the different parts of the infrastructure further enhances trust in the services of our society. The recent experiences of the disturbances in cyber operational environment (ICS-CERT, 2016) have showed that it is difficult to achieve perfect protection. Thus, the enterprises have acknowledged and accepted the fact that there will always be disturbances, and rather concentrate on preparing for them. The term resilience affiliates with tolerating disturbances. Generally, it means flexibility, and the ability to survive and adapt in unpredictable and surprisingly developing situations. According to Hilton, Wright and Kiparoglou (2012) there is not one universal definition for the word resilience. However, they approach the definition problem via systems thinking: resilience can be seen as an enterprise's capacity and capability to achieve its purposes in both predictable and unpredictable situations or under continuous stress.

According to Willis and Loa (2015) there are plenty of published reports on the resilience metrics applied to energy industry. They divide the reviewed metrics into five levels. The input level metrics depict the amount of the produced, transmitted or stored energy, or the number of people, facilities or equipment supporting the first-mentioned activities. The capacity level metrics depict the systems, policies and organizations supporting the energy capabilities. The capability level metrics depict the capability of energy systems for providing sources or factors. The performance level metrics depict the quality, amount and efficiency of the services provided by energy systems. Lastly, the outcome level metrics depict the influence of energy on health, safety and economy, i.e. societal welfare.

The EECSP-Expert Group (2017) emphasizes the following two high-level objectives as the goal of stakeholders in the energy sector: 1) The security of energy systems providing essential services to the European society, and 2) the data protection in the energy systems and the data privacy of the European citizen. In May 2018, the General Data Protection Regulation (GDPR) approved by the European Commission was entered into force, and the Directive on security of Network and Information Systems (NIS Directive) adopted by the European Parliament was supposed to be integrated in national laws. The purpose of the aforementioned GDPR and NIS directive is to better the trustworthiness of the online environment and that way the functioning of the EU Digital Single Market.

National Institute of Standards and Technology (NIST, 2018) introduces a cyber security framework that helps internal and external stakeholders to understand, manage and express cyber security risks in co-operation. It can be utilized for identifying and prioritizing actions in order to reduce cyber security risk. In addition, it can be used for aligning policy, business and technological approaches in order to manage that risk. The framework can be applied to the entire organization or to some specific critical service. So-called Framework Core guides in achieving specific cyber security outcomes and that way helps in managing cyber security risk.

**Table 1:** The consequences of power failure (Kananen, 2013).

| **Interruption time** | **Consequences** |
|---|---|
| 1 second | Sensitive industrial processes may stop. Data in information systems may be lost. |
| 1 minute | Some industry and hospital processes will stop. |
| 15 minutes | Shops will be closed. The failure may harm people's daily activities and cause traffic delays. |
| 2–3 hours | Industrial processes may undergo significant damage. Mobile phone networks will face problems. Domestic animal production will be disturbed. |
| 12–24 hours | Water supply to homes and offices will stop. Buildings will start to become cold in the winter. Frozen goods will begin to melt. |

| | |
|---|---|
| Several days | The operations of society will be seriously harmed. Industry and services will not function. Workplaces and schools will be closed. Buildings will suffer from frost damage. |

This paper presents a process created with the help of aforementioned cyber security framework, and thus stands out from the previous papers. It pays attention to the cyber security of an energy company as part of the organization's overall resilience planning and that way continuity management.

Preparedness planning enables the proactive contingency planning for the operation's continuity management and that way building of trust in the management of cyber security related problematic situations, i.e. the promotion of cyber resilience. It includes preliminary planning of contingency, the plan for encountering disturbance situations and for how to recover and learn from those. In this research, the following two fundamental questions of resilience review have been explored:

1. Is it possible to create such procedures for resilience review that help to do the planning as a continuous process for supporting the management?
2. What are the most essential matters taken into consideration when planning the resilience of a Finnish electricity generation company?

A procedure suitable to answer our first research question can be found from the earlier national research related to the situational awareness of Finland's cyber security (Pöyhönen and Lehto, 2017). The basis is in a certain present state analysis, SWOT analysis, which is used for analyzing and that way for bettering the cyber security level of an organization. A case study into a typical regionally operating electricity generation company is chosen as a research strategy. It helps to figure out the factors related to the cyber management of a single electricity company, and how these factors should be taken into account in the structures of the company's operational processes. The focus of the research is in the main process of an electricity company, which consists of the raw material supplies, i.e. supplier network, production process and distribution network (= customers). A resilience metrics framework proposed by Linkov et al. (2013a) is utilized by applying the resilience measures to the organization's operational processes. In addition, an OSINT utilizing framework introduced by Lee and Shon (2016) is used for collecting significant security information, and that way for improving the organization's preparedness planning.

The rest of the paper is organized as follows. Section 2 describes electricity company's cyber-physical operational environment and how its situational awareness can be analyzed and improved. Section 3 provides tools for resilience planning. Section 4 introduces our proposed model for how to add a company's resilience. Section 5 concludes the paper.

## 2. Electricity company's cyber-physical operational environment and its situational awareness

### 2.1 The structure of an electricity company's cyber-physical operational environment

The highest levels of IT system hierarchy include the general information systems of administration and the enterprise resource planning (ERP) system. The top level of a typical ERP system includes overall process management by, for example, guiding the production volume. It also covers the restocking of raw materials, storing, distribution, payment traffic and human resources. If needed, between ERP software and control rooms there may be a manufacturing execution system (MES), which makes it possible to transfer the information obtained from the control room to the ERP system.

The industrial automation systems of production within an electricity company comprise their own hierarchy levels. Topmost of them is the control room, from which the operation of the entire process is presented to the supervisors in graphic form. Based on the information, process alarms are handled and the operation of the process is monitored and controlled. The next level consists of process stations, which house devices for process control, measuring and regulation. The same level also includes the actions taken to monitor faults and interferences in devices. The

lowest level comprises the field equipment used to control and monitor process actuators and to gather measurement data.

Cyber-physical systems are software platforms that monitor, control and protect physical operational processes (Sadeghi, Wachsmann and Waidner, 2015). Their structure can be described as a five-layered structural model where each of the aforementioned systems and their parts can be placed. The structures are (Lehto, 2015):

1. Cognitive domain
   - humane problem solution and interpretation environment
   - the understanding and interpretation of the information's meaning
2. Service domain
   - public and commercial network services
   - operational and communicational services
3. Semantic domain
   - information and data content controlled by the user
   - the direction of the system operations controlled by the user
4. Syntactic domain
   - the control and management software of the system
   - network protocols, error handling, handshakes
5. Physical domain
   - network devices, switches, routers
   - wired and wireless communications

Related to the research target the following cyber-physical systems were recognized:

1. Supplier network (company level IT)
2. Production process (ICS operator)
3. Distribution network (company level IT / ICS operator)
4. Real estate automation (ICS operator)
5. Security system (company level IT / ICS operator)

These systems correlate in many ways, and via their data transmission networks they are also correlated to their operational environment.

**2.2 The situational awareness of an electricity company's cyber security**

The aforementioned IT and industrial automation systems are part of the common cyber world, in which the primary risks are related to the loss of money, sensitive information and reputation as well as to business hindrance. Security solutions are hereby the key elements in risk management. The vulnerabilities behind the risks can be analyzed as insufficient technology in relation to attack technology, insufficient staff competence or inappropriate working methods, deficiencies in the management of organizations, and lacks in the operating processes or their technologies. The most common motives of attackers are related to the aim of causing destructive effects on processes, making inquiries about process vulnerabilities, and anarchism or egoism. These attacks can even be carried out by state-level actors, but perhaps most commonly by organized activists, hackers or individuals acting independently (Lehto, 2015).

Harmful measures to the systems of an electricity company can be implemented by foisting mal- and spyware into the systems utilizing the staff; or they can include intruding or network attacks via wireless connections or the Internet. The intruders' goals may be related to the prevention of network services, the complete paralysis of operations, data theft or distortion, and the use of spyware. Components pre-infected with so-called backdoors, or the programming of components intentionally for the attacker's purposes is also increasingly common in today's cyber world (Lehto, 2015).

In the USA, the security threats to the electric power system concern power plant logistics. They involve interfering and harming raw material supply routes, doing physical damage to transmission and distribution networks as well as to the transformer and switching substations between them, or performing cyberattacks to the control and regulation systems of the power grid (Lewis, 2015).

The significance of the systems' usability is essential when considering the business result formation and the operation's reliability. In addition, the reliability and content integrity of the information included and used in the processes are essential objectives. As a result, the overall trust should be aimed to build. It is based on the targeted organization's realistic understanding of its own capabilities to manage reliably the challenges related to operating in cyber world. One solution for building up a company-specific understanding of the situational awareness is SWOT analysis (Pöyhönen and Lehto, 2017).

The term SWOT is an acronym of the words Strengths, Weaknesses, Opportunities and Threats. SWOT analysis is an important tool for analyzing an organization's performance and operating environment as a whole. The interviewing themes presented in Table 2 encompass perspectives linked to the cyber structure of a typical electricity company, which have been derived from the logistics framework of an electricity company and common IT and industrial automation systems.

In this study, a company's cyber security was analyzed from the perspectives of organizational strategy, operative measures, technological-tactical-level solutions and ability factors, with the company's cyber structure and operation considered as part of a networked society. Taking into account these perspectives, the cyber security strengths and weaknesses can be analyzed by evaluating their mutual relationship. The most central factor in analyzing opportunities and threats is the change in the operating environment of a company – in this study, the cyber environment. The analysis of opportunities is then connected to the company's possibility to utilize measures supporting change in order to improve its opportunities to function. The assessment of threats comprises operating environment analyses and threat analyses, based on which measures can be taken to reduce threats.

## 3. Electricity company's resilience planning

### 3.1 The adaptation of the resilience metrics framework to the planning

The trust on organizations' operation and its continuous maintenance with efficient actions is an essential matter when thinking of the factors influencing cyber security. The security is based on trust. If there is no trust, there is no security and vice versa. It is good to acknowledge that perfect security cannot be achieved, either when operating in cyber world, which is dynamic and difficultly foreseeable operational environment. Thus, it becomes even more important to understand how significant our trust in cyber world and its security is. The significance of the operations building up trust is emphasized. When building the operations in cyber world on a solid base, we are able to utilize its diverse possibilities (Limnéll, Majewski and Salminen, 2014).

Trust can be developed by utilizing preparedness planning. Linkov et al. (2013a) introduce a resilience matrix framework (later: "Linkov model") that can be used for this planning. It combines the four stages of a system 1) plan/prepare, 2) absorb, 3) recover and 4) adapt with the four domains of a system 1) physical, 2) information, 3) cognitive and 4) social. Later on Linkov et al. (2013b) apply their model further to cyber systems. Their purpose is to develop efficient metrics to measure the resilience of cyber systems (Linkov et al., 2013a; Linkov et al., 2013b).

In case of cyber systems, the cells of the resilience matrix can be interpreted as follows: How capable the system is to prepare/absorb/recover/adapt in case of a cyber disturbance executed within the physical/information/cognitive/social domain? Adding one metric to a certain domain often requires adding metrics to other domains too. Resilience metrics are used for recognizing and prioritizing the needs, for tracking progression and for sharing resources. Thus, they constitute an essential part of planning and decision-making (Linkov et al., 2013b).

### 3.2 The maintenance of the planning with the help of OSINT

Open Source Intelligence (OSINT) can be used for the collection of significant security information. This kind of open or i.e. public references consist not only of newspapers and magazines representing traditional media but also of the Internet representing digital media (Lee and Shon, 2016).

**Table 2:** The SWOT analysis interview themes (Pöyhönen and Lehto, 2017).

| Strengths and weaknesses | Opportunities and threats |
|---|---|
| • management<br>• staff competence<br>• cyber security products and services<br>• situational awareness<br>• stakeholder approach<br>• ensuring continuity of operation<br>• expert services | • acquisition of advanced technology<br>• new cooperation partners<br>• new opportunities for development<br>• analysing the operating environment<br>• analysing cyber threats<br>• analysing the operating network |

Lee and Shon (2016) introduce an OSINT utilizing framework for examining the cyber threats of critical infrastructure. Their solution helps to improve the security level of critical infrastructure by analyzing previously unnoticed cyber threats, and that way making it possible to prevent zero-day vulnerabilities too. OSINT adapts particularly well to the critical infrastructure data network because of the nature of its communication models and environments. Lee and Shon's solution can be used for completing the signature-based threat detection methods and for anomaly detection (Lee and Shon, 2016).

According to Lee and Shon (2016), the OSINT utilizing intelligence has to fulfil two conditions: the content and reference of the analyzed information have to be confirmed, and the intelligence has to be useful and meaningful in relation to its use. When making the OSINT plan, the target system is chosen first and then, the method and timetable for collecting the public information is decided. In the preparation phase, the internal information related to the target under examination is verified and based on that the initial intelligence database is created. Finally, the OSINT data collection tools are used for collecting the information about the target under examination. By utilizing the database created in the initial intelligence, the reliability of the collected information is verified, and at the same time, the initial intelligence information is updated (Lee and Shon, 2016).

### 3.3 The maintenance of the planning with the help of operating networks

The strategy-level strengths of electricity companies consist of the organization leaders who consider cyber security issues as a strategic goal, and a published cyber security policy and risk-based management as part of overall security and business activity. Nationwide clean networks are one of the main strengths for the electric power systems that provide a foundation for the entire critical infrastructure and its services. From an operational point of view, the strength of the stakeholder approach is based on the use of the best partners in outsourcing, clustering, public-private partnerships (PPP) and international cooperation. The strength of companies' situational awareness is the possibility to learn about threats often directly from the operating network or partners, and the use of announcements of the National Cyber Security Centre Finland. Competitive advantages include PPP activity and the possibility to create consistent situational awareness by using branch collaboration (Pöyhönen and Lehto, 2017).

## 4. Resilience adding operations

### 4.1 Resilience development as a continuous process

Establishing measures that increase cyber security and trust in a company is primarily the responsibility of corporate leadership. Integrating the necessary measures with the idea of ensured business activities increases their significance and benefits through better processes for the entire organization, interest groups and society. If security is not considered, risk analysis reveals potential damage as well as its costs and social consequences. The leadership's views and requirements brought out in the analysis play a central role in developing the security planning of the operating process. The costs and other resources allocated to the activities are simultaneously specified (Stouffer, Falco and Scarfone, 2011).

Systematical and good quality management of an organization is enabled with a proper management system. It pays attention to the customers, the significance of the staff, the efficiency and control of its operational processes, the continuous development of its operation and the

interest group communication. The management system can also be used for controlling the operational processes of the cyber operational environment.

As a solution for research question 1, the resilience management process presented in Figure 1 was developed. It can be linked to the management system of an organization. When creating the resilience management process, we utilized the following: the definition of the target organization's cyber-physical systems, SWOT analysis, Linkov model, OSINT and the electricity companies' strength in utilizing its own operating networks for data collection.

After defining the target organization, the cyber-physical systems related to its operational processes are recognized and placed in the systems' cyber structure described in section 2.1. After that, SWOT analysis can be applied to the organization as a theme interview by taking into consideration the cyber structure. This enables the drafting of the resilience basic plan during the normal conditions (Linkov model stages 1–3) for all the domains (physical, information, cognitive and social). The Linkov model stage 4 includes all the aforementioned domains too but their final content must be defined based on the aftermath of the possible disturbance situation. The purpose is that the organization learns from the disturbance situations as efficiently as possible. The operations of the organization are developed by repeating SWOT analysis. As a result, the plans are updated for each of the Linkov model stage's part as a repairing operation. The preparedness planning of the normal conditions (stage 1) should continuously be maintained with the help of OSINT model and by utilizing the company's own data collection channels, such as operating networks, in the update process.

It should be noted that the resilience process can be utilized for the impact evaluation of the system correlations when revising the cyber-physical systems. The process model in Figure 1 is recommended to be included as part of the organization's management system in order to accomplish practical operations.

The implementation process of the resilience operations serves all the decision-making levels of an organization. In SWOT analysis, the analysis of the organization's performance and its operational environment on the whole supports especially the strategic planning. It also produces information to other decision-making levels in learning and problem recognition, evaluation and development of operational processes. Linkov model serves the planning and maintenance of the organization's operational continuity management, which supports the operation of the operational and technological-tactical levels.

### 4.2 The most essential resilience adding operations

The basis for trust adding operations is the envisioning of the company's operations in order to achieve the goals. It is made possible with the strategy definition derived from the vision. The electricity company's operational business processes include systems such as fuel logistics and input system, production system and its support processes, and electricity distribution operation. Because all the aforementioned components are needed in the operation of an electricity company, their mutual dependence, and the control and supervision of functionality solve the succeeding of the whole operation. In order to achieve a successful cyber security management, the different operations should be considered as equal.

Linkov model and its different stages suit especially for the operational and technical-tactical level preparedness planning, and that way for ensuring the continuity of operation. Considering the structure of the previously described cyber-physical systems, it is possible to find those targets from the operation of an electricity company that are in a central position in preparedness planning. The company-specific content of the operations has to be based on the present state analysis carried out before using Linkov model, and on the situational awareness got from that in the form of target organization's strengths, weaknesses, possibilities, threats and their mutual relations. SWOT analysis described in section 2.2 gives a good overview of the cyber security of a critical infrastructure target against the managemental and national security requirements. Based on the analysis, the related needs of each organization can be planted on the planning stages of Linkov model (see Table 3).

