JYU DISSERTATIONS 562

Jussi Simola

Effects and Factors of the Hybrid Emergency Response Model in Public Protection and Disaster Relief

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 562

Jussi Simola

Effects and Factors of the Hybrid Emergency Response Model in Public Protection and Disaster Relief

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditorossa 2
syyskuun 24. päivänä 2022 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 2, on September 24, 2022 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2022

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

ISBN 978-951-39-9397-9 (PDF)
URN:ISBN:978-951-39-9397-9
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-9397-9

ABSTRACT

Simola, Jussi
Effects and Factors of the Hybrid Emergency Response Model in Public Protection and Disaster Relief
Jyväskylä: University of Jyväskylä, 2022, 106 p. (+ articles)
(JYU Dissertations
ISSN 2489-9003; 562)
ISBN 978-951-39-9397-9 (PDF)

In the future centralized hybrid emergency response model with predictive emergency response functions are necessary when the purpose is to protect the critical infrastructure (CI). Functioning Situational Awareness requires a common operational picture within Public Protection and Disaster Relief (PPDR) authorities and decision-makers. It means that a real-time information sharing link from a local level to a state-level exists. If a cyberattack interrupts electricity transmission, telecommunication networks will discontinue operating. If intrusion has not been detected, cyberattack becomes physical in urban and maritime areas. Hybrid warfare requires hybrid responses. The goal of this qualitative research was to find out the effects and factors of the Hybrid Emergency Response Model in Public Protection and Disaster Relief.

It has been assessed and defined those effects and factors that impact the development and designing process. The doctoral dissertation focuses on creating an example of a new kind of emergency response model that comprises separated public safety-related functionalities from the operational work to decision-making procedures. The proposed set of requirements and features offer needed elements that form the framework for the Early Warning Solution, which can be joined to the European Early Warning Solution.

The main results can be summarized so that fundamental human-based factors affect the whole cyber-ecosystem. Hybrid influencing can make society unstable in many ways. One of the main key aims is to influence political decision-making. The flow of reliable information among decision-makers must be ensured by using standardized Artificial Intelligence (AI) systems. The proposed system will use artificial intelligence to enhance situational awareness. Firstly, it works in smart society and uses automated or semi-automated systems. On the other hand, it supports decision-makers in their daily routine by producing relevant proposals for the decisions.

Keywords: Situational awareness, Artificial Intelligence, Information Sharing, Decision-making, Early Warning Solution, Public Protection and Disaster Relief

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Simola, Jussi
Hybridihälytysmallin vaikuttimet ja tekijät turvallisuusviranomaisten tehtävissä.
Jyväskylä: Jyväskylän yliopisto, 2022, 106 s. (+ artikkelit)
(JYU Dissertations
ISSN 2489-9003; 562)
ISBN 978-951-39-9397-9 (PDF)

Tulevaisuudessa keskitetty hybridivalmiusmalli ennakoivilla hätätilannetoiminnoilla on tarpeen kriittisen infrastruktuurin (CI) suojaamiseksi. Toimiva tilannetietoisuus edellyttää yhteistä operatiivista tilannekuvaa (PPDR) viranomaisilta ja päättäjiltä. Se tarkoittaa, että on olemassa reaaliaikainen tiedonjakoyhteys paikalliselta tasolta valtiotasolle. Jos kyberhyökkäys katkaisee sähkönsiirron, tietoliikenneverkot lakkaavat toimimasta. Jos tunkeutumista ei ole havaittu, kyberhyökkäys muuttuu fyysiseksi kaupunki- ja merialueilla. Hybridisota vaatii hybridivastuksen. Tämän kvalitatiivisen tutkimuksen tavoitteena oli selvittää Hybrid Emergency Response -hälytysmallin vaikutukset ja tekijät PPDR-palveluissa.

On arvioitu ja määritelty ne vaikutukset ja tekijät, jotka vaikuttavat kehitys- ja suunnitteluprosessiin. Väitöskirjassa keskitytään luomaan esimerkkiä uudenlaisesta hybridihälytysmallista, joka käsittää erilliset yleiseen turvallisuuteen liittyvät toiminnallisuudet operatiivisesta työstä päätöksentekomenettelyihin. Ehdotetut vaatimukset ja ominaisuudet tarjoavat tarvittavia elementtejä, jotka muodostavat puitteet Early Warning Solution eli varhaisvaroitusratkaisulle, joka voidaan liittää eurooppalaiseen EWS:ään.

Tärkeimmät tulokset voidaan tiivistää siten, että perustavanlaatuiset ihmisperäiset tekijät vaikuttavat koko kyberekosysteemiin. Hybridivaikuttaminen voi tehdä yhteiskunnasta epävakaan monin tavoin. Yksi tärkeimmistä keskeisistä tavoitteista on vaikuttaa poliittiseen päätöksentekoon. Luotettavan tiedon kulku päättäjien keskuudessa on varmistettava standardoitujen tekoälyjärjestelmien (AI) avulla. Ehdotettu järjestelmä käyttää kaksisuuntaista mallia parantaakseen tilannetietoisuutta. Ensinnäkin se toimii älykkäässä yhteiskunnassa ja käyttää automatisoituja tai puoliautomaattisia järjestelmiä. Toisaalta se tukee päättäjiä heidän päivittäisessä rutiinissaan tuottamalla asiaankuuluvia päätösehdotuksia.

Avainsanat: Tilannetietoisuus, tekoäly, tiedon jakaminen, varhaisvaroitusratkaisu, julkiset turvallisuuspalvelut

Author

Jussi Simola
Faculty of Information Technology
University of Jyväskylä
jussi.hm.simola@jyu.fi
ORCID: 0000-0002-8685-9494

Supervisors

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

Adj. Professor Jyri Rajamäki
Laurea University of Applied Sciences
Finland

Professor Pekka Neittaanmäki
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers

Professor Kirsi Helkala
Norwegian Defence Cyber Academy
Norwegian Defense University College
Norway

Professor Aki-Mauri Huhtinen
Department of Leadership and Military Pedagogy
Finnish National Defence University
Finland

Opponent

Professor Rauno Kuusisto
Information Technology Division
Finnish Defence Research Agency
Finland

ACKNOWLEDGEMENTS

It has been an honor to take part in several projects. I have had the pleasure to work with many talented teachers, such as Doctor Jyri Rajamäki from Laurea University of Applied Sciences and main supervising Professor Martti Lehto from the University of Jyväskylä. Also, Professor Pekka Neittaanmäki has supported the way of doing the doctoral thesis.

The doctoral dissertation has been done partly among EU-funded projects ECHO and MARISA. I'd like to thank for project leaders with whom I have had an opportunity to do the research work as a part of the wider community.

The prominent supporters were my parents, Anja and Heikki, who believed perseverance would be rewarded. They believed that every obstacle had a meaning.

Jyväskylä 1.8.2022
Jussi Simola

GLOSSARY

ABI	Agent-Based Intelligence
AI	Artificial Intelligence
AIS	Automatic Identification System
API	Application Program Interface
ATIX	Automated Trusted Information Exchange
C2	Control and Command Room
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CERT	Computer Emergency Response Team
COP	Common Operational (Operating) Picture
CPS	Cyber-Physical System
GPS	Global Positioning System
CSR	Case Study Research
CybOX	Structured Cyber Observable eXpression
DHS	Department of Homeland Security
DNP	Distributed Network Protocol
DoS	Denial of Service
DSiP	Distributed Systems intercommunication Protocol
DSR	Design Science Research
EC	European Commission
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations project
ECSO	The European Cyber Security Organization
ERC	Emergency Response Center
ERS	Emergency Response System
EU	European Union
EUROPOL	European Union's law enforcement agency
FBI	Federal Bureau of Investigation
FR	First Responder
GDPR	General Data Protection Regulation
HSA	Hybrid Situational Awareness
HERM	Hybrid Emergency Response Model
IA	Intelligent Agent
ICT	Information and Communications Technology
ISMS	Information Security Management System
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
IPsec	IP Secure Architecture
IPv4, IPv6	Internet Protocol version 4, Internet Protocol version 6
IRL	Integration Readiness Level
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization

ISE	Information Sharing Environment
ISI	Inter-System Interface
ISO	International Organization for Standardization
KPI	Key Performance Indicators
LAN	Local Area Networks
LTE	Long Term Evolution
MARISA	Maritime Integrate Surveillance Awareness
MAS	Multi-Agent System
M2M	Machine-to-Machine
MAV	Micro Air Vehicles
MIL	Military
ML	Machine Learning
MOBI	Mobile Object Bus Interaction
NATO	The North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center
NCI	National Council of Information Sharing and Analysis Centers
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NN	Neural Networks
PII	Personally Identifiable Information
PoC	Proof of Concept
PPDR	Public Protection and Disaster Relief
PPP	Public-Private Partnership
PSAP	Public Safety Answering Points
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SA	Situational Awareness
SC	Situation Center
SITCEN	The NATO Situation Centre
SOC	Secretary´s Operations Center
SOC	Security Operations Center
SP	Situational Picture
SSA	Shared Situational Awareness
SSI	Sensitive Security Information
STIX	Threat Information eXpression
SUPO	Finnish Security and Intelligence Service
TAXII	Trusted Automated eXchange of Indicator Information
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio
TRAFICOM	Finnish Transport and Communications Agency
TS	Top Secret
TTP/A	Time-Triggered Architecture
TTP/C	Time-Triggered Protocol
TTP	Tactics, Technics, Procedures
UN	United Nations

VHF	Very High Frequency
VIRVE	Viranomaisverkko
VPN	Virtual Private Networks
WLAN	Wireless Local Area Networks

FIGURES

TABLES

CONTENTS

LIST OF INCLUDED ARTICLES

Nine articles have been included in the dissertation:

I Simola, Jussi & Rajamäki, Jyri, (2017). "Hybrid Emergency Response Model: Improving Cyber Situational Awareness.". In Mark Scanlon & Nhien-An Le-Khac (eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security ECCWS 2017, 29 - 30 June 2017, Dublin, Ireland. (Jufo 1).

II Simola, Jussi & Rajamäki, Jyri, (2018). "Improving cyber situational awareness maritime surveillance". In Audun Jøsang (eds.) Proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS 2018, 29 - 30 June 2018, Oslo, Norway. (Jufo 1).

III Simola, Jussi & Lehto, Martti, (2019). "Effects of cyber domain in crisis management", In Tiago Cruz and Paulo Simoes (eds.) Proceedings of the 18th European Conference on Cyber Warfare and Security, 4 - 5 July 2019, Coimbra, Portugal. (Jufo 1).