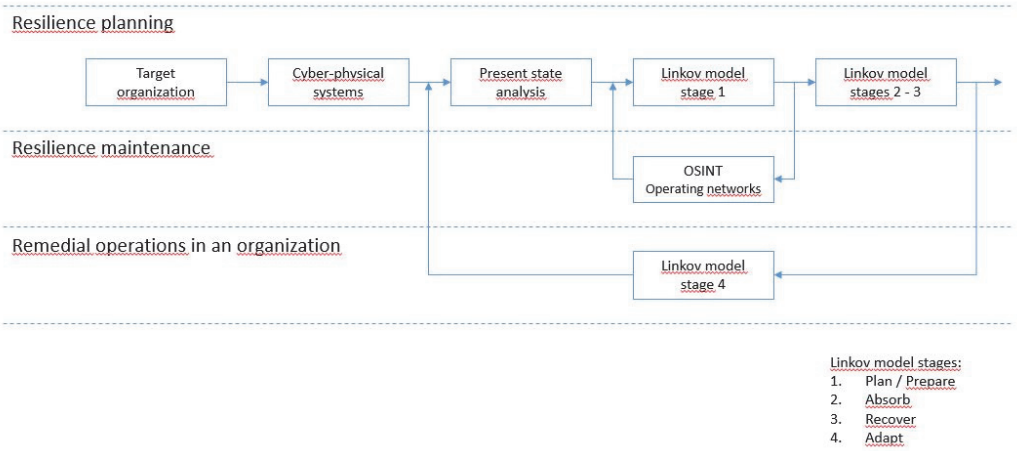



**Figure 1:** The implementation process of the resilience operations.

**Table 3:** Research results planted on the Linkov model.

| | Plan/Prepare | Absorb | Recover | Adapt |
|---|---|---|---|---|
| **Physical** | • technical situational awareness<br>• segmentation<br>• alternative resources | • recognition of disturbances, their scope and impacts<br>• protection of sensitive information<br>• deployment of alternative resources<br>• isolation of disturbance | • maintenance of situational awareness<br>• ramp-up<br>• testing | • updates |
| **Information** | • classification and prioritization of critical systems<br>• business impacts<br>• preparation of sensitive information protection<br>• communication plans | • documentation<br>• informing of authorities and stakeholders | • documentation<br>• informing of the press | • aggregation of documents |
| **Cognitive** | • perception of situational awareness<br>• scenarios and models<br>• situational management<br>• resourcing<br>• training and benchmarking<br>• feedback system | • analysis of situational awareness<br>• additional resources<br>• prioritization<br>• censor information | • allocation of expertise<br>• collection of data and log information | • log analysis<br>• impact analysis<br>• situation analysis<br>• feedback analysis<br>• system updates<br>• continuous improvement |

| | | | | |
|---|---|---|---|---|
| **Social** | • naming of stakeholders' contact persons<br>• training for exceptional situations | • informing about operations | • informing about operations | • staff training<br>• informing about development operations<br>• update of stakeholder information |

The following operations of the planning and absorb stages within the physical domain of Linkov model were recognized: taking care of the functionality, supervision and control of the technology, planning of the system isolation and needed operational segments, and planning of the alternative networks and routes. In case of a disturbance situation, firstly, the situational awareness of the incidence, its nature, distribution and scope are clarified, as well as its impact. After that, the plans are put to use for their needed parts. In the recovery stage, the cleanliness and functionality of the systems is ensured for all of their parts. Then, the comprehensive ramp-up of the machines is guided through. The adaptation stage is determined by the experiences got from the incident, but at least the technical protection operations must be considered carefully.

The documentation planning is emphasized in the operations of information domain, by paying attention to the situation-specific documentation itself, and the critical operations and related requirements has to be documented already in the planning stage. The aforementioned documentation both serves the operation in a disturbance situation and enables the information documentation during the disturbance situation and in a recovery stage, so that the utilization of situation-specific experiences and learning in the adaptation stage is made possible. The informing of essential stakeholders and different authorities must also be included in each stage.

In our case study, the plan of cognitive domain grew the most of all domains. Thus, it can be seen very significant in both management, in building the situational awareness, in continuity management, in prioritizing the operations, and in managing and controlling different resources, including services. All these operations play a decisive role in a disturbance situation, in the recovery stage and in the adaptation stage when utilizing the knowledge gained from the previous stages.

The planning stage of the social domain consists of more specific communication plans than in the information domain, including the named contact persons, and both internal and external interest groups. The widescale situation-specific informing in the different stages results from the planning of the social domain. In addition, the planning of the social domain includes the whole staff training in managing all the different stages.

## 5. Conclusions

The national electric power system and its electricity generation is part of the national critical infrastructure. The operation of a modern society is based on a reliable national electric power system. To ensure the usability and reliability of the electricity companies' operational processes in all the operational environments is an essential part of the critical infrastructure's performance. Therefore, the electricity companies' operations to manage the cyber security of their processes form an important part in ensuring the reliability of electricity generation.

The most significant cyber environment related risks of the electricity company's operational processes require building up and maintaining the trust in all the business levels. The comprehensive cyber trust adding operations of the company together with the development of the cyber operational abilities improve its competitiveness too.

In the case study part of this research the process flowchart for the electricity company's resilience planning was developed, and a Linkov model compatible preparedness planning was made in a table format and on the title level to better the resiliency of the target organization. The previous research results of SWOT analysis have been utilized in this paper as described earlier, and the analysis has been targeted at the company's operational networks and its cyber-physical systems' structures. The Linkov model compatible tables were compiled by utilizing the SWOT

analysis themes and by keeping in mind the structure of the target's cyber-physical systems. From the results an analogy between the structures of Linkov model and Lehto's cyber-physical systems can be drawn. Especially the planning of Linkov model's physical and cognitive domains benefits from the detailed knowledge of the system structure. The planning of the information domain is targeted also at the cyber-physical system covering all of its levels, and in addition, it is targeted at all the organization's interest groups. The social planning domain serves the consideration of all the interest groups. The conclusions from the usage of the models are the following:

1. Linkov model expands the preparedness planning outside the cyber structure.
2. The cyber structure of systems enables the detailed targeting of the planning at all the domains of cyber-physical systems.
3. By combining the models, it is possible to get a comprehensive planning environment for the resilience review of the cyber-physical systems and for securing the continuity.

The preparation for cyber threats and a concrete preparedness planning form the basis for the organization's proactive preparation in its cyber operational environment, when it comes to the electricity company's cyber security management and to the development of trust in the operation. These cyber resilience adding plans and operations are recommended to be included as a fixed part of the company's overall security, when they support the management of an organization in all of its levels.

Since the energy companies are essential service providers for the society, the introduced process for developing the organization's resilience answers to the basic requirement of NIS Directive (The European Parliament and the Council of the European Union, 2016): "Operators of essential services and digital service providers should ensure the security of the network and information systems which they use".

Investigations have revealed that the extensive power failure in Ukraine on 23 December 2015 was caused by a coordinated cyberattack by an external party to the control systems and data warehouses of three enterprises in charge of power distribution. One potential target of the attack is suspected to be the industrial automation system, which the hackers may have managed to enter via a remote access service. When preparing for cyberattacks against industrial automation systems and trying to improve their resistance, organizations are recommended, in the first place, to introduce the best practices of cyber security management (ICS-CERT, 2016).

The generalization of the research results can be examined by utilizing the process flowchart of the resilience planning. It enables the repeatability of this research and the generalization of the material, such that the procedure can be applied to other energy companies too. In addition, a single case of the research target can be handled thoroughly enough by combining the domains of Linkov model, and the structure model of the cyber-physical systems presented by Lehto.

The further research needs are suggested to be targeted at developing the resilience of other critical infrastructure organizations.

**References**

EECSP-Expert Group (2017). *Cyber Security in the Energy Sector*. EECSP Report.

The European Parliament and the Council of the European Union (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council. *Official Journal of the European Union*.

Finnish Energy (2015). *Electricity generation*. [online] Available at: https://energia.fi/en/energy_sector_in_finland/energy_production/electricity_generation [Accessed 16 Nov. 2017].

Hilton, J., Wright, C. and Kiparoglou, V. (2012). Building resilience into systems. *2012 IEEE International Systems Conference SysCon 2012*.

ICS-CERT (2016). *Cyber-Attack Against Ukrainian Critical Infrastructure*. [online] Available at : https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [Accessed 16 Nov. 2017].

Kananen, I. (2013). *Sähköjärjestelmä yhteiskunnan toimivuuden perustana*. National Emergency Supply Agency.

Lee S. and Shon T. (2016). Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures. *2016 Future Technologies Conference (FTC).*

Lehto, M. (2015). Phenomena in the Cyber World. *Cyber Security: Analytics, Technology and Automation*. Springer.

Lewis, T. (2015). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. 2nd Edition. Wiley.

Limnéll, J., Majewski, K. and Salminen, M. (2014). *Kyberturvallisuus*. Jyväskylä: Docendo.

Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. and Seager, T. (2013a). Measurable Resilience for Actionable Policy. *Environmental Science & Technology*.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen J. and Kott, A. (2013b). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), pp. 471-476.

National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1.

Pöyhönen, J. and Lehto, M. (2017). Cyber security creation as part of the management of an energy company. *Proceedings of the 16th European Conference on Cyber Warfare and Security* [also] ECCWS2017, Dublin, Ireland, June 2017. Academic Conferences International.

Sadeghi, A., Wachsmann, C., and Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*.

Stouffer, K., Falco, J. and Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82.

Willis, H. H. and Loa, K. (2015). *Measuring the Resilience of Energy Distribution Systems*. [online] Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR883/RAND_RR883.pdf [Accessed 27 May 2018].

World Economic Forum (2018). *The Global Risks Landscape 2018*. [online] Available at: http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape [Accessed 23 Jan. 2018].

**Artikkeli P3:**

ResearchGate

# Cyber security of vehicle CAN bus

2019

Jouni Pöyhönen, Pyry Kotilainen, Janne Kalmari, Janne Poikolainen, Pekka Neittaanmäki, University of Jyväskylä, Jyväskylä Finland

Originally published in the proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS2019, 4 - 5 July 2019, University of Coimbra, Portugal, pages 354-363

# Cyber security of vehicle CAN bus

Jouni Pöyhönen, Pyry Kotilainen, Janne Kalmari, Janne Poikolainen, Pekka Neittaanmäki
University of Jyväskylä, Jyväskylä, Finland
jouni.a.poyhonen@jyu.fi
pyry.kotilainen@jyu.fi
janne.a.e.kalmari@jyu.fi
janne.poikolainen@jyu.fi
pekka.neittaanmäki@jyu.fi

**Abstract**

There are currently many research projects underway concerning the intelligent transport system (ITS), with the intent to develop a variety of communication solutions between vehicles, roadside stations and services. In the near future, the roll-out of 5G networks will improve short-range vehicle-to-vehicle traffic and vehicle-to-infrastructure communications. More extensive services can be introduced due to almost non-delayed response time. Cyber security is central for the usability of the services and, most importantly, for car safety.

The Controller Area Network (CAN) is an automation bus that was originally designed for real-time data transfer of distributed control systems to cars. Later, the CAN bus was developed as a universal automation system for many automation solutions. One of its characteristics is that bus traffic is not supervised in any way due to the lack of timing of control. In other words, there are no authentication mechanism.

This article highlights different approaches and their usability to reveal the car's CAN bus malfunctions. The study complements earlier studies on the safety of vehicles in the CAN bus. Based on the test results, practical methods can be evaluated to detect changes in CAN bus traffic, such as targeted cyber-attacks. The article is based on the results of a study on the cyber-security of cars conducted at the University of Jyväskylä (AaTi study).

Initially, the AaTi study attempted to identify the message content of the bus and to detect interferences via the Neural network solution. However, the problem with the neural network was the computational performance required and the lack of prediction accuracy. After that the study was focused on experiments that were based on the arrival times of control messages, that is, their timing-based intrusion detection. In this sense the research did concentrate on kernel density estimation, one-class support vector machine solution, absolute deviation method and categorization. Due to methodological challenges, a method for detecting intrusions based on statistical processing of message traffic was ultimately developed as an outcome of the study.

Keywords: Cybersecurity, car, CAN bus, intrusion detection

## 1. Introduction

The term intelligent transport systems (ITS) refers to using roadside infrastructure and communication solutions for improving traffic flows and making traffic safer. In order to realize the perquisites for smart traffic, current national and international research projects are focusing on the development of platforms for weather, security and geolocational solutions. These include test environments for real-time road weather reports based on location data as well as for ITS cyber security. (Finnish Meteorological Institute, 2017)

Service usability is closely linked to cyber security, in which taking care of vehicle cyber security can be seen as a primary objective. CAN bus is a network solution originally developed

for real-time communication in distributed automotive control systems, such as in engine control units, ABS brakes and drivetrains. (Alanen, 2000)

CAN bus later evolved as a general-purpose automation solution to accommodate other use cases in addition to automotive use. The real-time requirement makes minimizing network delays one of the main principles of CAN-bus functionality. This optimization also leads to design decisions that excluded many safety mechanisms, including authentication. These features make CAN bus implementations vulnerable to several types of attacks, including network traffic forgery, unauthorized access to data and denial of service attacks. As the growing use of automation means also the growing use of network connectivity, the attack surfaces in vehicles can be divided into two groups: surfaces that can be exploited remotely and surfaces requiring physical access. Because of development of intelligent transport systems and smart traffic the need of remote connections will grow even more in the future as ITS develops further. Vehicle network security research has emerged in past years, especially after the inherent vulnerabilities in commonly used technologies have been realized.

The purpose of this article is to present different approaches and their abilities to detect anomalies in vehicle CAN buses. Based on the results of this study, methods plausible for real-world scenarios are proposed. The ultimate goal of the study has been to develop real-time situational awareness methods for automation systems. This report is based on a study (AaTi) conducted at the University of Jyväskylä, which concluded on 30 September 2018.

In addition to the chapters dealing with introduction and the CAN bus description, the paper includes a short description from other relevant vehicle studies and explanations from the methods used in the AaTi study to detect harmful bus traffic and the results obtained from their use. The conclusion chapter includes the summary of the AaTi study.

## 2. The CAN BUS Electricity

### 2.1 The CAN Standard

The CAN communications protocol, ISO-11898: 2003, describes how information is passed between devices on a network and conforms to the Open Systems Interconnection (OSI) model, which is defined in terms of layers. Actual communication between devices connected by the physical medium is defined by the physical layer of the model. The ISO 11898 architecture defines the lowest two layers of the seven-layer OSI/ISO model as the data-link layer and the physical layer, shown in Figure 1 (Corrigan, 2016).

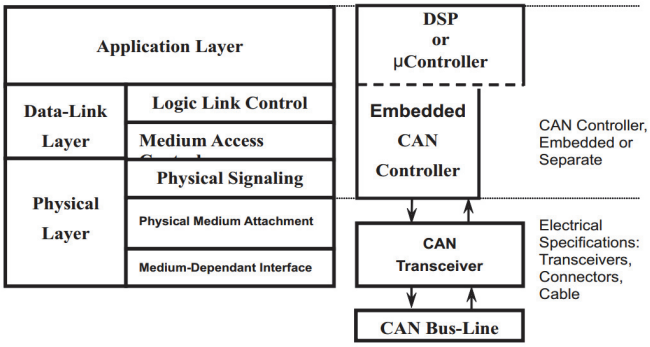



Figure 1 CAN bus in the OSI/ISO model

The application layer establishes the communication link to an upper-level application specific protocol such as the vendor-independent CANopen™ protocol. This protocol is supported by CAN in Automation (CiA), the international users and manufacturers group. Many protocols are dedicated to particular applications, such as industrial automation, diesel engines, or aviation. (Corrigan, 2016)

### 2.2 CAN message and frames

The four different message types, or frames (see Figure 2, CSS Electronics, 2018), that can be transmitted on a CAN bus are the data frame, the remote frame, the error frame, and the overload frame.


Figure 2 CAN bus message

CAN bus frames: (Corrigan, 2016)

The data frame

The data frame is the most common message type, and comprises the arbitration field, the data field, the CRC field, and the acknowledgment field. In Figure 2 the arbitration field contains a 29-bit identifier (or 11-bit identifier) and the RTR bit, which is dominant for data frames. Next is the data field, which contains zero to eight bytes of data, and the CRC field, which contains the 16-bit checksum used for error detection. The acknowledgment field is last.

The remote frame

The intended purpose of the remote frame is to solicit the transmission of data from another node. The remote frame is similar to the data frame, with two important differences. First, this type of message is explicitly marked as a remote frame by a RTR bit in the arbitration field, and second, there is no data.

The error frame

The error frame is a special message that violates the formatting rules of a CAN message. It is transmitted when a node detects an error in a message and causes all other nodes in the network to send an error frame as well. The original transmitter then automatically retransmits the message. An error mechanism in the CAN controller ensures that a node cannot tie up a bus by repeatedly transmitting error frames.

The overload frame

The overload frame is mentioned for completeness. It is similar to the error frame with regard to the format, and it is transmitted by a node that becomes too busy. It is primarily used to provide for an extra delay between messages.