IV Simola, Jussi, (2019). "Privacy Issues and Critical Infrastructure Protection". In Vladlena Benson, John Mcalaney (eds) "Emerging Cyber Threats and Cognitive Vulnerabilities." Academic Press. Elsevier. (Jufo 2).

V Simola, Jussi, Lehto, Martti & Rajamäki Jyri, (2021). "Emergency response model as a part of smart society", In ECCWS 20th European Conference on Cyber Warfare and Security, Chester, UK. (Jufo 1).

VI Simola, Jussi, (2021). "The Literature Review of Scientific Literature about Information Sharing Models". Journal of Information Warfare, Volume 20, Issue 3. (Jufo 1).

VII Simola, Jussi (2020). "Comparing Cybersecurity Information exchange models and standards for the common secure information management framework". In: Tagarev T., Atanassov K.T., Kharchenko V., Kacprzyk J. (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, vol 84. Springer. (Jufo 2).

VIII Simola, Jussi, (2021). "Enhancing the European Cyber Threat Prevention Mechanism. Journal of Information Warfare." Volume 20, Issue 1. (Jufo 1).

IX Simola Jussi, (2022). "Saving Lives in a Health Crisis Through the National Cyber Threat Prevention Mechanism Case COVID-19." In: Lehto M. and Neittaanmäki P. (eds) Computational Methods in Applied Sciences, Springer. (Jufo 2).

Authors Contribution

The author of the doctoral dissertation is the only researcher and writer of all research; so the author has the main responsibility for the articles. The role of other authors' has been more statistical and is related to the structural questions. Character A means that the candidate is the only author of the section. B means that the candidate is the principal author of the section, which means at least 90 percent participation but less than 100 percent. The author's contribution to the included articles is as follows:

Article	**IDEA**	**Role**	**Structure**	**Role**	**Data gathering**	**Role**	**Writing**	**Role**	**Conclusions**	**Role**	**Author's role**
I	X	A	X	B	X	A	X	A	X	A	MAIN A
II	X	A	X	A	X	A	X	A	X	A	ONLY A
III	X	A	X	A	X	A	X	A	X	A	ONLY A
IV	X	A	X	A	X	A	X	A	X	A	ONLY A
V	X	A	X	B	X	A	X	A	X	A	MAIN A
VI	X	A	X	A	X	A	X	A	X	A	ONLY A
VII	X	A	X	A	X	A	X	A	X	A	ONLY A
VIII	X	A	X	A	X	A	X	A	X	A	ONLY A
IX	X	A	X	A	X	A	X	A	X	A	ONLY A

The included articles cover all essential factors that impact implementing the proposed hybrid emergency response model. The contribution of the author consists of empirical research work that is a crucial unifying element in almost all cases. Articles I, II, III, V, VI and VIII were published in Jufo 1 classified conference proceedings[1]. IV, VII and IX were published in a Jufo 2 classified books. Julkaisufoorumi (Jufo) is the Finnish publication forum rating channel where peer-reviewed publications are rated between three levels: 1 = basic; 2 = leading; 3 = top. The author has been the main writer of the research. The author has written articles V, VI, VII and VIII as a cybersecurity specialist in the ECHO project.

[1]Tieteellisten seurain valtuuskunta, 2022, https://www.julkaisufoorumi.fi/fi

Other articles and public presentations

Several other studies are linked to the topic but are not included in the compilation dissertation. The results of these studies were presented and published as follows:

Article	**Place of public presentation**
J. Simola, J. Rajamäki: Common Cyber Situational Awareness: An Important Part of Modern Public Protection and Disaster Relief.	10th International Conference on Computer Engineering and Applications (CEA' 16), Barcelona, Spain, February 13-15, 2016.
J. Rajamäki, S. Sarlio-Siintola and J. Simola. "Ethics of Open-Source Intelligence Applied by Maritime Law Enforcement Authorities".	Proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS 2018. 28-29.6.2018. Oslo, Norway. (Jufo 1).
J. Rajamäki, J.Simola "How to apply privacy by design in osint and big data analytics? 18th European Conference on Cyber Warfare and Security	Proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS 2019. 4.-5.2019 Coimbra. Portugal. (Jufo 1).
J. Simola. Comparative Research of Cybersecurity Information Sharing Models official publications, scientific	An International Journal. 2019 journal-issue, DOI: 10.11610/isij.v43. Digilience 2019. Digital Transformation, Cyber Security and Resilience. Sofia, Bulgaria.
J. Simola & M. Lehto "National Cyber Threat Prevention Mechanism as a part of the E-EWS	Proceedings of the 15th International Conference on Cyber Warfare and Security ICCWS 2020. 12-13-3-2020 Norfolk, USA. (Jufo 1).

1 INTRODUCTION

There is a mutual aim in the European Union Cybersecurity Strategy and European Union Maritime Security Strategy to strengthen security through border management and enhance the standardization and interoperability of systems within western countries, including for crisis purposes (European Commission, 2020a; General Secretariat of the Council, 2014). One of the essential aims of hybrid influencing is destabilizing political decision-making in society. In practice, this leads to a need to rationalize organizational, administrative, and operative functions, as a report from Safety Investigation Authority (2017) represents. Reliable information sharing among decision-makers, intelligence authorities, and data protection authorities must be guaranteed by using artificial intelligence-aided systems. In an ideal framework, national protection of vital functions would be provided automatically as a part of the functionalities of the cyber platform, including analyzed human-based decisions of decision-makers. (Simola, Jussi, Lehto, & Rajamäki, 2021). As ongoing global Covid-19 and the crises within Russia, Belarus and Poland have shown, the cross-border crisis can spread very quickly, and the spread of misinformation sets new challenges for information sharing.

As Simola & Rajamäki (2016) demonstrates, European Public Protection and Disaster Relief (PPDR) services such as law enforcement, firefighting, emergency medical, and disaster recovery services must enhance technical systems' interoperability and cooperation between authorities. This research will be made parallel with ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations), and MARISA (Maritime Integrated Surveillance Awareness) project, which are part of the EU's Horizon 2020 research and innovation program and are situated under CISE-umbrella (Common Information Sharing Environment).

The research will also give research data to all these projects. Enhancing information exchange between public safety authorities is one of the key objectives of the research and ECHO project. European Early Warning Solution (E-EWS), as part of the ECHO purposes, has been an essential research objective for the researcher. The ECHO consortium consists of several partners from the

health, transport, manufacturing, ICT, education, research, telecom, energy, space, healthcare, defence, and civil protection sector. The ECHO and MARISA solution aims to improve decision-making and reaction capabilities with a data fusion toolkit based on various big data sources. States carry out surveillance activities, but most of the activities and threats they address are transnational in nature and crossing borders.

The critical decision-making in disaster situations has to be based on the availability, accuracy, and timeliness of the information that can be made available to the decision-makers because the importance of overall situation pictures increases at the beginning of the alarm. (Simola, Jokinen, & Rajamäki, 2015) For example, patients in the operating room within one hour of traumatic injury have a much higher survival rate. Traumatic injury is referred to as the "golden hour" (ATLS, 2008). Due to that, patient survival may be conditional that the treatment is already started at the accident scene. A human, as the rescue manager, gathers information about the incident and is responsible for decision-making at the accident scene despite the use of different decision-support systems. Understanding the happened situation is partially subjective and individual differences affect the formation of situational awareness. How can these decision-making procedures be developed? The researcher has examined the phenomena. As Simola & Rajamäki (2016) demonstrates, the PPDR authorities' operational fieldwork should be more standardized so that implementing new technology would be useful. There is a need to enhance cooperation between situation centers to create common situational awareness. Cyber situational awareness is an essential capability in emergency and crisis management because the scene of the incident will increasingly often be a cyber-physical system.

Due to increased cyber threats, authorities need to respond to growing challenges despite formal stability in Europe. As terrorism, hybrid warfare, and major accidents have shown, preparation for different kinds of threats challenges critical infrastructure protection. Public Protection and Disaster Relief (PPDR) authorities and politicians have noticed the importance of a mutual understanding and shared situational awareness in their preparation plans. Cyber situational awareness is an essential part of situational awareness, which concerns the "cyber" environment (Simola & Rajamäki 2016). Therefore, a combination of (hybrid) threats needs hybrid response models to fight against them.

If we think about the hybrid threats, it is crucial to take into account the cyber domain. It is not enough that we create a real-time picture from the accident site only with real-time video solutions. We need a predictive or at least proactive way to gather and share information between public safety workers and decision-makers. The connection between local, regional, and central government must exist enhancing for overall situational awareness. In addition to this, information sharing-connection must exist between the EU countries within the western world. It is not enough that the separate operative emergency response units do their work in a closed loop. Personnel in situation centers and

emergency response centers, as well as regional and central administration, need to be updated situational picture and common operating picture from the major accident. It is possible only with automated and artificial intelligence-aided solutions. The state is that because we have several public safety-related organizations. The cost of the inefficiency of multi-layered public organizations is not optimal base when creating a common situational awareness system for public safety actors.

The highest state decision-makers, such as members of the Finnish government or the highest officers may use the results of this doctoral dissertation. The new intelligence legislation package by the Finnish government includes provisions on the principles of intelligence activities. It enhances the ability of the PPDR authorities to respond to cross-border hybrid threats because it allows the use of new decision support system technologies. Because of this also legal, ethical, and societal dimensions must be taken into consideration.

The doctoral research closely concerns the ongoing research area of Cyber security of Critical Infrastructure Protection (CIP) in the Faculty of Information Technology at the University of Jyväskylä. The research focuses on enhancing situational awareness within public safety authorities from local to national and international levels by using a Cyber-Physical System (CPS).

After the introduction and central concepts, Chapter 2 provides the theoretical background of the research, including applied methods and research processes. Chapter 3 summarize the paper contents. Chapter 4 consists discussion of the conclusions.

The primary purpose of the research is to design a smart hybrid emergency response -model that consists of hybrid-threat prevention mechanisms and information sharing practices. It is based on intelligent emergency management architecture by utilizing a design science research framework. The purpose is also to find out local, regional, national, and transnational (international) level organizational factors that affect the utilization of the system. The doctoral dissertation defines the set of (system) requirements for the system development and how does the operating environment affect the designing process and what are those essential factors affect its design and implementation?

2 BACKGROUND OF THE RESEARCH

This research focuses on enhancing situational awareness within public safety authorities from local to transnational macro level in the cyber-ecosystem by using the cyber-physical system. The research aims to design an emergency response system for critical infrastructure protection. The solution will strengthen security through border management and enhance standardization and interoperability of systems, including emergency purposes.