### 2.3 CAN bus arbitration

Arbitration is a mechanism for conflict resolution between network nodes. When the network path is free, any of the nodes in the network can start the message send process. If another node also wishes to send at the same time, the order

of the transmissions is decided using a bitwise arbitration mechanism. During arbitration, both nodes start their transmission. The transmission starts with a start bit, followed by an id field (identifier, CAN-ID). The sending order decision is made based on the value of the id field and the other node or nodes discontinue their transmissions. The messages are sent ordered by priority, where the zero value is dominant. In practice this means that if a node currently sending a bit with a value of one sees that another node is sending a zero bit, it backs off. In other words, it discontinues its own transmission, forfeiting its turn to the node sending the dominating bit. In practice the message with the smallest decimal id value has the highest priority. (Johansson et al., 2005)

From the viewpoint of attacks, this mechanism enables denial of service attacks. As an example, sending large quantities of forged messages having an id value of zero.

### 2.4 CAN bus pros and cons

CAN bus was designed for maximal speed and reliability. At the technical level this mean, among other aspects, that the network communication uses a provider–consumer model instead of the common sender–receiver model. The second feature aiming for performance gains was the lossless bus arbitration described above. (Voss and Comprehensible, 2005)

Improving the reliability of the data transmitted between the nodes was achieved with a mechanism that insures the integrity and timeliness of the messages. These mechanisms are based on bus arbitration, using checksums checking the payload and resending failed messages. (Voss and Comprehensible, 2005)

Based on these design decisions, CAN bus is effectively a broadcast network, where any node can send a message and all nodes are listening to the network and reacting to the messages they are interested in. The only thing the recipients check is the protocol correctness of the received message. (Voss and Comprehensible, 2005)

CAN bus speed is 1 Mbit/sec, which these days does not seem fast. Yet for transmitting short messages and having an effective collision avoidance mechanism, CAN bus is more suitable to be used in real-time applications than connected protocols such as TCP/IP, even if those would be using greater transmission speeds. (Voss and Comprehensible, 2005)

With further development the CAN bus has became a dominant technology for the data transmission of vehicle basic functions. During the last two decades the number of electronic systems in vehicles has increased and at the same time they have become more complex. CAN bus vulnerabilities can be traced back to design decisions described above, the most significant of these being the lack of authentication mechanism. The receiving entity does not have any mechanism to verify the origins of the received message or the validity of the data received. In other words, the control unit does not have a mechanism to detect message forgery. This characteristic makes vehicle CAN busses vulnerable to attacks, such as message forgery, unauthorized data use and denial of service. The DoS vulnerability can be exploited by sending a large number of high priority messages. These attacks can affect the vehicles systems in such a way as to cause loss of control, incorrect functionality, premature wear or rendering the vehicle unable to function at all. (Carsten et al., 2015)

### 2.5 Attack surfaces

The taxonomy of CAN bus attack surfaces is usually divided into two parts: remote exploits and exploits requiring physical access to the CAN bus. In addition to this, some researchers have expanded the use of physical connections by constructing experiments that enable man-in-the-middle type of attacks on the CAN bus (Lebrun and Demay, 2016).

Physical connection to a CAN bus is not technically complex to achieve. The simplest physical connection can be implemented through the vehicle's diagnostics port. This approach does not require any alterations to the vehicle in question. The limitation of this approach is the amount of network data observable at this point of entry, depending heavily on the make and model of the vehicle. CAN bus traffic seen through the diagnostic port is restricted by segmenting the network. These limitations can be avoided by choosing another point of entry from the desired segment. In most cases this approach requires alterations to the vehicle's wiring harnesses, because segment-specific connectors are rarely implemented in production vehicles.

Remotely exploitable attack surfaces that would have a direct effect on the vehicle's physical functionalities are usually more challenging to exploit. In practice, this normally means a multistage attack where the attacker first has to find a vulnerable and remotely accessible service to gain a foothold. As an example, this kind of service can be found from the vehicle telemetry or infotainment systems. After gaining a foothold on one of the connected systems, the attacker needs to find a way to gain access to another system that has connectivity to the more critical segments of the vehicle's CAN bus. This type of attack has been successfully conducted by some vehicle security researchers (see Miller and Valasek, 2013).

## 3. The AaTi study

### 3.1 Previous research

Wolf et al. (2004) found that vehicle networks are open and for this reason vulnerable on many levels. The attacker can exploit vehicle wireless connections and networks. Wolf et al. (2007) continued their work in an article where they were attempting to form a full picture of the current situation of automotive electronic systems. This article listed commonly used automotive systems and their properties, including details about communication and cryptography.

The possibility of cyber-attacks as a subject of scientific articles became more prevalent around a decade ago. At that time, the articles started to touch on the subject of, among other things, how to protect vehicles for possible attacks (Larson et al., 2008).

A research group consisting of researchers from the University of Washington and the University of California, San Diego conducted a system security analysis through experiments on a passenger vehicle. This article was aiming for a comprehensive security analysis of a vehicle system rather than an analysis of individual devices. The article also proposed a part threat model that identified the physical connection and wireless functionalities as individual attack vectors. (Koscher et al., 2010) This group continued their

work the next year by publishing an article, focusing on a broader analysis of the vehicle attack surfaces. (Checkoway et al., 2011)

Vehicle cyber security research was brought to more common knowledge by Valasek and Miller, who published their first article on this subject in 2013. In this article they examined two vehicles from different manufacturers and got results on how vehicle functionality can be affected that were similar to what previous academic research efforts had shown. In addition to their results, they published most of the reverse engineered CAN messages they discovered, and the source code of the tools used in their research. The additional information was published to encourage other groups to conduct similar research in the future (Miller and Valasek, 2013). Miller and Valasek (2015) continued their work and published an article that describes in detail how an unaltered vehicle can be taken into partial control without a physical connection. As a point of entry to the vehicle system they used a security flaw in the infotainment system of the vehicle in question.

### 3.2 Analysis methods

#### 3.2.1 Introduction to the analysis methods used in this research

The anomaly detection methods proposed in previous academic articles can be divided into groups using several different taxonomies. The first example of such a taxonomy is dividing the methods based on the use of system specification. When system specification is available, detecting anomalies is based on detecting traffic that does not fit the given specification. This type of approach has been suggested in the method used by Larson et al. (2008), where anomaly detection is delegated to the network nodes. The nodes then inspect the traffic and sound an alarm if they see some else sending a message type only they are supposed to send. The second category of systems assumes that system and message specifications are present. In these systems the anomaly detection is based on features such as message timing, data semantics, entropy, repeating message sequences, protocol correctness and signal characteristics differing from normal network traffic.

Anomaly detection methods can also be grouped according to their method of detection. The majority of normal CAN bus traffic is cyclic by nature. This means that a series of messages repeat cyclically after very predictable intervals. Based on this property many proposed methods use message timing as a basis for anomaly detection. Time-based detection methods can also be divided into two main groups: those that measure message frequency and those that measure interval. Methods that fall into the first group have been proposed by Hoppe et al. (2008-2009), Münter et al. (2010) and Miller and Valasek (2014). Miller and Valasek (2014) proposed a substantial rise in the frequency of sent messages for a detection method. Taylor et al. (2015) proposed a more advanced method where the frequency monitoring is based on Hamming distance.

However, methods based on message frequency have their weaknesses. For example, when only message frequency is monitored short-term anomalies are not necessarily detected. However, if instead of frequency the detection method is based on message intervals, even short-term changes in network traffic can be detected more accurately. The use of interval analysis has been proposed by Son et al. (2016) and Moore et al. (2017). The latter article proposes a method based on absolute time deviation.

Several methods based on correctness of data carried by the messages have been proposed. Hoppe et al. (2008) described a method where only gross abuse of messages is detected. They continued their work in 2009 by proposing a method where consecutive messages are monitored for semantic correctness.

Münter and Asaj (2011) described a method based on data entropy, where changes in entropy are detected on the binary level. In addition, their method monitored communication entropy in protocol and signal levels.

Methods based on monitoring repeating message sequences in a specified time window has been proposed in several articles. Narayanan et al. (2015) based their method on a hidden Markov model and Marchetti et al. (2017) observed the order and changes in repeating messages.

The AaTi project used a test vehicle (Toyota Prius Hybrid). The data used in the study was first recorded from a test vehicle. It could then be inspected in laboratory environment. The vehicle-specific CAN bus interference messages were first generated under laboratory conditions and then verified on a test vehicle. The first goal of AaTI study was the ability to distinguish between normal and abnormal network traffic in real-time using recorded samples from a vehicle. In this research, a system of message specifications was not used, so anomaly detection of data payloads proposed a challenge. Mainly for this reason most of the methods that were researched were time based. This has also been the primary approach for previous research.

The only method during this research that was based on anomaly detection in data payloads was a neural network that could learn to predict incoming message payloads based on previous data it had inspected.

#### 3.2.2 Neural network

For inspecting message data payloads, a neural network was built based the method presented in Taylor et al. (2016). In this method the neural network builds a model based on normal data traffic by inspecting network traffic. The method described in the article has produced promising results. Different metrics for identifying and measuring deviations in the data streams have also been proposed in multiple articles (e.g., Taylor et al., 2015).

The Long Short-Term Memory (LSTM) network architecture used in this research consisted of layers of nodes with an adjustable feedback loop. This architecture enables the network to have a “memory” as well as the ability to “forget”. The majority of data in CAN bus traffic is regular by nature, in other words the data changes gradually and follows distinct trends. Therefore, predicting should be viable for at least some parts of the network traffic. In the experimental design the neural network was constructed to predict the data bits of an incoming message based on data bits of previously observed messages.

The biggest problems using the described neural network was its resource demand and probable difficulties in making the predictions more accurate. In addition, reasonable accuracy can only be achieved in regular dataflows, so some parts of the CAN bus traffic cannot be inspected using this method.

#### 3.2.3 Kernel density estimation

The first method implemented for interval analysis was kernel density estimation. This method can model interval distribution characteristics for each message identifier. The distribution characteristics can then be compared to incoming message distribution to detect anomalies.

Modeled distribution gives the intervals a density function that can be used to calculate reliability values for new messages. If the calculated reliability drops too low, the situation is declared an anomaly and an alarm can be given.

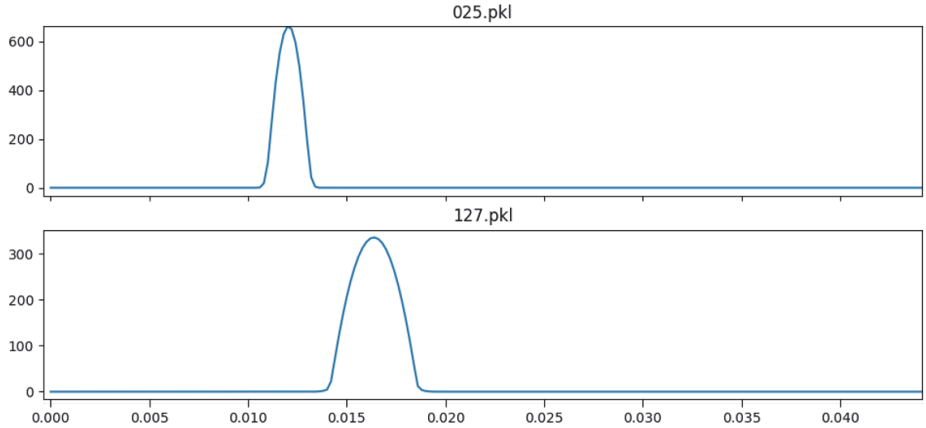



Figure 3 Arrival interval distributions of two different message identifiers.

Figure 3 shows arrival interval distributions for two message identifiers that have been modeled using kernel density estimation. In the first graph, the interval deviates between 10 and 15 milliseconds. In the second graph, it deviates between 15 and 20. If incoming traffic shows interval deviations to be different than the peaks showed in the graphs, an indication of anomalous traffic can be given.

The advantage of kernel density estimation is that it can model systems that implement different sending speeds. For example, an engine control unit can send messages with different intervals when the engine is in idle or when the vehicle is moving. This kind of situation would show in the model as two distinct peaks. However, this kind of behavior was not observed in the test vehicle used in the study.

### 3.2.4 One-class support vector machine

One-class support vector machine (OCSVM) is a variation of a support vector machine, which is a popular machine learning method for classification. However, a normal support vector machine requires examples of each class that it should identify. An OCVSM, on the other hand, classifies the elements into two categories: normal and abnormal. This means examples of normal behavior are sufficient and it does not require examples of abnormal behavior. The method defines a boundary around normal behavior and classifies all messages outside this boundary as abnormal.

Therefore, a one-class support vector machine is fit for detecting abnormal behavior, because it is challenging to find examples of all possible abnormal behaviors for training. Examples of normal behavior, on the other hand, are in most cases easily available. Normal data sets were recorded from test vehicle.

Taylor et al. (2015) presented an application of OCVSM, and the AaTi study implemented a variant of this machine. A moving window containing a set number of messages was used as a data element. From the data elements the characteristics were calculated that could be used to define the whole inspected window as either normal or abnormal. Characteristics calculation was based on mean interval and standard deviation of the messages within a window.

### 3.2.5 Absolute deviation

Because the kernel density estimation method described above (see 3.2.3) is resource intensive and no multiple peaks were observed in the gathered data, a decision was made to implement a simplified method using the same principles. This method attempted to model the interval deviation for each message identifier, which would give considerable gains in performance and, at the same time, maintain similar performance for detection.

A decision was made to model the intervals with a normal deviation, because this made it possible to describe the deviation using only mean and standard deviation values. In the training phase it was also decided to include upper and lower bound values for each message identifier for classification. The distinct upper and lower bound values were added because positive deviations were more common in the normal network traffic, possibly due to message collisions. In addition, doing these calculations in the training phase made the classification faster. The boundary values were chosen so that no deviations were classified from the training data and a small marginal was added.

Again, a moving window was used for data-element as in the one-class support vector case. The messages in the window were classified based on its average interval. If this value was smaller than the lower bound or greater than the upper bound value then the traffic within the window in question was defined as abnormal.

An almost identical sensor was implemented in an article by Moore et al. (2017). The difference being that they did not use a moving window as a data element (Müter et al., 2010). An alert caused by a single abnormal message would produce too many false positives, so in the implementation described in the article only three consecutive abnormalities will trigger an alarm. In testing this method showed similar performance with other methods tested and it was less resource intensive. A decision was made to do a proof of concept implementation of this method.

### 3.2.6 Categorization

Based on the previously described methods, it was observed that most false positives originate from control units that send their messages in irregular intervals. For this reason, the possibility of categorizing the messages by their send profiles was examined. Some of the control units send messages at regular intervals and others send irregular messages of events between regular status messages. A simple absolute deviation detection would categorize these messages as abnormal and initiate an alarm.

Based on the observations made during the research. It would be possible to reduce the number of false positives using categorization. But the number of send profiles would pose challenges for an implementation of such a categorization method. In addition, some messages that have the same message identifier can use multiple send profiles. In addition to these two drawbacks, there is uncertainty over what kind of send profiles exist in addition to the ones observed.

### 3.2.7 Method comparison

Time-based methods were compared by drawing a receiver operating characteristic (ROC) curve for each individual method using the same data recorder from a vehicle CAN bus that included a test attack. All methods used the same window size of five messages per window so that comparability could be maintained. All methods were given a setting that if they detected even one message that was part of the attack, they should mark the whole window as abnormal.

The best threshold value in Figure 4 shows the threshold value for which the best accuracy without any false positives was achieved. The number of true positives is shown in parentheses labeled “TPR” (True Positive Rate). The main interest in this figure should be the threshold value, since a practical real-time sensor would require a minimal number of false positives.

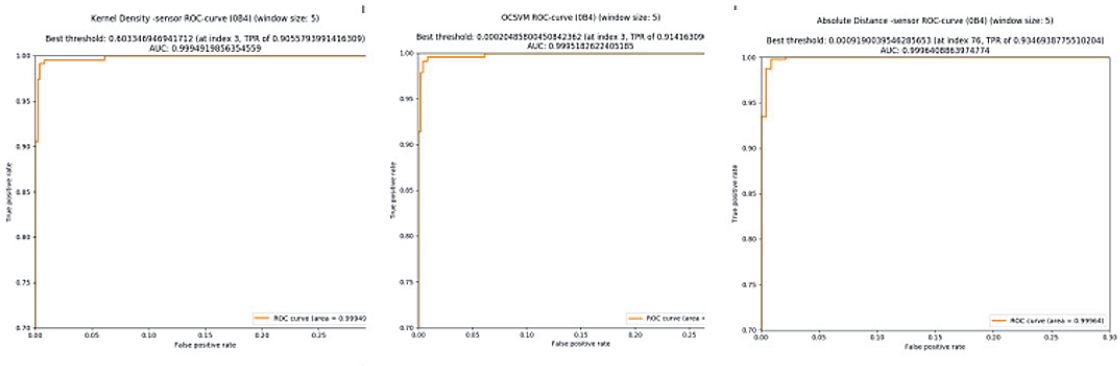


Figure 4. ROC graph (Vertical axis: true positive rate and horizontal axis: false positive rate).