2.1 Relevance of the research topic

There is a need to understand how public safety authorities can act in a preventive manner so that a potential accident or offense can be prevented. In addition, decision-makers like government politicians must receive the correct information in real-time. At present, the main problem in the emergency procedures is that PPDR authorities react to national and cross-border threats mainly after threats are realized. Decision support technology is not utilized enough to replace human labor. Separate emergency response functions, procedures and methods are losing available resources. There is also a need at the EU level to strengthen information exchange to optimize the surveillance of the European borders, including the EU maritime area and its maritime borders. There is a need to utilize real-time data from fairways and vessels in Maritime Rescue Coordination Centre (Simola, J. & Rajamäki, 2018). It is important to note that The Coast Guard promotes the maritime environment's protection and covers 1250 km of territorial waters (Kaukanen & Möttönen, 2010).

The developed Hybrid Emergency Response -model is one kind of concept which can also cover the Finnish maritime environment. Firstly, it will generate and gather essential data from the environment and combine data into an understandable form that first responders and rescue units may begin their rescue operations while the AI-aided automated systems have been activated.

The study aims to develop a DSS system that helps to improve the situational awareness level of critical infrastructure by inspecting cybersecurity threats. Coordinated hybrid responses are required to tackle hybrid threats. Therefore, also a cyber situational picture is an essential element. As I have examined in the study, human beings have limited observation capabilities to react always without errors (Simola, Jussi, 2015). Physical components, hardware, and software together form the base for modern intelligence infrastructures. These integrated systems are examples of cyber-physical systems (CPS) that integrate computing and communication capabilities to monitor and control entities in the physical world. FIGURE 1 presents a CPS that consists of a cyber layer between two physical layers (platform layer and human layer).

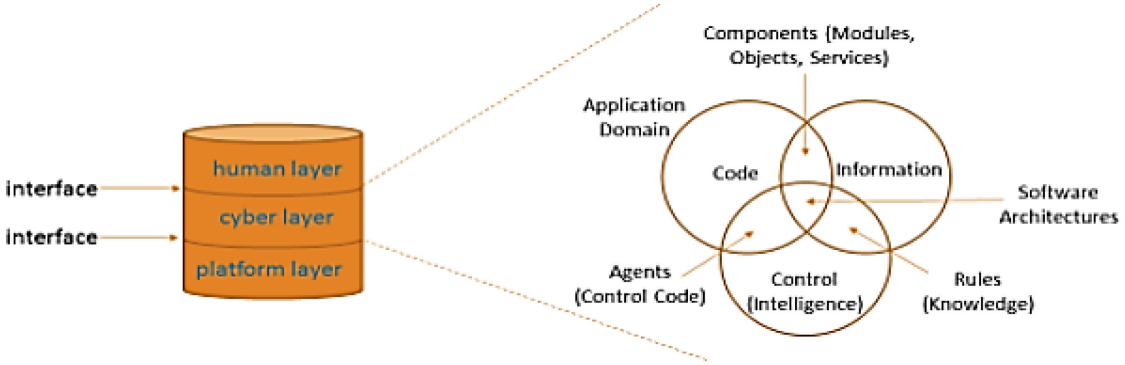


FIGURE 1 Layers of cyber-physical system modified from (Hevner & Chatterjee, 2010)

Internal and external security can no longer be separated traditionally. This trend forces us to think about overall security differently. A dynamic and efficient cyber-physical ecosystem and infrastructure are essential development areas to respond to rapidly evolving alerts—ineffective and separate management of public safety organizations causes harm to continuity management. (Simola & Rajamäki, 2017) Different threat types create combined threats, therefore public safety organizations must prepare to prevent new kinds of hybrid threats and respond to them by enhancing the information sharing between the public sector, private sector, volunteer associations, and citizens. The evolving threat must be able to prevent and respond faster. It is essential to decompose organizational structures to model next-generation emergency response systems into other environments when creating expanded utilization of systems.

There are some challenging privacy issues concerning legislative acts. Despite the legislative possibilities of using new innovative technology, criminality and hybrid threats become more difficult to manage without cooperation. A modeling platform for an intelligent emergency response model can lead to significant new results in improved public safety. The cyber domain produces potential added value by enhancing information sharing and data fusion for more accurate overall (hybrid) situational awareness where physical and cyber situational awareness is combined. Processing raw data of anomaly behavior in advance, PPDR authorities can use intelligence emergency response functions before any threats have occurred (Simola & Rajamäki, 2017). The

governance structure of the state PPDR organizations and the political power and responsibility concerning the rapid response of the security authorities are significant factors when the emergency response functions are being automated. The technical development and structural changes within the public sector influence public sector employees' work processes continuously. How can state administrative functions be rationalized regarding emergency response functions in crises without compromising rescue operations and overall security?

In order to do that, we can design something new, and we need insight into the framework of the compilation dissertation. This research project consists of several studies that produce knowledge for the development work of the next generation emergency response model, which is designed to work in two ways to support decision-making. Firstly, it will generate and gather essential data from the environment and combine it to an understandable form that public safety officials and rescue units may begin their operative fieldwork while the AI-aided automated systems have been activated. Secondly, it will share relevant data by using physical- and cyber sensors for the decision-makers in a preventive way. The system will offer alternative outputs for the base of the decisions. The research will not develop or design the finished product. It will provide a proposal of the framework that is based on cross-case analyzed case study research.

The second part of this research project is a continuum to my master´s thesis (Simola, 2015) which handled mainly the formation of situational awareness and information sharing from the micro-level to the situation centers by using a real-time video solution. The first part concentrated on applications, devices, techniques, telecommunication solutions, and routers that are central equipment to use in communication in the rescue process at an accident site. The solution was tested in an authentic simulation context at the Pori camp.

The doctoral dissertation, in other words, the second part defines the set of (system) requirements for the system development and how does the operating environment affect the designing process and what are those essential factors affect its design and implementation? Essential is also how the proposed system affects public safety authorities' operating environment. In this dissertation, the Empirical section of Public Protection and Disaster Relief consists of a regional Emergency Response center, Law Enforcement (Southwestern Finland Police Department and the Border Guard in the Southwest region of Finland), Emergency Services (including rescue, safety, and emergency care), Hospital District (Emergency Medical Services). Regional Command and Control functions of the Defence Forces have been excluded from the closer survey due to the secrecy aspect. It must be noticed that the researcher has conducted an empirical study without fieldwork assistance. The research would have taken too many resources in this context, and the investigation would have become challenging to manage. Therefore, the Command and Control functions of the Defence Forces should be investigated in the future. The Defence forces have been involved in the research at a general level, and it is intended to be taken into account more thoroughly in further studies.

As mentioned above, the formation of situational awareness is the central concept in this doctoral dissertation. It has been examined how situational awareness forms among public safety units and workers and what are the crucial user needs for enhancing the formation of situational awareness at the accident site. We need data and processed information when the purpose is to keep the preparedness level high enough, and that data has to share in real-time within and among public safety organizations and decision-makers. Shared situational awareness and shared situational picture mean that the same information is simultaneously usable with all participants, including cyber situational awareness. The shared information must be understood in the same way. Public safety organizations need standardized procedures to keep situational awareness at the same level at every administrative stage, not forgetting information sharing between the western countries. The commission of the European Union is trying to create a platform that collects different countries under the cyber-security umbrella fighting against cross-border threats like hybrid threats. The ECHO project is one example that focuses on creating collaborative European early warning solutions for that kind of threat. Despite the research done as a part of the ECHO project, the research has been a separate project offering data for the ECHO designers and architects.

2.2 Research objective, method, and process

2.2.1 Research questions

In current practice, public safety authorities' operational work does not utilize the cyber domain widely and efficiently enough. The problem is that public administration has separately operating cybersecurity organizations with their administrations and responsible organizations of cybersecurity operations are separated from emergency services, including official public actors. For example, they hardly do not share cyber threat-related information at all, or the information does not reach the recipient. Under the administrative umbrella of (Finnish Transport and Communications Agency) TRAFICOM, The National Cyber Security Centre Finland (NSCS-FI) generate information on Cyberthreats as vulnerabilities for stakeholders, but the data is not shared with emergency response centers or situation centers. Organizations that operate their cybersecurity functions independently and utilize different information-sharing methods and procedures prevent effective coordinated responses to cyber-physical threats. Also, human-based weaknesses affect efficient information sharing, e.g., verbal communication problems and written problems by email are very common.

New systems may be out of date when they are introduced. Cybersecurity challenges also concern maritime areas, including fairways and ports. For example, the growing importance of maritime traffic in cross-border trade has created a need to develop new technologies for accident prevention (Simola &

Rajamäki, 2018). The busiest shipping lanes in the Baltic Sea carry an average of more than 100 vessels a day, and approximately 2,500 commercial vessels operate continuously in the Baltic Sea (Ojala & al., 2018). Maritime safety is also a matter of concern for continuity management. Traditional automatic ship alarm systems, coastal radars, and coastal cameras are not enough sufficient equipment to build maritime awareness. A lot of communication equipment uses a vulnerable technical structure. Internationally utilized AIS tracking system is highly vulnerable to hacking. If transponders send false position signals or do not work at all, a major maritime traffic problem arises (Simola & Rajamäki, 2018).

Combining Artificial Intelligence-based solutions, Open-Source Intelligence (OSINT) data from social media, Signals Intelligence data (SIGINT) (Morrow & Odierno, 2012) and traditional intelligence sources as Human Intelligence (HUMINT), overall situational awareness arises. A cyber situational picture is needed because hybrid threats need coordinated hybrid responses.

The research comprises one main research question and five sub-research questions. The main research question (RQ) is

RQ How do elements of the cyber ecosystem impact (in) traditional Public Protection and Disaster Relief?

The sub-questions are

RQ1 How to improve cyber preparedness level within PPDR authorities from local to national and international level as a part of PPDR services?
RQ2 How to improve and combine emergency response procedures by using the cyber dimension?
RQ3 How do intelligent technologies affect to PPDR -organizations and central government?
RQ4 How hybrid emergency response model affects maritime security?

RQ5 What are the main obstacles to the implementation of the new system?

The answer to all these research questions is sought through design science research guidelines.

2.2.2 Design Science Research with a case study approach

Identified problems that have been mentioned above lead to the DSR methodology selection. DSR allows to development of constructive solutions that solve the problem that has been found.