Figure 4 left, kernel density estimation method; best achieved TPR without false positives: 0.9056. Figure 4 middle, OCSVM; best achieved TPR without false positives: 0.9142. Figure 4 right, absolute deviation method; best achieved TPR without false positives: 0.9347.

The comparison shows the analysis of a single message identifier attacked during the data recording. The results suggest that the performance of the methods shown is similar. At least with the test data ware used in the comparison. The absolute deviation, which is also the simplest method, achieved the most accurate results, maintaining a zero false positive rate.

Based on the observations, the methods described above show that most false positives originate from electronic controller units with irregular send profiles. Message send profile categorization could be used to improve the result in these cases, but it has its drawbacks, as described in section 3.2.6.

## 4. Conclusions

The focus of the AaTi study was to survey anomaly detection methods applicable to vehicle networks. This research complements previous research and patents by understanding network-traffic characteristics using recordings obtained from a test vehicle. The study shows that attacks against vehicle networks can be categorized into three groups. The network can be injected (a) with special messages such as diagnostics messages; (b) with normal messages that disturb vehicle functionality or (c) by sending normal messages after the real sender has been rendered unfunctional. The most common situation is probably when the real sender is still functional, and the attacker sends normal CAN messages. These kinds of attacks can be detected by observing message send intervals, since in a normal situation the intervals should remain regular.

In the first phase of research a neural network implementation was tested for its ability to detect abnormalities in message data payloads. The aim of this implementation was to provide technical means to learn different payload possibilities and predict the data incoming in the following messages. This would have created the possibility to detect abnormal data payloads. The problem with using neural networks arose from its resource intensiveness and lack of prediction accuracy. The next experiments focused on anomality detection methods based on message timing.

The first time-based method we tested was One-Class Support Vector Machine (OCSVM), which is a variation of the popular machine learning method. This method defines boundaries around normal behavior and classifies all other traffic as abnormal. In the implementation, a moving window with a set number of messages was used as a data-entity. The characteristics of the messages are then calculated using OCSVM and, based on the results, the whole window is declared normal or abnormal. The characteristics used in this implementation were average interval and standard deviation.

After this fist experiment, other methods based on message interval were surveyed. Kernel density estimation models interval deviation for each message identifier. This value can then be compared to incoming messages in order to detect abnormalities. Modeled deviation provides a density function for the interval that can be used for likelihood value calculation for incoming messages. A drop in the calculated likelihood that exceeds a predetermined threshold can be detected as an anomaly and an alarm can be triggered. Because kernel density estimation is also a resource-intensive method and the observed test data did not show multipeak properties, a simplified version using the same principles of this method was implemented. This method aims to model message identifier deviation using key values. This implementation of absolute deviation achieves substantial gains in resource efficiency and without decline in the performance of the detection properties. The modeling was done using standard deviation in order to use the two key values: average and standard deviation. In the practical implementation training phase average, lower and upper bound values were calculated for each message identifier for classification purposes. A moving window was used as a data entity. If the values within the window went below

the lower bound or exceed the upper bound, the whole window is declared an anomaly in the network traffic.

All of the above mentioned methods have their own challenges in either resource intensiveness, accompanied in some cases with inaccuracy of predictions.

Based on the experience described in the method comparison chapter, a novel method for detecting CAN bus anomalies based on message arrival intervals was developed and a patent application for this method has been filed. The description of this method is part of the patent. The functionality of this method was verified in a computational environment.

As different digital platforms become ever more common in automated processes, the protection of different processes and the cyber security of the infrastructure is going to play a significant role in the overall safety of these platforms. For future researchers in this field, the group would like to recommend the usage of outcomes found in the AaTi study as well as the utilization of the patented method as a part of future CAN bus implementations in order to improve cyber security.

**References**


Alanen J. (2000). CAN ajoneuvojen ja koneiden sisäinen paikallisväylä. Tampere: VTT Automaatio, koneautomaatio.

Carsten P., Yampolskiy M., Andel T.R. and McDonald J.F. (2015). In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions. CISR '15 Proceedings of the 10th Annual Cyber and Information Security Research Conference (apr 2015), 477–482

Checkoway S., McCoy D., Anderson D., Kantor B., Savage S., Koscher K., Czeskis A., Roesner F. and Kohno K. (2011). Comprehensive Experimental Analysis of Automotive Attack Surfaces, in Proceedings of the USENIX Security Symposium, San Francisco, CA.

Corrigan S. (2016). Introduction to the Controller Area Network (CAN). Texas Instruments. http://www.ti.com/lit/an/sloa101b/sloa101b.pdf

CSS Electronics (2018). A Simple Intro to CAN Bus. https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en

Finnish Meteorological Institute, (2017). Intelligent Transport. https://ilmatieteenlaitos.fi/alykas-liikenne

Hoppe T., Kiltz S. and Dittmann J. (2008). Security threats to automotive CAN networks - practical examples and selected short-term countermeasures. In SAFECOMP.

Hoppe T., Kiltz S. and Dittmann J. (2009). "Applying Intrusion Detection to Automotive It-Early Insights and Remaining Challenges." Journal of Information Assurance and Security (JIAS) 4 (6): 226–235.

Johansson K. H., Törngren M. and Nielsen L. (2005), Vehicle applications of controller area network, in Handbook of Networked and Embedded Control Systems, William S. Levine Dmiitris Hristu-Varsakelis, and,ed., Birkhauser.

Koscher K., Czeskis A., Roesner F., Patel S., Kohno T., Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H. and Savage S. (2010). Experimental security analysis of a modern automobile. In D. Evans and G. Vigna, editors, IEEE Symposium on Security and Privacy. IEEE Computer Society.

Larson, U. E., Nilsson D. K. and Jonsson E. (2008). "An Approach to Specification-Based Attack Detection for in-Vehicle Networks." In 2008 IEEE Intelligent Vehicles Symposium, 220–25. doi:10.1109/IVS.2008.4621263.

Lebrun A. and Demay J. C. (2016). Canspy: a platform for auditing can

devices. https://www.blackhat.com/docs/us-16/materials/us-16-Demay-CANSPY-A-Platorm-For-Auditing-CAN-Devices.pdf.

Marchetti M. and Stabili D. (2017). "Anomaly detection of can bus messages through analysis of id sequences," in 28th IEEE Intelligent Vehicle Symposium (IV2017).

Miller C. and Valasek C. (2013). Adventures in automotive networks and control units, DEFCON 21, Las Vegas, NV.

Miller C. and Valasek C. (2014). A survey of remote automotive attack surfaces, BlackHat USA.

Miller C. and Valasek C. (2015). Remote exploitation of an unaltered passenger vehicle, Black Hat USA.

Moore M. R., Bridges R. A., Combs F. L., Starr M. S. and Prowell S. J. (2017). “Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks,” in 12th CISRC. ACM.

Müter M., Groll A. and Freiling F. C. (2010). “A Structured Approach to Anomaly Detection for in-Vehicle Networks.” In 2010 Sixth International Conference on Information Assurance and Security (IAS), 92–98. doi:10.1109/ISIAS.2010.5604050.

Müter M. and Asaj N. (2011). "Entropy-based anomaly detection for in-vehicle networks." IEEE IVS.

Narayanan S. N., Mittal S. and Joshi A. (2015). “Using Data Analytics to Detect Anomalous States in Vehicles.” arXiv Preprint arXiv:1512.08048. http://arxiv.org/abs/1512.08048.

Song H. M., Kim H. R. and Kim H. K. (2016). "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in 2016 International Conference on Information Networking (ICOIN), pp. 63-68

Taylor A., Japkowicz N. and Leblanc S. (2015). “Frequency-Based anomaly detection for the automotive CAN bus,” in Proc. of WCICSS, 2015, pp. 45–49.

Taylor A., Leblanc S. and Japkowicz N. (2016). “Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks”. IEEE DSAA (2016).

Voss W, and Comprehensible A. (2005). Guide to Controller Area Network. Massachusetts, USA: Copperhill Media Corporation.

www.br-automation.com

Wolf M., Weimerskirch A. and Paar C. (2004). Security in automotive bus systems. In Proceedings of the Workshop on Embedded Security in Cars 2004.

Wolf M., Weimerskirch A. and Wollinger T. (2007). State of the art: Embedding security in vehicles. EURASIP Journal on Embedded Systems.

**Artikkeli P4:**



# Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organization

2019
Jouni Pöyhönen, University of Jyväskylä, Jyväskylä Finland,
Viivi Nuojua, University of Jyväskylä, Jyväskylä Finland,
Jyri Rajamäki, Laurea University of Applied Sciences, Espoo, Finland
Martti Lehto, University of Jyväskylä, Jyväskylä, Finland

Originally published in book Information & Security: An International Journal, Digital Transformation, Cyber Security and Resilience, Edited by Todor Tagarev, Volume 43, 2019, pages 236-255
DIGILIENCE 2019 conference, 2 - 4 October 2019, Sofia, Bulgaria

# Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations

Jouni Pöyhönen[1], Viivi Nuojua[1], Jyri Rajamäki[1,2], Martti Lehto[1]
[1]University of Jyväskylä, Jyväskylä, Finland
[2]Laurea University of Applied Sciences, Espoo, Finland
jouni.a.poyhonen@jyu.fi
viivi.nuojua@jyu.fi
jyri.rajamaki@laurea.fi
martti.j.lehto@jyu.fi

**Abstract**

Cybersecurity-related capabilities play an ever-growing role in national security, as well as securing the functions vital to society. The national cyber capability includes the resilience of companies running critical infrastructures, their cyber situational awareness (SA) and the sharing of cybersecurity information required for cyber SA. As critical infrastructures become more complex and interdependent, ramifications of incidents multiply. The EU Network and Information Security Directive calls for cybersecurity collaboration between EU member states regarding critical infrastructures and places the most crucial service providers and digital service providers under security-related obligations. Developing better SA requires information sharing between the different interest groups and enhances the preparation for and management of incidents. The arrangement is based on drawing correct situation-specific conclusions and, when needed, on sharing critical knowledge in the cyber networks. The target state is achieved with an efficient process that includes a three-level—strategic, operational and technical/tactical—operating model to support decision-making by utilizing national and international strengths. In the dynamic cyber environment strategic agility and speed are needed to prepare for incidents.

Keywords: cybersecurity, situational awareness, information sharing, critical infrastructure, vital societal functions

## Introduction

The capability related to national cybersecurity plays an even more important role when it comes to the overall security and securing the crucial functions of society in the future. The national capability consists of most of the resilience of the critical infrastructure companies and the situational awareness of the cyber environment, they constantly maintain.

The critical infrastructures become more complex and their parts are even more strongly dependent on each other, and that way, the ramifications of the incidents can be multiple compared with the original impact. The operation of critical infrastructure and the threats having an impact on them are not limited to organizations or administrative borders. [18]

The EU Network and Information Security (NIS) Directive [4] increases the collaboration between the member states in the important field of cybersecurity. It puts the most crucial service providers (critical industries such as energy, transport, health, and financing) and digital service providers (online marketplaces, search engines, and cloud computing) of society under the security-related obligations. The application of the Directive

results in imposing the security and information requirements concerning the aforementioned operators. The goal is to develop even better situational awareness and information sharing. The critical infrastructure consists especially of the crucial service providers defined by the NIS Directive. In Finland, the administrative sector coordinates the operations required by the Directive, when both monitoring and the duty to notify are decentralized. The National Cyber Security Centre Finland builds situational awareness.

Principally, the functional observation and analysing ability collected from the different trust circles gives a good basis for the development of Finland's national situational awareness, and information sharing. [9] Critical infrastructure can be described as a three-levelled system of systems (Fig. 1); efficient and appropriate operations can be targeted at its three levels, from bottom to the top: power grid, data transmission network, and services. [14]

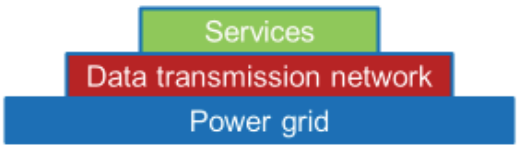



Figure 1: Plain structure of critical infrastructure.

The situational awareness of critical infrastructure is emphasized also in the Security Strategy for Society, [16] as part of maintaining vital national operations. Efficient incident management requires tight collaboration between the management, situation awareness and communication. Good management requires:

- unquestionable managerial responsibility, the casting of different operators and the decision-making ability of the ministerial authority
- building of situation awareness (situational understanding, evaluation of situational development)
- crisis communication
- information sharing, and supporting technical solutions
- business continuity management
- co-operation.

**Research purpose, research questions and article structure**

The research questions deal with the situational awareness and understanding of an organization, as well as the data analysis and information sharing between the different interest groups. The aim is to develop the preparation for incidents and their management in the whole society. The arrangement is based on drawing correct situation-specific conclusions and, when needed, on sharing critical knowledge in the cyber networks of society. The research questions are:

1. How the cyber situational awareness of an organization can be developed?
2. How do the organizations exchange their cybersecurity-related information?
3. Can an organization's cybersecurity capability be utilised more extensively?

This paper is a continuum of the research "Cyber strategic management in Finland," [10] in which one task was to formulate management proposals for the management of nationally pervasive incidents concerning cyber environment. Good situational awareness and information sharing between the different interest groups have an essential impact on incident management. The research method was an open theme interview with material-

based content analysis. All three levels of the critical infrastructure system of systems (see Figure 1) were represented. There were altogether 40 interviewees from 25 private or public organizations, which were leaders or persons responsible for the information/ cybersecurity of their organizations.

In Finland, the significance of the private businesses is emphasised in the operation of critical infrastructure, since approximately 80 % of the operations can be estimated to belong to their responsibility. Researchers interviewed six private businesses, as well as public authorities, such as the National Cyber Security Centre Finland and the National Emergency Supply Agency.

Section 2 deals with the need for situational awareness, and related decisionmaking levels and the theory of situational awareness. In Section 3, the information sharing needs of an organization are explored, ever since the national and European Union needs. Section 4 describes the formation of situational awareness into the different levels of an organization, and the information-sharing procedures at the national level. Finally, Section 5 concludes with the conclusion.

**Situational awareness**

To function, every organization needs information about its environment and happenings, and also about its impact on its operation. An appropriate and fast situational awareness is based on correct information and evaluations, and it is emphasized in the case of incidents when very pervasive decisions must be made quickly. To make correct solutions, decision-makers have to know the base for their decisions, consequences how the others react to them and what risks the decisions include. For that reason, decision-makers must have sufficient situational awareness and understanding of all the operational levels, which enables timely decision-making and operation. Situational awareness and understanding require collaboration and expertise, which enables the comprehensive monitoring of the operational environment, data analysis, and aggregation, information sharing, recognition of the research needs and network management. The information systems must enable the systematic use of information sources and collaboration and the flexible sharing of situation information related to it.[11]

The organizations' and decision-makers' formation of situational awareness is supported by the situation awareness arrangements. In general, situation awareness means the description of the dominant circumstances and the operational preparedness of different operators aggregated by the specialists, the happenings caused by an incident, its background information and the evaluations concerning the development of a situation. In addition, data analysis based operational recommendations may be related to situation awareness. The general view is constituted by utilizing a networked operational model based on different sources. The process consists of data acquisition, information aggregation, classification and analysis, and of a timely and efficient sharing of the analysed information with those in need. The surrounding data space is organised such that the information is understood correctly, and that the operators have a chance to get the information important to their operation.[11]

The pervasive incidents targeting society are a challenging cyber environment when it comes to the critical reaction speed required by the situation management. Advanced Persistent Threats (APT) are unfamiliar attacks to the traditional protection ways and can proceed quickly when fast information sharing and good situational awareness play an important role in incident management. In a worstcase scenario, the delegation of responsibility should be able to make possible in a few minutes, the response evoked without delay, and the abilities and tools put to use.[12]

### Decision-making levels

Organizations operate in very complex, interrelated cyber environments, in which the new and long used information technology system entities (e.g. a system of systems) are utilized. Organizations are depended on these systems and their apparatus to accomplish their missions. The management must recognize that clear, rational and risk-based decision are necessary for business continuity. The risk management at best combines the best collective risk assessments of the organization's individuals and different groups related to strategic planning, and also the operative and daily business management. The understanding and dealing of risks are an organization's strategic capabilities and key tasks when organizing the operations. This requires, for example, the continuous recognition and understanding of the security risks on the different levels of the management. The security risks may be targeted not only at the organization's operation but also at individuals, other organizations and the whole society.[8]

Joint Task Force Transformation Initiative recommends implementing the organization's cyber risk management as a comprehensive operation, in which the risks are dealt with from the strategic to tactical level.8 That way, risk-based decision-making is integrated into all parts of an organization. In Joint Task Force Transformation Initiative's research, the follow-up operations of the risks are emphasised in every decision-making level. For example, in the tactical level, the follow-up operations may include constant threat evaluations about how the changes in an area can affect the strategic and operational levels. The operational level's follow-up operations, in turn, may contain for example the analysis of the new or present technologies to recognize the risks to the business continuity. The follow-up operations of the strategic level can often concentrate on the organization's information system entities, the standardization of the operation and for example on the continuous monitoring of the security operation.[8]

From the necessity of the organization's risk, follow-up operations can be drawn the necessity of the whole organization's situational awareness. As mentioned, the formation of the organizations' and decision-makers'situational awareness is supported by the situation awareness arrangements. Thus, an appropriate situational awareness supports cyber risk management and more extensively the evaluation of the organization's whole cyber capability.

### Theory of situational awareness

Mica Endsley has developed a situational awareness model when working on several different research assignments in the service of the United States Air Force.[3] Figure 2 describes the general structure of the model. The core of situational awareness consists of three basic elements: detection (Level 1), situational understanding (Level 2) and its impact assessment towards the future (Level 3). This situational awareness provides the foundation for conclusions and the following decision-making. Depending on the situation, the assignment- and system-specific features and the decision-maker's experience and evaluation ability bring their impacts on the table. Decision-making, in turn, guides the operation that reflects the observed operational environment.

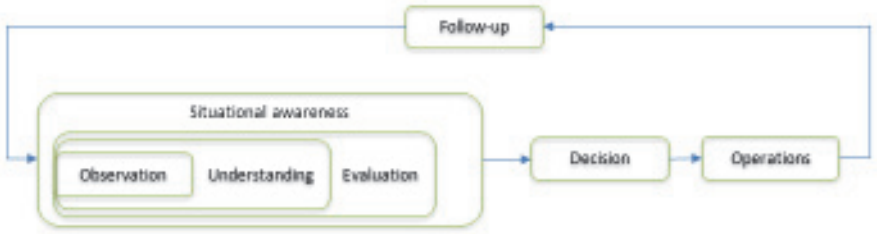



**Figure. 2:** Situational awareness and dynamic decision-making (adapted from Endsley [3]).

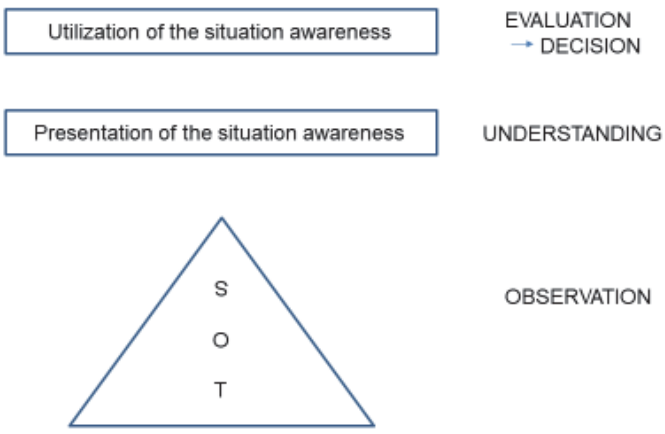



**Figure 3:** Framework for forming situational awareness.

Sid Faber regards the situational awareness development operations, concerning both public and private businesses, as one of the most significant near-future goals aiming to improve cybersecurity.[5] He recommends applying Endsley's model to the follow-up needs of a cyber-operational environment.

The general structure of Endsley's situational awareness model is applied when solving our research questions.[3] The framework for forming the critical infrastructure situational awareness is introduced in Figure 3. The detection part (Level 1) of Endsley's structure is presented as the organization-specific detection needs of the strategic (S), operational (O) and technical/tactical (T) decision-making levels. The goal is to gain a perception that serves each decision-making level. The situation awareness that is formed of observations is a prerequisite for understanding the observations (Level 2). After that, the impact analysis and assessment of the observations are made possible by utilizing the understanding about situation awareness (Level 3). There, analysis capability plays an important role. The final goal is to make appropriate and situation-specific decisions on each decision-making level and conduct the operations followed by the decisions.

### General requirements of situation awareness

Horsmanheimo and co-workers set some requirements for the situation awareness in their research:[6]

- Situation awareness is a series of presentations whose shape does not matter. It is more essential than somebody manages it, makes analysis and decisions.

- Information is brought to the situation awareness system in collaboration. Every operator is independently responsible for the production and validity of the information related to their knowledge area.
- The information must be processed, analysed and understandable. It has to be meaningful for both oneself and other receivers.
- The information must be performed visually and clearly.
- The information must be performed without unnecessary technical details. The information must be understandable for people from other industries.
- Situation awareness system should be dynamic and tailored by users and industries. Information should be able to put on different views.
- Terminology and classifications should be uniform.
- Situation awareness system should be able to be included in the organization processes such that the maintenance of the situation awareness system would not become an extra task in grand incidents.
- Different operators should be able to define what kind of information they need and what kind of information they can input to the system.
- Situation awareness system should be able to be utilised for information exchange between different operators on different organization levels. Information should be able to be shared also with the supervisory organizations.
- The situational awareness system should be able to make predictions of what is happening by 3, 6 or 12 hours.
- The situational awareness system should be able to perform a temporal dimension to how the things have developed – whether the direction is worse or better.

**Information sharing needs of an organization**

The EU Network and Information Security (NIS) Directive increases the collaboration between the member states in the important field of cybersecurity. It puts the most crucial service providers (critical industries such as energy, transport, health, and financing) and digital service providers (online marketplaces, search engines, and cloud computing) of society under the security-related obligations. The application of the Directive results in imposing the security and information requirements concerning the aforementioned operators. Also, the Directive supports in developing nationally better situational awareness.

The operations of the concerned Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 have been carried out nationally since 2018. The Directive states the subject matter and scopes the following: [4]

1. This Directive lays down measures to achieve a high common level of security of network and information systems within the Union to improve the functioning of the internal market.
2. To that end, this Directive: a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems; b) creates a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among the Member States and to develop trust and confidence amongst them; c) creates a computer security incident response teams network (‘CSIRTs network') to contribute to the development of trust and confidence between the Member States and to promote swift and effective operational cooperation; d) establishes security and notification requirements for operators of essential services and digital service providers; e) lays down obligations for the Member States to designate national competent authorities,

single points of contact and CSIRTs with tasks related to the security of network and information systems.

Principally, a functioning observation and analysing ability composed from different trust circles provides a good starting point for the development of Finland's national situational awareness. 9 By the most crucial service providers' and digital service providers' duty to notify, the national situational awareness can be developed. The duty to notify expands the previous procedure considerably and therefore covers a significant part of the critical infrastructure by private businesses. Also, the operation involves information sharing between the authorities, and more than before between the authorities and private business operators. In Finland, the operations required by the Directive relate to sector-specific laws and, consequently, their monitoring as well as the duty to notify happen sector-specific. The laws include the definitions of the crucial service providers' duty to notify. The situational awareness is built by the National Cyber Security Centre Finland.

**The National Cyber Security Centre Finland**

The National Cyber Security Centre Finland (NCSC-FI) is part of the Finnish Transport and Communication Agency, Traficom. Traficom is an authority in a permit, license, registration, and monitoring of transport and communication. It promotes traffic safety and the smooth functioning of the transport system and speeds up the development of digital society. Also, the agency supports sustainable development and ensures that everyone in Finland has access to high-quality and secure communications connections and services.[17]

Nationally, the NCSC-FI plays the most crucial part in forming and analysing the cyber situational awareness, and in incident management. It has three main tasks:

1. The NCSC-FI acts as a national communications security authority (NCSA) and is responsible for the security matters related to the electrical data transmission and processing of the safety-classified material. The NCSA operation is part of Finland's security authority organization.
2. The CERT (Computer Emergency Response Team) operation of the NCSC-FI takes care of the prevention, investigation and announcement tasks in case of information security breaches. The main purpose of the CERT operation is to produce and maintain the cyber situation awareness together with domestic and foreign cooperation partners and counterparts. As an essential part of the CERT operation, the NCSC-FI acts as a national point of contact for information security breaches and threats. It also investigates these cases and helps the concerned parties.
3. The NCSC-FI manages the information security regulation tasks of Traficom. It acts as a national regulatory authority (NRA), i.e. as a guiding and monitoring authority.

The NCSC-FI is an authority that aggregates and builds national situational awareness. It collaborates closely with other authorities and private business operators.

HAVARO is a service that detects and warns about information security breaches, serves the critical companies for security of supply and the state administration. From the HAVARO system, the NCSC-FI has visibility to practically all the upcoming and outgoing traffic (metadata and content data). Many critical companies for security of supply and the state administration operators have put to use the HAVARO service, which indicates the trust in the NCSC-FI. That way, the information security breaches targeted at the organization can be reported automatically to the authority without a chance for censoring the incidents beforehand. The system has been implemented in collaboration with the National Emergency Supply Agency.

The companies and public administration operators participate in the HAVARO operation voluntarily. The operation of the system is based on the information security threat identifiers coming from different sources. With the help of the identifiers, harmful or anomalous traffic can be detected from the organization's network traffic. The NCSC-FI receives information about the anomalies and analyses them. In case of an information security threat, the organization is warned about it. Based on the information got from the HAVARO, also the other operators can be warned about the detected threat. That way, the system helps not only individual organizations but also in forming a general view about the information security threats against Finnish information networks.

The observation ability of information security threats is an important part of comprehensive risk management. For its part, HAVARO secures the organization's business continuity against the threats of the operational environment. However, HAVARO is not meant to be an organization's only information security solution, but it is designed to complete the other information security solutions of information security investing organization.

Also, Traficom provides the GovHAVARO service for the state administration operators. It completes the information and cybersecurity threat detection of the state administration's Internet traffic. The service providers are Traficom, Valtori – Government ICT Centre and Telia. The GovCERT services, in turn, support the state's round-the-clock information security operation by producing the support services for preventing, detecting and investigating information security breaches, as part of the GovSOC operation. They are provided by Traficom and Valtori.[7]

The incident management of the state administration and other public administration organizations, so-called VIRT operation, is a cross-administrative operational level collaboration, which prepares for severe and extensive information security incidents. It consists of operational planning and rehearsing for different information security incidents.[7]

The industry-specific cyber information-sharing groups (ISAC, Information Sharing and Analysis Centre) are established as collaboration organs between the organizations of different industries. Their operation enables:

1. Confidential handling of information security matters between the participants.
2. Augmentation of the organizations' information security know-how.
3. Development of the NCSC-FI's overall situational awareness. The ISAC operation is based on regular meetings and specified operational models and participants.

The ISAC information sharing groups have been established for the following industries: state administration (VIRT), Internet service providers, chemistry and lumber industry, banks, media, energy industry, food production and distribution, social and health care, and software manufacturers.

**The National Emergency Supply Agency**

The National Emergency Supply Agency (NESA) is an institution working under the Ministry of Economic Affairs and Employment of Finland. It is tasked with planning and operations related to maintaining and developing the country’s security of supply. As part of the security of supply organization, the NESA’s mission is to support the operation of the pools and sectors and to take care of the other legislative tasks given to it. Security of supply means the ability to maintain such economical basic operations of society that are necessary for securing the populations' living prospects, society's functioning and safety, and the material prerequisite for national defence in severe incidents and extraordinary circumstances.[13]

The national cybersecurity management requires a close-knit collaboration between the critical infrastructure operators (Public-Private Partnership, PPP). The NESA's information society pools take care of the collaboration.

**Formation of situational awareness**

The analysed collection of data was created based on interview material, document analysis, and international comparison information. The observations, presentations, and models presented in this article, are based on this data.

***Situational awareness on a tactical level***

Both technical, networked and management situation awareness are emphasized when building the situational awareness. During the last years, Finland has formed its cyber situation awareness through the information-sharing mechanisms of different operators. It is about national and international collaboration. The improvement of information sharing and perception is still a matter of development when it comes to Finland's cybersecurity.[9]

The critical infrastructure operators use such protection techniques in their ICT systems that extend from the interface of the Internet and the organization's internal network right up to the protection of a single workstation or apparatus. These technical solutions make it possible to verify different harmful or anomalous observations. The typical technologies are related to security products such as network traffic analysis and log management (Security Information and Event Management, SIEM), firewall protection, intrusion prevention and detection systems (IPS and IDS) and antivirus. The situation awareness builds up to centralized monitoring rooms (Security Operations Centre, SOC). These technical solutions can be under the organization’s control, or the service can be outsourced to the information security operator. A crucial goal is the situational awareness and protection of the business processes.

Also, especially the critical companies for security of supply have the HAVARO system in the external interface of their network. The system follows the network traffic and detects harmful and anomalous traffic. Then, the warnings come from the NCSC-FI.

The observation ability relates also to a so-called advance warning that can be received from the organization's international or national operation networks. In the centre of operation, there is always the organization's capability to pay attention to the abnormal operation that possibly occurs in the system. The overall observation ability is developed for example by benchmarking and practicing.

The organizations implement the analysis of incidents and anomalies from their own starting points, at the hands of their own or carried out by the service provider. The analysing ability requires more and more the securing of the organization’s business process operation. The intensification of protection operations or for example the introduction of alternative operational models are the most important goals of the operation. The analysing capability determines the choice of needed operations and, that way plays an important role in the organization's decision-making process. The analysing ability must enable a severity classification and so-called cyber-physical view.

The analysing usually happens in centralized monitoring rooms (Security Operations Centre, SOC) based on situational awareness. In the monitoring rooms, the information coming from different sensors is aggregated and a situation-specific analysis is formed. Based on the analysis the needed operations are launched. The organization's possibilities to utilize the information gotten from international or national operational networks relate

to the analysing ability. The personnel's capability to interpret the available observations correctly has a significant meaning in composing situation-specific analyses.

A typical reaction to an incident or anomalous operation comes at first from an incident response manager based on the situation awareness and its analysing. The magnitude and severity of an incident have an impact on the operations. Besides fast-reacting, the organization's management can be congregated to decide on the extension of the operations, and the allocation of the needed resources. Depending on the magnitude of an incident, the whole organization's management to the supervising board can be informed. Regarding the publicly traded companies, the organization's external informing is guided by the informing obligations based on the law.

In the case of a nationally extensive incident, the critical infrastructure organizations keep in touch with the NCSC-FI and utilize not only the authority network but also the industry's network and their business networks. In this communication, the organization's situation awareness and its situation-specific analysing are combined.

Part of the critical companies for security of supply have a communication demand for authorities, such as NCSC-FI, in case of an incident. Based on the NIS Directive, an authority can expand this demand to the critical infrastructure organizations whom the duty to notify does not yet apply.

### *Developing Competences for Situational Awareness of the Organization*

Awareness of the Organization The nationally significant critical infrastructure organizations have developed in forming the cyber situational awareness and observation ability concerning the technical and tactical preparedness. It is also improved by the industry-specific and even more large-scale networking of the organizations. Networking and information sharing are supported by a functional collaboration between the authorities and the private sector. The good situational awareness of different companies (situational awareness and its analysing) and the information sharing via their interest groups is, indeed, a crucial factor in the whole national cybersecurity. Figure 4 sums up the factors that have come up in this research and further the organization's tactical level cybersecurity. The starting point is always the capability of the organization's personnel in recognizing the possible anomalous activity in the used systems and in operating reliably and organized in different situations. In an ideal case, the operation is supported by the technical systems or the used services of the ICT or information security operators or by utilizing the operational network, participating in the authority collaboration, utilizing the consulting services or benchmarking or testing and exercising the operation.

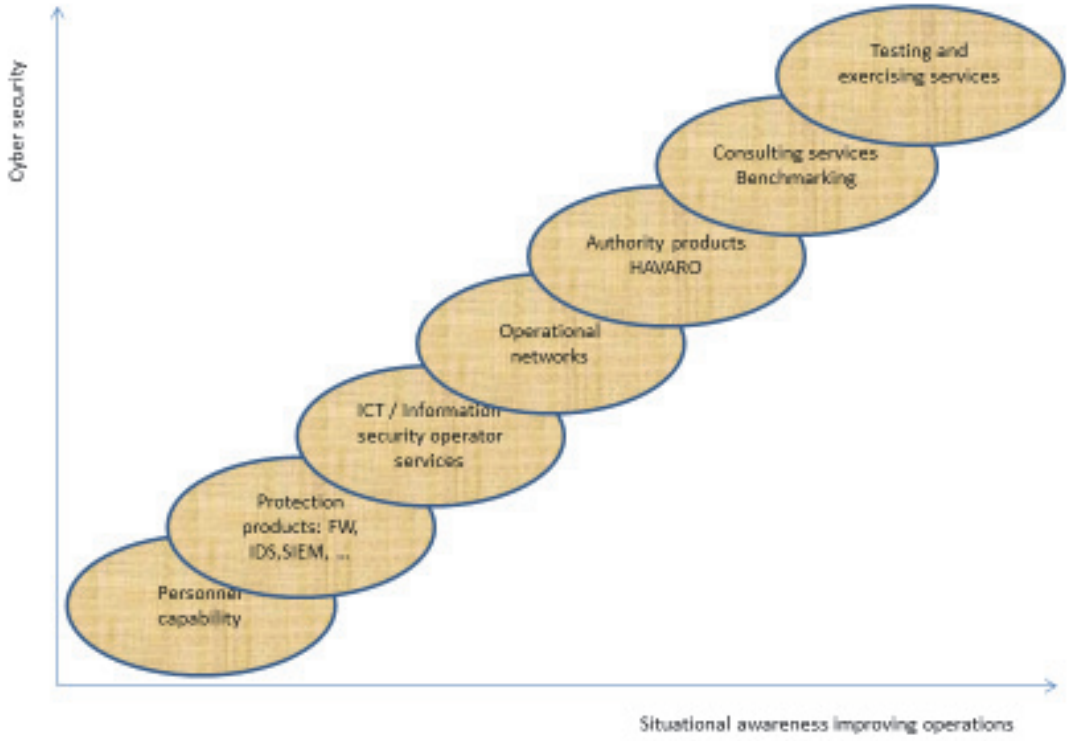



**Figure 4:** Development of an organization's cyber situational awareness as part of comprehensive cyber security. [10]

### *Operational level situational awareness*

The operational level operations are used to advance strategic goals. Comprehensive security- and trust-adding operations require comprehensive cybersecurity management. Its starting point has to be the target's risk assessment, and the operation analyses carried out based on it. The operational level's concrete handson operations must be targeted at the confirmation of information security solutions and the composition of the organization's continuity and disaster recovery plans. The goal has to be the continuous monitoring of the operational processes' usability, and the decision-making support in case of incidents that require analysing and decisions.