As Hevner & Chatterjee (2010) demonstrates, the DSR method requires a knowledge base and understanding of the environment and its business needs. The compilation dissertation consists of several cases that form the bases for designing and evaluating the artifact as a part of the Relevance Cycle. The used Hevner's conceptual framework combines the behavioral science and design science paradigms. Hevner & et al. (2010) refers to seven guidelines and criteria for the design that are listed below:

TABLE 1 Seven guidelines from Hevner & Chatterjee (2010)

I.	Design as an artifact	Guideline Design research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation
II.	Problem Relevance	Design research aims to develop technology-oriented solutions for relevant business problems.
III.	Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation plans.
IV.	Research Contributions	Effective design research must provide clear and verifiable contributions in the design artifact, design foundations and/or design methodologies.
V.	Research Rigor	Design research relies on the design application of rigorous methods in both the construction and evaluation of the design artifact.
VI.	Design as a Search Process	The search for an effective artifact requires utilizing the available means to reach desired ends while satisfying laws in the problem environment.
VII.	Communication of Research	Design research must be presented effectively to both technology-oriented as well as management-oriented audiences.

2.2.3 Design Science Research approach with a case study evaluation

As FIGURE 2 illustrates, the Information Systems research framework focuses on three inherent research cycles as follows; The Relevance Cycle links the research project´s contextual environment with the design science activities. The Rigor Cycle connects the design science activities with the knowledge base of scientific foundations, experience, and expertise that informs the research project. The central Design Cycle iterates between the core activities of building and evaluating the design artifacts and processes of the research. These three cycles above have to be clearly illustrated in a design science research project. The following sections briefly expand on the definitions and meanings of each cycle (Hevner, 2007). The selected cases that are included in the relevance cycle form the primary artifact. The case studies are used in the evaluation process in this dissertation.

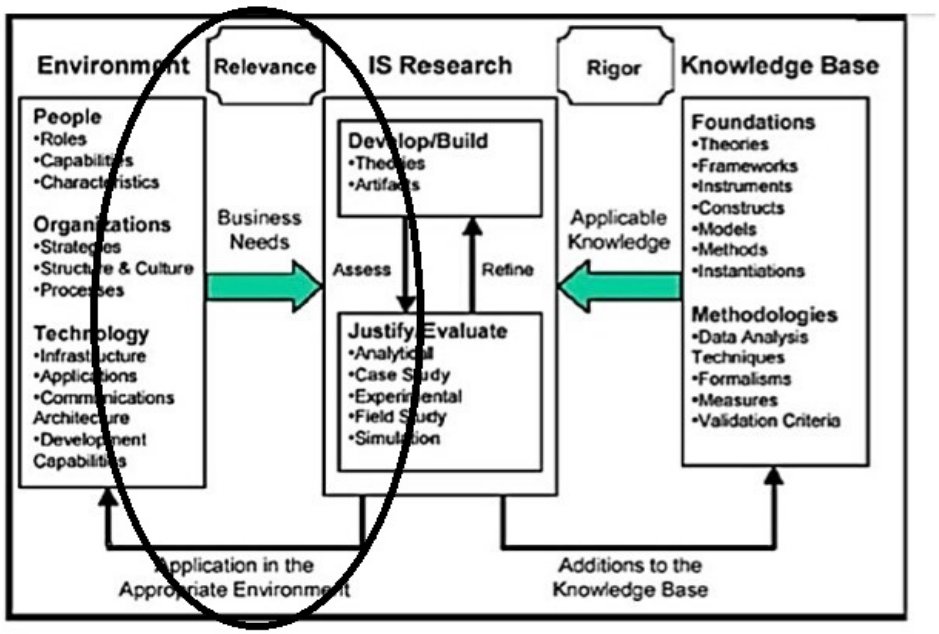


FIGURE 2 Design Science Research Cycle modified from (Hevner & Chatterjee, 2010)

Nunamaker & al. (1991) presents a systems development framework via five steps: conceptual design, constructing the system's architecture, analyzing the design, prototyping (may include product development), and evaluation.

Regardless of sources for the methods and methodology, it is easy to create a base for understanding that elements of the construct are almost equal. A basic ethnographic understanding of the PPDR working environment forms the researcher´s living area. The researcher has grown up within the culture of PPDR authorities. In this dissertation, part of the DSR cycle titled Environment consists of the specific empirical part, including observation and interviews in selected four situation centers in Turku.

A knowledge base has been accumulated from data, theories, methods, and previous findings. This ongoing cycle redesign proposed a system by applicable knowledge and business needs.

Design science research cycles, as FIGURE 3 illustrates, are an essential part of the designing process. In this research, case studies are situated in the relevance cycle. It provides the defined acceptance criteria for the evaluation process. The evolving relevance cycle is connected to the design science cycle producing the primary artifact. It defines acceptance criteria for the ultimate evaluation of the research results. In this study, the artifact is named the Hybrid Emergency Response Model (HERM). Design science absorbs a knowledge base of scientific theories and engineering methods that offers the foundations for rigorous design science research (Hevner & Chatterjee 2010).

The rigor cycle offers past knowledge to the research project to make certain its innovative bases. Researchers have to accurately research and reference the knowledge base (KB) to ensure that the produced designs are research

contributions instead of that designs based on the application of known design processes and the reproduction of known and existing design artifacts. (Hevner 2007). According to Hevner & Chatterjee (2010)

1. The middle design cycle is the central point in the design science research project, as FIGURE 3 presents
2. The requirements are input from the relevance cycle
3. The design and evaluation theories and methods are attached from the rigor cycle to the design cycle