The NCSC-FI and NESA are identified as state administrative point of contacts on the business level. The NESA and different pools, especially the digital pool, support companies in developing and maintaining the situation awareness of the cyber operational environment. Because of the operation goals, the NESA brings together a significant part of the authorities and IT businesses. The private sector recognizes its tasks in advancing national cybersecurity. The collaboration models between the authorities and private businesses have been created, and they are internationally comparable.

With the support of the authorities, have been developed not only HAVARO for the security of supply critical operators but also KRIVAT service for critical infrastructure organizations such that the operators themselves form the network. The purpose is to strengthen the collaboration between organizations in grand incidents and speed up the recovery from them.

The technical protection ability of the most significant critical infrastructure organizations and the observation ability based on that are on a good level. Different collaboration

networks are widely used. Organizations and the NCSC-FI keep in touch regularly. The analysing ability of anomalous operation and the incident management ability base on the capable personnel and functional collaboration networks.

***Situational awareness on an uppermost management level***

One of the most fundamental cybersecurity tasks of the organization's uppermost management is the continuous development and maintaining of the trust in operation as part of the national critical infrastructure. The strategic choices relate to the reputation of an organization. The management is required to make concrete strategic choices and to support and guide the performance of the chosen operations through the whole organization. An important task of the management is to take care of the adequate resourcing of operations. About the chosen operations must be communicated extensively with the organization's personnel and other interest groups.

It is important to create a cybersecurity assessment model for the needs of the uppermost management. With the help of that model, for example, other organizations can evaluate their cybersecurity level, become aware of their weaknesses and insufficient contingency planning, and take care of at least of the basics. The operations require strategic level decisions from the organization's uppermost management.

Finland's national cybersecurity execution program 2017–2020 aggregates the pervasive and significant information and cybersecurity improving projects and operations of the state administration, business, and associations, and their responsibilities. The progress of the execution program can be followed by following the development of the different organization's capabilities during the concerned inspection period. The execution program includes extensively effective operations that are developed by other administrative-specific operations, and by the work related to the development of cyber and information security and business continuity management. At the same time, the follow-up results in the formation of national cyber situational awareness.[10, 15]

The National Cyber Security Index (NCSI) is developed for the follow-up of the national cybersecurity-related capability. It is based on twelve sectors that are sorted into four groups as follows: [2]

- General cybersecurity indicators
- Cybersecurity basic indicators
- Event and crisis management indicators
- International event indicators

The NCSI index has four cybersecurity viewpoints per every twelve sections. These are the effective legislation, functioning individuals, collaboration arrangements and the results from different processes. The operation of the index is based on the evaluations of the specialist group.

Table 1 introduces a measure that is based on the NCSI index. It measures the cybersecurity capability of an organization and is developed for the use of businesses and other organizations. The evaluation is based on the requirements, business, interest group collaboration and results. In this organization measure, the twelve sectors of cybersecurity are arranged into four groups as follows:

1. General indicators
2. Basic level indicators
3. Event and incident management indicators
4. National impact indicators.

**Table 1**. Structure of an organization-specific measure.

| | Requirements | Business | Interest group collabora- tion | Results |
|---|---|---|---|---|
| GENERAL INDICATORS | | | | |
| Ability to develop the organization's cyber security culture | | | | |
| Ability to analyze its cyber environment | | | | |
| Magnitude of cyber security training | | | | |
| BASIC LEVEL INDICATORS | | | | |
| Confirmation of operational resources | | | | |
| Risk assessments | | | | |
| Quality requirements of the information systems' operation | | | | |
| Operation follow-up and measures | | | | |
| EVENT AND INCIDENT MANAGEMENT INDICATORS | | | | |
| Quality of contingency planning for incidents | | | | |
| Situational awareness 24/7 | | | | |
| Ability to manage incidents | | | | |
| Ability to recover from incidents | | | | |
| NATIONAL IMPACT INDICATORS | | | | |
| Operation in cyber operational networks | | | | |
| POINTS | | | | |

The commissioning of the measure can be seen to be targeted at the national cybersecurity execution program's goal "A national light cybersecurity evaluation, by which the organizations can take care of reaching the minimum level of security, has been composed." By the organization-specific commissioning of measure, the aforementioned goal can be seen as achieved. The widespread commissioning of the measure in critical infrastructure organizations would make it possible to follow the cybersecurity development of the whole area in the same way as it serves the strategic level needs of a single organization.

### Information sharing on a national level

The NIS Directive requires explicit, identifiable and concrete operations to develop the national situational information sharing. The identification of collaboration partners and information producing operators generates prerequisites for society's encompassing information sharing and, that way, for the development of situational awareness. Figure 5 introduces a national information-sharing structure that enables the NIS Directive-based operation.

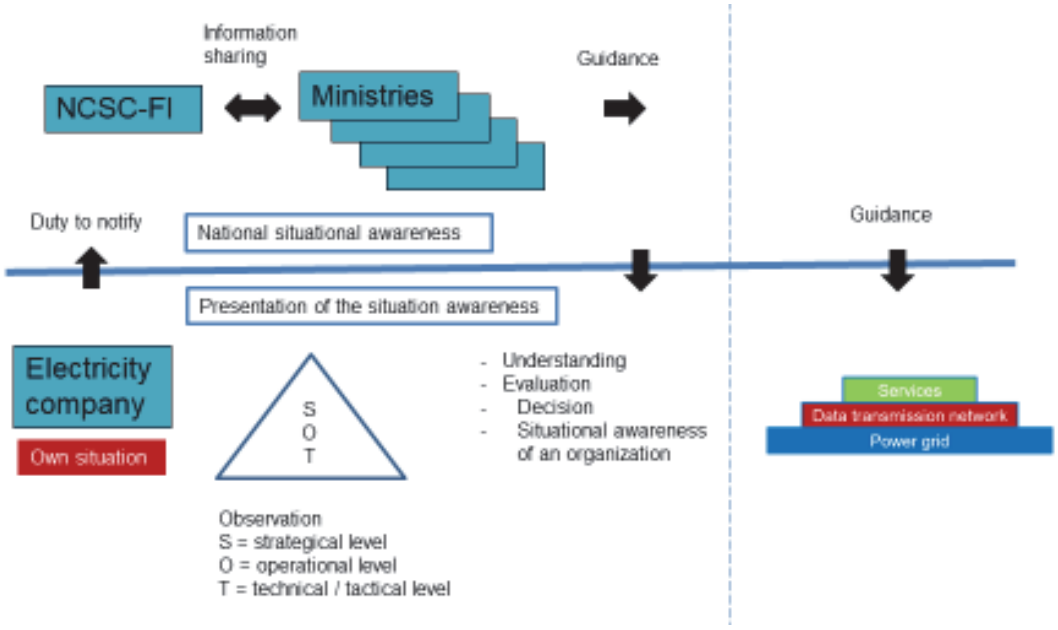



**Figure 5:** Information sharing on a national level.

The European EECSP report "Cyber Security in the Energy Sector" encourages to use the best practices of information sharing through some kind of analysing centre or analysing the process. Thus, the best practice sharing via interest groups and learning from that can be supported. The challenges related to the introduction of new technologies, the challenges caused by the mutual dependence of the market operators, or the challenges build-up by the links between the energy systems and networks are typical scenarios that can especially benefit from the sharing of best practices. Also, the procedure can be used for sharing delicate information that helps the operators in protecting their network proactively.[1]

In national information sharing, a critical infrastructure organization (electricity company in Figure 5) forms a cyber situation awareness from its starting points. In an ideal case, it bases on the observations from the different levels of the organization that is strategic, operational and technical/tactical level. Based on the information, the electricity company maintains its continuous situational awareness to support its decisions. In case of a cyber incident, the electricity company delivers information about its situation-specific analysis, based on the duty to notify, to the NCSC-FI and when need also to the responsible ministry. Based on their mutual information sharing, the NCSC-FI and responsible ministry form a national situational awareness about the matter. The responsible ministry takes care of the related and needed guidance operations to the other interest groups and the organizations of its area of responsibility. The NCSC-FI carries out continuous information sharing with the critical infrastructure organizations about the cybersecurity situation.

Finland's national strength in the organizations' possibilities in utilizing different networks when sharing the cybersecurity information has been emphasized in different researches. [9, 10] Here, three confidential information-sharing networks that are utilized actively are introduced. These have been formed in connection with business operation, or a separate trust circle has been established between some industry's companies that can

reach also into an international collaboration. Also, nationally operates a trust circle between the authorities and private sector (Public-Private Partnership, PPP). Figure 6 illustrates the aforementioned trust circles in the company field.

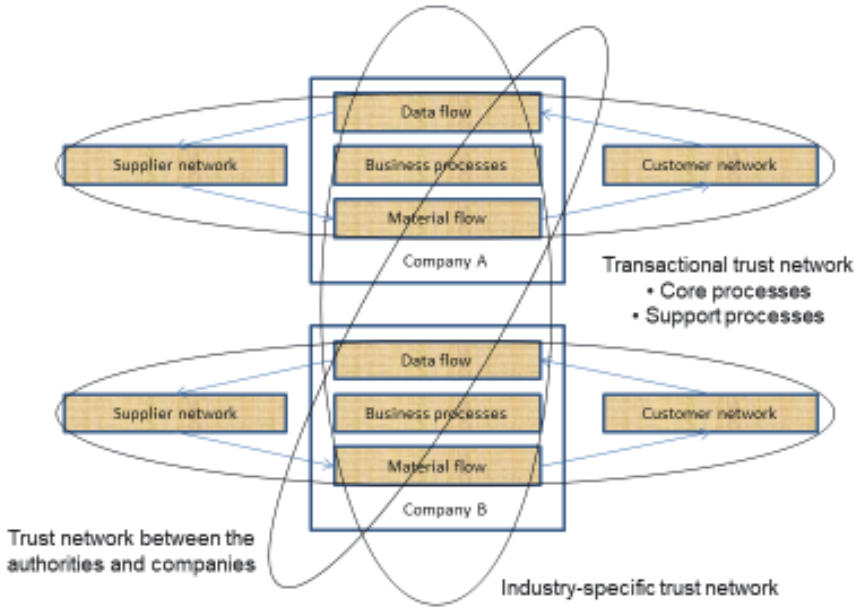



**Figure 6:** Trust networks related to an organization's cyber situational awareness development.

The critical infrastructure organizations have functioning situation awareness arrangements and analysing capability, and they exchange information by utilizing their networks and are capable of incident management based on their starting points. The risk assessments and the procedure option analyses based on the evaluations are a significant part of the continuity management of the organization's business processes. The concrete hands-on operations of the operational level must be targeted at securing the information security solutions and composing the organization's operational continuity and disaster recovery plans. The goal must be in the continuous follow-up of the operational processes' usability, and the contingency planning for incidents.

The cyber operational environment is dynamic, which means that especially the strategic agility is required when preparing for incidents. On the other hand, the organization's strategic decision-making level must also have tools for evaluating the development of the whole organization's cybersecurity. In this paper, the commissioning of the measure that follows the organization-specific capability is recommended. There, the evaluation is carried out via the requirements set for the operation, business, interest group collaboration and results by utilizing four indicators. The four indicators have been derived from this cybersecurity measure from the international index, and they are the organization's general indicators, basic level indicators, event and incident management indicators, and national impact indicators.

**Summary**

The main novelty value of this study is the promotion of their practical measures which the NIS Directive required. In the big picture, the different parties related to the development of situational awareness must yet be able to improve their operation by even more

efficient technical procedures, strengthen the network-like operation, and increase the utilization of public sector services. There will be good preconditions to the above-mentioned matter when cybersecurity capabilities of the organization are widely promoted as a part of the national critical infrastructure and the common objectives determined by the EU.

For the first research question, it is stated that as the target state of the organization's cyber situational awareness and its interest groups' information sharing can be set the operation where the recognition of threatening incidents and reacting to them happens in an efficient process. It must include all the organization's decision-making levels (strategic, operational and technical/ tactical) and utilize the national and international strengths of information sharing.

Based on the research the following basic requirements apply to the development of the organization's incident management:

- Strategic goals: a) Cybersecurity management in all circumstances; b) Strategic choices for operational continuity management
- Critical success factors: a) Good situational awareness on all the organizational levels; b) Fast reaction ability and executive guidance; c) Clear operational models and their sufficient resourcing; d) Good information sharing between the different interest groups; e) Crisis communication
- Evaluation criteria and target levels: a) Effectivity of the operation; b) Optimal resourcing.

For the second research question, the techniques used by organizations, procedures developed for incident reacting and different trust circles form a nationally useful observation ability. This scattered organization-specific observation ability and the analysing information and data reserve it contains can be utilised nationally in the analysing phase for the management of wide-scale incidents. The arrangement requires the creation of mutual operational models for information sharing. Because it is very presumable that there are not enough centralized resources to be used for analysing a wide-scale and quickly evolving cybersecurity incident, as a solution should be outlined a network-like operation consisting of the experts from different organizations (virtual analysing). Then, the data reserve should be jointly used, and the experts would use their trust circles that reach to the international information sharing relations. The usability of data reserve forms the key for analysing. When building it must take into account not only confidentiality but also the data integrity and amount questions. In the referenced research, the evaluations of i.e. the formation of excessive data amount were presented, and then the analysing becomes more difficult too. Thus, the different technical solutions of data processing should be examined.

For the third research question, the main conclusion is that the organizationspecific measures, which promote cybersecurity and situational awareness, make the filling of the obligations of the NIS directive (Part D) possible. Part D requires that the providers of central and/or digital service should take into use the security and notification requirements. In every member state, national and EU -level situational awareness is based on the ability to maintain situation consciousness. Thus, the measures presented in this study also will promote other objectives appointed by the NIS directive.

**Acknowledgements**

The part of the work performed by Laurea University of Applied Sciences was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

## References

1. EECSP Expert Group, "Cyber Security in the Energy Sector," Europe: Energy Expert Cyber Security Platform (EECSP), 2017.
2. e-Governance Academy, "National Cyber Security Index (NCSI)," 2017, https://ncsi.ega.ee/, accessed August 6, 2019.
3. Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors and Ergonomics Society 37, no. 1 (1995): 32-64.
4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, Official Journal L 194, July 19, 2016, https://eurlex.europa.eu/eli/dir/2016/1148/oj.
5. Sid Faber, "Flow Analysis for Cyber Situational Awareness," Software Engineering Institute, Carnegie Mellon University, December 7, 2015, https://insights.sei.cmu.edu/ sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html, accessed August 6, 2019.
6. Seppo Horsmanheimo, Heli Kokkoniemi-Tarkkanen, and Jouko Vankka, "Kriittisen infrastruktuurin tilannetietoisuus (Situational Awareness of Critical Infrastructure)" (Helsinki: Prime Minister's Office, 2017).
7. Kirsi Janhunen, "Valtionhallinnon häiriötilanteiden hallinta - miten VIRT-toimintaa kehitetään?" (Helsinki: Ministry of Finance, 2015). Cyber Situational Awareness and Information Sharing in CI Organizations 255
8. Joint Task Force Transformation Initiative, "Managing Information Security Risk – Organization, Mission, and Information System View," NIST Special Publication 800-39 (Gaithersburg, MD: National Institute of Standards and Technology, 2011).
9. Martti Lehto and Jarno Limnéll, "Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi (Finland's Cyber Security: The Present State, Vision and the Actions Needed to Achieve the Vision)" (Helsinki: Prime Minister's Office, 2017).
10. Martti Lehto, et al., "Kyberturvallisuuden strateginen johtaminen Suomessa (Strategic Management of Cyber Security in Finland)" (Helsinki: Prime Minister's Office, 2018).
11. Ministry of Defence of Finland, "Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society)" (Helsinki, Ministry of Defence, 2010).
12. National Audit Office of Finland, "Kybersuojauksen järjestäminen" (Helsinki, National Audit Office of Finland, 2017).
13. National Emergency Supply Agency – Organisation, www.nesa.fi/organisation/, accessed August 6, 2019.
14. Jouni Pöyhönen and Martti Lehto, "Cyber Security Creation as Part of the Management of an Energy Company," 16th European Conference on Cyber Warfare and Security, Dublin, 2017, pp. 332-340.
15. The Security Committee, "Suomen kyberturvallisuusstrategian toimeenpanoohjelma 2017-2020 (Implementation Programme for Finland's Cyber Security Strategy for 2017- 2020)" (Helsinki: The Security Committee, 2017).

16. The Security Committee, “Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society)” (Helsinki, The Security Committee, 2017).
17. Traficom – About us, https://www.traficom.fi/en/traficom/about-us, accessed August 6, 2019.
18. Kirsi Virrantaus and Hannes Seppänen, “Yhteiskunnan Kriittisen Infran Dynaaminen Haavoittuvuusmalli,” Helsinki, Matine, Apr 10, 2014.

**Artikkeli P5:**

# Cyber Situational Awareness in Critical Infrastructure Organization

2019
Jouni Pöyhönen, University of Jyväskylä, Jyväskylä Finland,
Jyri Rajamäki, Laurea University of Applied Sciences, Espoo, Finland
Viivi Nuojua, University of Jyväskylä, Jyväskylä Finland,
Martti Lehto, University of Jyväskylä, Jyväskylä, Finland

Submitted to be published in book Springer, in publishing process

Request a copy from author.

**Artikkeli P6:**

ResearchGate

# Cyber security: Trust based architecture in the management of an organization security

2020

Jouni Pöyhönen, University of Jyväskylä, Jyväskylä Finland,
Martti Lehto, University of Jyväskylä, Jyväskylä, Finland

Originally published in the proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS2020, 25-26 June 2020, University of Chester, UK, pages 304-313

# Cyber security: Trust based architecture in the management of an organization security

Jouni Pöyhönen, Martti Lehto
University of Jyväskylä, Finland
jouni.a.poyhonen@jyu.fi
martti.lehto@jyu.fi

**Abstract**

The functioning of a modern society is based on the cooperation of several organisation, whose joint efficiency depends increasingly on trustable business processes. Trust is based on availability, reliability and integrity of ICT system data in the operating environment, whose cyber security risks are continuously augmented by threatening scenarios of the digital world.

Information and Communications Technology (ICT) can be seen a critical asset of organization. To prevent loss of customers the trust and that way revenue and money, as well as to protect organisational reputation, this asset must be protected from cyberattacks. Trust in cyber environment is critical factor for organization in order to contentiously run the business processes that the customers can count on.

This article emphasizes the system view, the trust and the trust-based architecture measures as an essential part of organization cyber security management. The article integrates several basic standards and three decision making viewpoints as an organisation cyber security architecture framework. The cyber trust factors for organization have been also defined by the researchers in this article.

We have also examined how the measures can be considered part of the organization's process structures while creating trust in its operation within a dynamic cyber environment. Thus, the article recommends and utilizes the PDCA (Plan, Do, Check, Act) method in developing cyber security management practices.

In order to put the measures into practice, the leadership of an organisation regard trust-enhancing measures related to cyber security as a strategic goal, maintain efficient processes and communicate their implementation with a policy that supports the strategy.

Keywords: Organization, Cyber security, Process, Trust, Architecture, PDCA

## 1 Introduction

The functioning of a modern society is based on the cooperation of several critical infrastructures, whose joint efficiency depends increasingly on a cyber secure organization. Crucial in the cyber environment are the usability, reliability and integrity of system data in the operating environment, whose cyber security risks are continuously augmented by threatening scenarios of the digital world. A modern society depends entirely on a cyber environment that provides dynamic services.

In Finland's first Cyber Security Strategy, the cyber environment (domain) is defined as an electronic information (data) processing environment that consists of one or more information technology infrastructures. According to the Strategy, cyber security refers to a desired end state in which the cyber environment is reliable and in which its functioning is ensured. Critical infrastructure, furthermore, refers to the structures and functions that are indispensable for the vital functions of society. They include physical facilities and structures as well as electronic functions and services. (Secretariat of the Security Committee, 2013)

The global threats within the cyber environment have remained at a high level over the past few years, as stated in the annual international business world surveys by the World Economic Forum. They are seen to be among the major global threats based on the probability and impact of their realization. (World Economic Forum, 2019)

The role of organization ICT-systems in the cyber world as well as the factors that affect their cyber security, it is of primary importance to be aware of the most central features of the systems. Organizations can use different standards, frameworks and best practices when addressing cyber security. These governance documents are used typically to implement different kind of controls. In addition to that most of these documents also describe very specific capabilities, and an organization can use them to develop in securing their cyber domain. By enhancing capabilities, consisting of people, processes and technology, are meant to achieve outcomes or effects, that are applicable to the operational domain. (Jacobs, P. C., von Solms, S. H. and Grobler, M. M., 2016)

The ICT and industrial automation systems are part of the common cyber world, in which the primary risks are related to the loss of money, sensitive information and reputation as well as to business hindrance. Security solutions are hereby the key elements in risk management. The vulnerabilities behind the risks can be analysed as insufficient technology in relation to attack technology, insufficient staff competence or inappropriate working methods, deficiencies in the management of organizations, and lacks in operating processes or their technologies. The most common motives of attackers are related to the aim of causing destructive effects on processes, making inquiries about process vulnerabilities, and anarchism or egoism. These attacks can even be carried out by state-level actors, but perhaps most commonly by organized activists, hackers or individuals acting independently. (Lehto M., 2015)

The basic research question of this paper is “How can we gain cyber trust at the organizational level?

## 2 An organization’s cyber structure

Martin C. Libicki has created a structure for the cyber world, whose idea is based on the Open Systems Interconnection Reference Model (OSI). The OSI model groups communication protocols into seven layers. Each layer serves the layer above it and is served by the layer below it. The Libicki cyber world model has the following four layers: physical, syntactic, semantic and pragmatic. (Libicki, 2007)

Organization´s supply chains are complex systems of systems characterized by a conglomeration of interconnected networks and dependencies. The general networks and working processes involved in the operation of an organization can be illustrated with a logistics framework that comprises a supplier network, a production process, a client network, and information and material flows that connect them. According to EU commission “the ICT sector is vital for all segments of society”. Information and communication technology (ICT) systems are part of critical organization’s infrastructure and thus constitute a significant part of the operations that support an organization’s core processes. Corporate-level ICT systems are related to administration and to the management of information and material flows in the network. The production level includes industrial automation systems (industrial control systems, ICS). (Edwards N, et al. 2016, EU Commission, 2009)

Cyber security professor in University of Jyväskylä, Martti Lehto, has updated the Libicki`s four layers cyber world model by adding the fifth layer in order to consider organisation networking needs. The structure is described in figure 1.

In the case of five-layers model structure, the physical layer contains the physical elements of the communications network, such as network devices, switches and routers as well as wired and wireless connections. The syntactic layer is formed of various system control and management programs and features which facilitate interaction between the devices connected to the

network, such as network protocols, error correction, handshaking, etc. The semantic layer contains the information and datasets in the user's computer terminals as well as different user-administered functions, such as printer control. The service layer is the heart of the entire network. It contains such as administrative services, ICT-services, security services, IT based manufacturing services, supply and logistics services. The cognitive layer portrays the user's information-awareness environment: a world in which information is being interpreted and where one's contextual understanding of information is created.

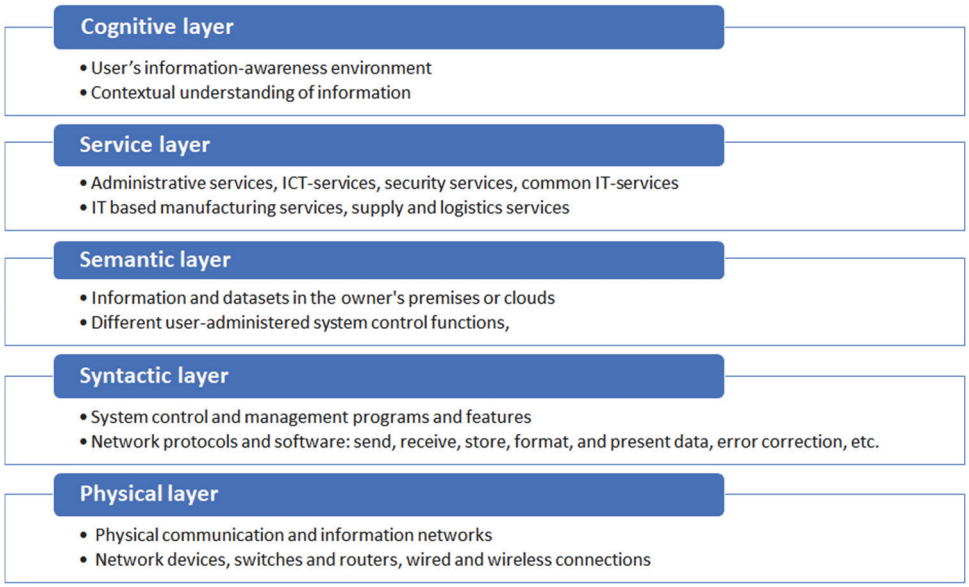



Figure 1. The five layer structure for the cyber world (modified from Lehto & Neittaanmäki, 2018)

Protecting the ICT-systems against threats implies measures taken based on risk assessment, and they ensure the availability of primarily digital information in the operating processes being examined. The measures are highly significant for the overall availability of the systems that support the organization´s business processes. Availability plays a key role in achieving business results and promoting the reliability of activities. Further central goals include the reliability and content integrity of information within the processes and used by the processes. Overall trust should be built from these starting points, based on the target organization's realistic idea of its own capabilities to reliably manage the challenges involved in operations within the cyber world. The following section addresses the significance of trust in the cyber environment for the operations of an organization. Moreover, trust-enhancing measures applicable to an organization will be mapped.

## 3 Trust in an organization's cyber security

### 3.1 The significance of trust for cyber security

Trust in the operation of organizations and its continuous maintenance with effective measures are central factors affecting cyber security. Security is based on trust. Without trust there is no security, and vice versa. It is also good to be conscious of the fact that perfect safety is in general hardly achievable, and this also applies to the cyber world, which is a dynamic environment difficult to anticipate. Therefore, it is particularly important to understand the great significance of trust in the cyber world and its security. The role of measures enhancing trust is emphasized. When we build operations in the cyber world on a foundation that is as sustainable as possible, we can utilize the diverse opportunities it offers. (Limnell J., Majewski K. and Salminen M., 2014)

Finland's national cyber security strategy highlights the need to increase general cyber trust throughout the entire society. The strategy emphasizes that all actors, from individuals to enterprises and public administration, are responsible for their own preparedness in order to achieve cyber trust. (Secretariat of the Security Committee, 2013)

The ISO 9000 Standard states that an organization achieves success by acquiring and maintaining the trust of clients and other relevant interest groups. Understanding their present and future needs contributes to the organization's continuous success. The standard includes the central concepts of quality management and the principles for building trust. It can be applied by organizations that pursue ongoing success in their operation by utilizing a quality management system of their own. The quality of an organization's products and services is determined by how its clients experience that their needs and expectations are met. Clients also look for guarantees on the organization's ability to systematically produce products and services that correspond to their requirements. The ISO 9000 Standard comprises seven quality management principles, which constitute a commonly accepted basis for applying the standard series. The standard also specifies the benefits to an organization that has adopted the principles in its operation. The seven basic quality management principles are related to customer focus, leadership, the engagement of staff, a process approach, continuous improvement, evidence-based decision-making, and relationship management. (Finnish Standards Association SFS, 2016)

### 3.2 Cyber trust and process management

Establishing measures that increase cyber world security and trust in an organization is primarily the responsibility of corporate leadership. Integrating the necessary measures with the idea of ensured business activities increases their significance and benefits through better processes for the entire organization, interest groups and society. If security is not considered, risk analysis reveals potential damages as well as their costs and social consequences. The leadership's views and requirements brought out in the analysis play a central role in developing security planning for the operating process. The costs and other resources allocated to the activities are simultaneously specified. (Stouffer K., Falco J. and Scarfone K., 2011)

Process management theory has developed along with industrial production. The development of industrial mass production led to the use of variation theory while developing production process control: to perform control measures, uniform product quality was monitored with statistical methods. Statistical process analysis led to the observation that variation occurs everywhere in nature and in the processes and systems created by humans. After analysing distributions that involved variation, variation was classified into two types according to its causes: variation due to common causes (or the system itself) and variation due to special causes (i.e. named and assignable causes). Systemic variation has random causes and it is therefore often normally distributed, according to Gaussian distribution. Variation resulting from special causes does not follow any regularities. The common causes of variation are thus constantly present in the process. An individual cause produces only little deviation, but several causes together generate considerable variation. The causes of special variation, on the other hand, are not constantly present in the process. They come from outside of the process and usually generate more variation in the process than the common causes. In uncontrolled processes, deviation as a result of both types occurs simultaneously. (Lillrank P., 1998)

In principle, Lillrank's theory on the causes of process variation can also be generalized to the processes of an organization. The measures taken by organization leadership can be targeted at reducing variations resulting from both aforementioned types of causes. Proper planning and control of process performance reduce variation generated by random causes. At a general level, it is always recommended to aim at reducing this variation. If organization leadership, in particular, concentrates too much on process changes resulting from random causes, it can lead to overreactions in process control due to the measures chosen. At its worst, this can lead to loss of control in managing the overall process. The actions of organization leadership should indeed be targeted primarily at proactively preventing variation generated by special causes.

Almost without exception, serious cyber security disturbances occurring in the operating process cause harms. They do not represent normal process variation but are deviations resulting from special causes. They are not in the normal range of variation. Taking these special causes

into account in planning and proactively implementing managerial activities reduces related risks and improves the overall reliability of the organization's operations.

### 3.3 Measures increasing cyber trust

The following measures related to cyber security management in an organization encompass of leadership, process management and seven principles quality management.

In order to comprehensively build organization cyber security, organization leadership must define and guide actions at the strategic, operational and technical-tactical levels. The strategic level provides answers to 'why' and 'what' questions. The operational and tactical levels answer the 'how' question. The approach guided by questions ensures that the right things are done and that they are done in line with the set goal. The technical-tactical level must implement the goal-oriented activities defined at the strategic level, not create it. The organization's organizational capability in implementing the cyber security measures required by the technical-tactical level ultimately determines how the organization manages potential disturbance situations. (Limnell J., Majewski K. and Salminen M., 2014)

Building organization cyber security management begins from the level of vision and strategy work. The visions created by organization leadership to enhance cyber trust are translated into strategic goals, operational-level actions, guidelines and a policy. The practical measures derived from the strategy are realized at the technical-tactical level. Organizational capability factors enable the success of the measures.

The strategic choices supporting the creation of visions are primarily related to organization social responsibility, organization reputation, and ensuring business and its economic efficiency. The leadership is expected to make concrete strategic choices as well as support and guide the execution of the chosen measures throughout the organization. It is also important that the leadership ensures sufficient resource allocation to the measures. The chosen measures should be comprehensively communicated to the organization's interest groups. (Stouffer K., Falco J. and Scarfone K., 2011, Finnish Standards Association SFS, 2016)

The measures at the operational level promote the strategic goals. Comprehensive measures that increase security and trust call for holistic cyber security management. It must be based on risk assessment and analyses of the measures based on the assessment. It is also important that the organization declares and communicates the policy with which the leadership commits to the measures required to develop cyber security management. The declaration of a policy that ensures cyber security and the development of related procedures must be integrated with the organization's general policies. The highest organizational level is responsible for creating a policy that defines acceptable risk levels and the measures used in the reduction of risks (Stouffer K., Falco J. and Scarfone K., 2011). The concrete measures at the operational level must be targeted at ensuring data security solutions and at creating business continuity and recovery plans (Finnish Standards Association SFS, 2012). The maintenance of situational awareness regarding the cyber environment of the organization's processes, furthermore, makes it possible to monitor the effects of the operational measures and, when needed, to react efficiently to events that constitute a threat within the organization's operating environment. The aim must be to continuously monitor the availability of processes and to support decision-making in disturbance situations that require analyses and decisions. (Faber, 2015)

The tactical organization level encompasses the systems and processes that comply with the he tactical organization level encompasses the systems and processes that comply with the structure of the cyber world. Consistent and predictable results are achieved more efficiently when operations are handled and managed as interrelated processes that function as a coherent system (Finnish Standards Association SFS, 2016). Cyber security threats set special requirements for these processes in addition to other operational requirements. At a general level, the performance of processes is determined according to their client-based demands. In the cyber environment, the target can be achieved by defining the processes to be protected, choosing process control mechanisms successfully, and by using expedient technological solutions and services to protect the processes (Stouffer K., Falco J. and Scarfone K., 2011). Successful operation also calls for the adoption of security-oriented values to guide the activities of staff (Lillrank P., 1998).

The aforementioned solutions suitable for the cyber environment constitute an entity that can be called a technical-tactical level.

The continuous improvement of activities related to cyber security as well as the development of staff competence enhance the organization's capability to proactively prevent disturbances and tolerate potential changes in process operation caused by them. Taking the staff into account at all organizational levels, as well as focusing on competence and the possibilities it opens to fully influence in the organization, develops the overall operations of the organization (Finnish Standards Association SFS, 2016).

Staff competence is a crucial factor that determines the level of the entire organization's activities. The capacity of human resources can be increased by developing employees' knowledge and skills related to cyber security and thus developing the organization's capabilities. Challenges related to capabilities grow when an enterprise's cyber environment becomes more complex along with globalization and technological development. Investment in staff competence can transform the enterprise's capability into core competence, which can be used to pursue competitive advantage through trust. This will provide unique added value to both the organization and its customers. Valuable capabilities are helpful in an organization's threat and risk management and can consequently facilitate, in particular, the utilization of profitable opportunities. (Hitt, M. A., Ireland, D. R. and Hoskisson, R. E., 1997)

The Finnish Cyber-Trust research program was conducted 2015-2017 and University of Jyväskylä was one of the research partners in this program. We have determined the cyber trust for organization and described the relationship between cyber trust and comprehensive actions at organizations strategic, operational and technical-tactical levels at one of the research programs reports. The information from the report has been transferred to this scientific article in the way we have now shown. The cyber security and continuous development activities and staff competence support the measures taken at the strategic, operational and technical-tactical level. The summarized measures taken to increase an organization cyber trust is illustrated in Figure 2.

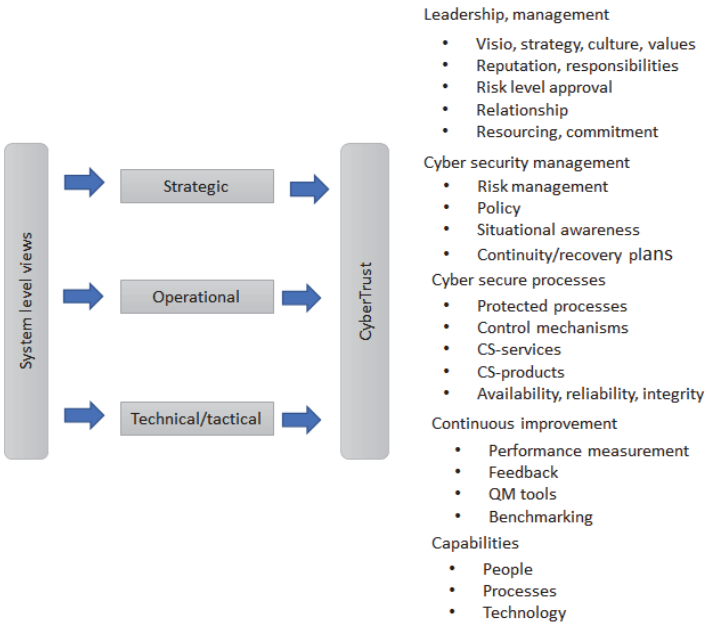



Figure 2. Measures increasing an organization cyber trust

## 4 Implementing the measures that enhance cyber trust

### 4.1 An integrated management system and its components

The latest standard of the ISO 9000 series (ISO/IEC 9004: 2018) emphasizes the importance of trust in an organization's ability to achieve continuous success and to recognize at all levels of management the factors influencing its operations in a constantly changing operating environment. (ISO/IEC 9004: 2018)

When management in an organization is performed systematically, we talk about the organization's management system. A management system can comprise various control systems that comply with different standards, such as a quality management system, an information security management system and an environmental management system. In order to put into practice principles that comply with different standards, an organization may describe the required measures in its integrated management system (IMS). The IMS is a description of the procedures everyone should apply in the organization. With the help of guidelines and operations models jointly defined by the leadership and staff, the aim is to purposefully maintain a high level of activities and to develop the activities with an eye on set goals as well as the needs of clients and interest groups. The integrated management system compiles process descriptions, guidelines, recordings, indicators, tasks and feedback into a functional whole, which guides and supports the organization's mission and vision as well as the actions taken to realize and assess them.

**4.2 Decision-making levels and system view**

Organizations operate in very complex, interrelated cyber environments, in which the new and long used information technical system entities (e.g. system of systems) are utilized. Organizations are depended on these systems and their apparatus in order to accomplish their missions. The management must recognize that clear, rational and risk-based decisions are necessary from the point of view of business continuity. The risk management at best combines the best collective risk assessments of the organization's individuals and different groups related to the strategic planning, and also the operative and daily business management. The understanding and dealing of risks are an organization's strategic capabilities and key tasks when organizing the operations. This requires for example the continuous recognition and understanding of the security risks on the different levels of the management. The security risks may be targeted not only at the organization's own operation but also at individuals, other organizations and the whole society. (Joint Task Force Transformation Initiative, 2011)

Joint Task Force Transformation Initiative (2011) recommends implementing the organization's cyber risk management as a comprehensive operation, in which the risks are dealt with from the strategic to tactical level. That way, the risk-based decision-making is integrated into all parts of an organization. In Joint Task Force Transformation Initiative's research, the follow-up operations of the risks are emphasized in every decision-making level. For example, in the tactical level, the follow-up operations may include constant threat evaluations about how the changes in an area can affect the strategic and operational levels. The operational level's follow-up operations, in turn, may contain for example the analysis of the new or present technologies in order to recognize the risks to the business continuity. The follow-up operations of the strategic level can often concentrate on the organization's information system entities, the standardization of the operation and for example on the continuous monitoring of the security operation. (Joint Task Force Transformation Initiative, 2011)

From the necessity of the organization's cyber security operations can be drawn as a necessity of comprehensive awareness in system level. The organization's and decision-maker's awareness can be seen as a system level awareness arrangement. Thus, an appropriate awareness supports the cyber risk management and more extensively the evaluation of the organization's whole cyber capability. We have integrated organization´s three decision-making levels to five-layers cyber structure in order to have comprehensive system view from organization cyber security environment. It is system thinking approach to the organization cyber security subsect and subject and the principle is described in figure 3.

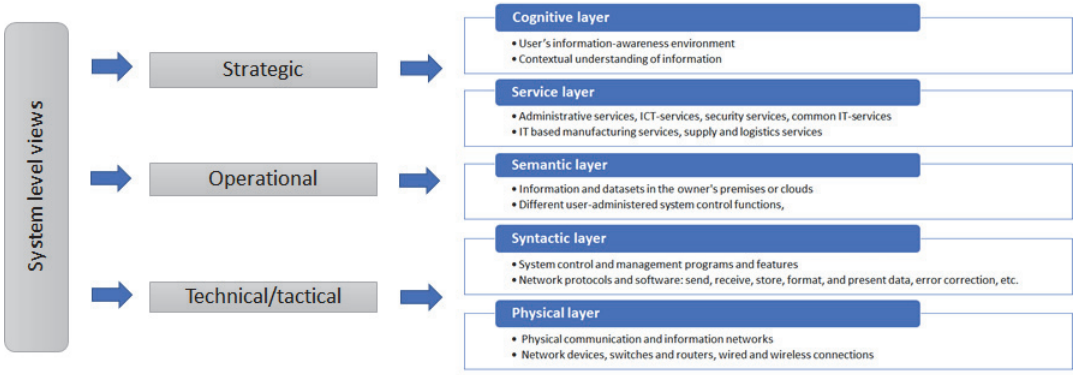



Figure 3. System level view to organization cyber security

**4.3 Trust-enhancing measures based on trusted architecture**

By adding three decision-making levels to five-layers cyber structure in order to have comprehensive system view from organization cyber security environment. The following standards were utilized to support the idea to create trust based cyber security architecture framework based on comprehensive system view from organization cyber world.

NIST 800-39 publication places information security into the broader organizational context of achieving mission/business success. The objective is to: (NIST 800-39, 2011)

- Ensure; senior leaders/executives recognize cyber security risks and managing such risks;
- Ensure; risk management process are being conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster; cyber security risks in mission/business processes are designed within comprehensive enterprise architecture, and system development life cycle processes; and
- Help; people in system implementation or operation understand how cyber security risks in systems affect the mission/business success (organization-wide risk).

The ISO 9000 standard family of quality management systems helps organizations ensure meets of stakeholders needs related to products or services. The main goal is the customers satisfaction. The fundamentals of quality management systems, including the seven quality management principles (customer focus, leadership, the engagement of staff, a process approach, continuous improvement, evidence-based decision-making, and relationship management) are the basic principles of the standard family. (Finnish Standards Association SFS., 2016)

The ISO 27000 standard family provides recommendations for information security management system (integrated elements of an organization to establish policies and objectives and processes to achieve those objectives), risk treatments and controls. (ISO/IEC 27000: 2018)

Integration of the measures increasing an organization cyber trust (Fig 2.) and the system thinking approach to organization fife layer cyber structure (Fig. 4) makes possible to have trust based cyber security architecture framework. The content of the aspects of it is derived from the organization-wide risk management standard, NIST 800-39 (NIST, 2011) and perspectives from ISO 9000 standard family (seven quality management principles) and ISO27000 standard family.

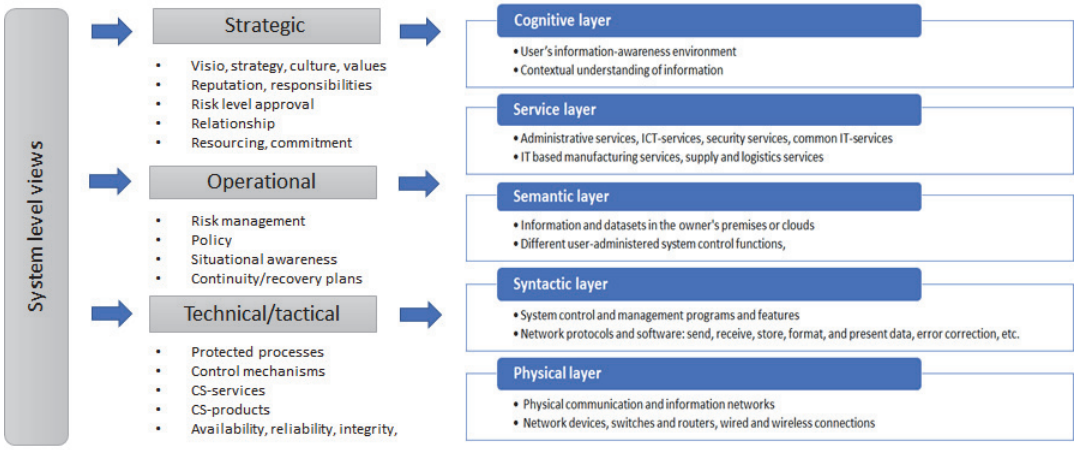



Figure 4. Trust based cyber security architecture framework.

Business Dictionary.com defines a capability in general as the "measure of the ability of an entity (department, organization, person, system) to achieve its objectives, especially in relation to its overall mission", and in quality perspective as the "total range of inherent variations in a stable process". (BusinessDictionary.com 2020). Dickenson and Mavris defines a capability as "the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks" and also "the ability to execute a specified course of action". (Dickerson C. and Mavris D. N., 2010). Thus, the capability of organization can be seen also as an ability to learn from its experiences and use relevant information to improve cyber security processes. Organization capabilities support actions of the architecture framework.

The process approach promoted by ISO 9001 systematically identifies processes that are part of organization quality system. Related to the quality management system, the PDCA cycle is a dynamic cycle that could be implemented in each process throughout the organization. It combines planning, implementing, controlling and continual improvement. That way organization would achieve continual improvement once it will implement the PDCA cycle. (9001 quality)

**4.4 The PDCA method as a tool for developing activities**

An organization's cyber security architecture framework could demonstrate how cyber thrust measures can be addressed, committed and implemented in all decision-making levels, strategic, operational and technical/tactical. In that means continuous improvement of processes can based on activities, whereby risk analysis has been considered. In order to create the measures, the organization must have a systematic approach to developing its operations.

The ISO9000 Standard recommends the PDCA (Plan, Do, Check, Act) method for a systematic development of an organization's activities. The method is based on a cycle of four development phases. The first phase (Plan) set the objectives of the system and processes to deliver results ("What to do" and "how to do it"). In the second phase realization (Do), implement and control what was planned. The third phase (Check), monitor and measure processes and results against policies, objectives and requirements and report results. At the last (Act), take actions to improve the performance of processesphase. After the cycle has been implemented once, one will return to the first phase and start a new cycle with improvement actions based on a new situation analysis. Development can thus proceed as an endless process, in which a new level of activities is achieved after each cycle. The method is based on the idea of continuous improvement, with risk-based thinking at each stage of activities. (ISO/IEC 9001: 2015)

The measures during one round of the cycle usually require a lot of planning, so sufficient time should be reserved for it. It is important to select the measures in relation to the resources needed for their implementation. The maturity level of the organization's development activities affects the evaluation of the implemented measures. When developing cyber security, at an initial stage the aim can be to recognize the need for cyber security management and to define cyber security risks for business. Hereby, the PDCA cycle may comprise the administrative actions most

necessary according to risk assessment, such as a coherent information security policy in production, practical guidelines for maintaining information security in production, and potential preliminary system-specific cyber security checks. The targets for development must later be chosen according to risk prioritization.

## 5. Conclusion

Ensuring the availability and reliability of processes and data integrity is vital for the efficient functioning of trust based cyber security. Therefore, the measures taken in organizations in order to manage and control its processes and implement continuous improvement actions are an essential component of the trust of business processes.

The major cyber environment risks within the processes of an organization require that trust is enhanced and maintained at all levels of business activity. For the basic research question "How can we gain cyber trust at the organizational level?", this paper includes system view and standards-based way to form cyber trust architecture framework for organization use. Firstly, the cyber trust activities for organization have been defined in this article. After that the secure architecture. Comprehensive measures to increase cyber trust and trusted architecture framework together with the development of organization capabilities related to cyber activity, also improve an organization's continuity and competitive edge. The integrated management system (IMS) of organization supports the way for assess the actions to be taken.

Serious cyber security disturbances occurring in the organization operating process cause in many cases harms. They are resulting from special causes in the process. So, they do not represent normal process variation. Implementing the cyber trust architecture framework, these special causes would be taken into account proactively and measures reduce process related risks and improves the overall reliability of the organization's operations.

## References


Faber S., 2015. Flow Analytics for Cyber Situational Awareness. SEI Blog, 2015. https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html

Dickerson C. and Mavris D. N., 2010. Architecture and Principles of Systems Engineering, CRC Press.

Edwards N., Kao G., Hamlet J., Bailon J. and Liptak S., 2016. Supply Chain Decision Analytics: Application and Case Study for Critical Infrastructure Security. Proceedings of The11th International Conference on Cyber Warfare and Security ICCWS 2016 s. 99-106.

EU Commission, 2009. Critical information infrastructure protection (2009), COM (2009) 149 final, Commission of the European Communities, Brussels, 30.3.2009

Finnish Standards Association SFS., 2012. SFS-käsikirja 327. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. SFS ry, Helsinki, 2012.

Finnish Standards Association SFS., 2016. Johdanto laadunhallinnan ISO 9000 -standardeihin. Available on 27 January 2020: slideplayer.fi/slide/11133323/

Hitt, M. A., Ireland, D. R. and Hoskisson, R. E., 1997. Strategic Management, 2th edison, St Paul, West Publishing Company, 438 s.

Jacobs, P. C., von Solms, S. H. and Grobler, M. M., 2016. Towards a framework for the development of business cybersecurity capabilities. International Conference on Business and Cyber Security (ICBCS), London, UK. The Business and Management Review, Volume 7 Number 4, 51–61.

Joint Task Force Transformation Initiative, 2011. NIST Special Publication 800-39: Managing Information Security Risk - Organization, Mission, and Information System View, Gaithersburg: National Institute of Standards and Technology.

ISO/IEC 27000: 2018. International Organization for Standardization. Information technology. Security techniques. Information security management systems. Overview and vocabulary. Retrieved on 27 January 2020 from https://www.iso.org/standard/73906.html

ISO/IEC 9001: 2015, International Organization for Standardization. THE PROCESS APPROACH IN ISO 9001:2015. Retrieved on 27 January 2020 from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso9001-2015-process-appr.pdf

ISO/IEC 9004: 2018. International Organization for Standardization. Quality management. Quality of an organization. Guidance to achieve sustained success Retrieved on 27 January 2020 from https://www.iso.org/standard/70397.htmlhttps://www.iso.org/standard/70397.html

Lehto M., 2015. Cyber Security: Analytics, Technology and Automation. Springer.

Lehto, M. & Neittaanmäki, P., 2018. The modern strategies in the cyber warfare. Cyber Security: Cyber power and technology. Berlin: Springer.

Libicki, M. C., 2007. Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York 2007.

Lillrank P., 1998. Laatuajattelu. Laadun filosofia, tekniikka ja johtaminen tietoyhteiskunnassa. Otavan Kirjapaino Oy, Keuruu, 1998.

Limnell J., Majewski K., and Salminen M., 2014. Kyberturvallisuus, Docendo Oy, Jyväskylä, 2014.

Secretariat of the Security Committee. Finland's Cyber Security Strategy. [online document], 2013. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Stouffer K., Falco J., Scarfone K., 2011. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce. [online document]. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

World Economic Forum. The Global Risks Report 2019. 14th Edition. Retrieved on 27 January 2020 from http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/#frame/20ad6

9001 quality. 2020. The Plan Do Check Act (PDCA) cycle. Retrieved on 27 January 2020 from http://9001quality.com/plan-do-check-act-pcda-iso-9001/

**Artikkeli P7:**

# Cyber Situational Awareness in Critical Infrastructure Protection

2020
Jouni Pöyhönen, University of Jyväskylä, Jyväskylä Finland,
Jyri Rajamäki, Laurea University of Applied Sciences, Espoo, Finland,
Harri Ruoslahti, Laurea University of Applied Sciences, Espoo, Finland,
Martti Lehto, University of Jyväskylä, Jyväskylä, Finland.

Article approved 2nd March 2020. Cyber Security of Critical Infrastructure 2020 (SYSEC2020) conference, October 27th - 28th 2020. Dubrovnik. Croatia.

Request a copy from author.