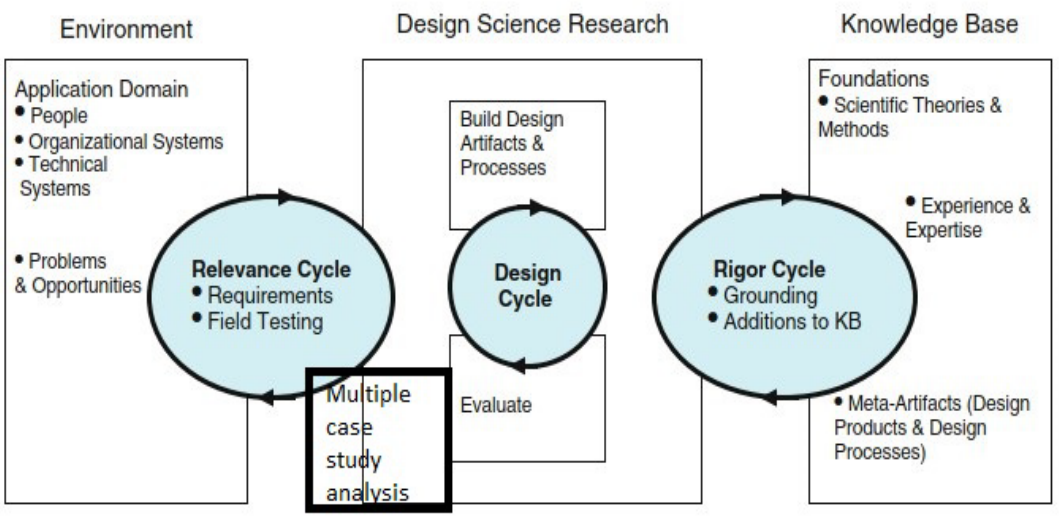


FIGURE 3 Modified DSR cycles from (Hevner, 2007)

2.2.4 Case studies within the relevance cycle

When the purpose is to create a mindmap about the coherent wholeness of the research subject, the empirical research helps to understand PPDR authorities' working culture and entity. A case study research strategy enables the investigation of the interaction between the different factors. Theory building, experimentation, observation, and systems development create four case study research strategies in the applied multimethodological approach (Nunamaker, Minder Chen, & Purdin, 1991).

Yin (2014) determinates five points of research design for case studies as follows: (1) the questions of the study; (2) its propositions if any; (3) its unit(s) of analysis; (4) the logic linking the data to the propositions; and (5) the criteria for interpreting the findings. The multiple-case study approach is used in this dissertation; the used method is well known and explained well in references (Benbasat, Goldstein, & Mead, 1987; Kananen, 2013; Miles & Huberman, 1994; Yin, R. K., 2014).

Concerning Ojasalo et al.'s (2009) illustrates case study produces essential information about the research object by enabling the understanding of the development of holistic items in a realistic operational environment.

The analyzing unit comprises the PPDR emergency services and how different artificial intelligence-based threat detection systems may affect the formation of situational awareness at local, regional, state and international levels. In summary, the unit of analysis is the enhanced formation of a hybrid situational awareness at the command and situation centers.

The research material was collected through a combination of several sources and was analyzed with several methods. In order to achieve triangulation, data was gathered from multiple sources. Participating in observation, semi-structured interviews, scientific publications, collected articles and literary materials create the sources. The collecting and analysis of the research material will be carried out based on the theoretical framework. Usually used four triangulation types in evaluation: triangulation of data sources, triangulation among different evaluators, triangulation of perspectives and triangulation of methods (Kananen, 2013; Patton, 2002; Yin, 2014). All of these triangulation types were used.

It is also essential to understand the operative culture of working groups. For example, how do they share information, what they share, and with whom? As Hughes et al. (1993) stated, in system use and system design, a researcher´s participation in the social life as an ethnographic observer means emphasizing studying the functionalities of a technological system as they evolve from their incorporation into the socially organized work activities of those who use them.

2.2.5 Selected studies

The research area consists of several studies and without a selection process, research expands too much. The selected research allows the creation of coherent proportionate wholeness. TABLE 2 consists of selected articles for the dissertation. The research topic consists of eighteen sub-research, of which nine were selected as the body of the compilation dissertation.

The unit of analysis comprises three sections: The PPDR emergency services include situation and command & control centers. Data & Telecommunications consist of equipment and technical features. In summary, the primary unit of analysis is the enhanced formation of a hybrid situational awareness in the CPS selected PPDR environment, as TABLE 3 demonstrates. TABLE 4 demonstrates each sub-artifacts that move toward the proposed Hybrid Emergency Response Model.

TABLE 2 Selected case studies

Article	Type of the research	The Subject of the research	Research methods	Empirical data collection and analyzing methods
I	Conference paper	Hybrid Emergency Response Model: Improving Cyber Situational Awareness	Interviews, participant observation, literature	Qualitative data analysis and collection method by triangulation
II	Conference paper	Improving cyber situational awareness in maritime surveillance	Interviews, participant observation, literature	Qualitative data analysis and collection method by triangulation
III	Conference paper	Effects of Cyber Domain in Crisis Management	Interviews, participant observation, literature	Qualitative & quantitative data analysis and collection method by triangulation
IV	Chapter of the book	Privacy issues and critical infrastructure protection	Official publications, scientific articles, and literary	Qualitative data analysis and collection method by triangulation
V	Conference paper	Emergency Response model as a Part of the Smart Society	Official publications, scientific articles, and literary	Qualitative & quantitative data analysis and collection method by triangulation
VI	Journal article	Literature Review of the Scientific Articles about the Cyber Information Sharing	Official publications, scientific articles, and literary	Qualitative & quantitative, triangulation data collection method
VII	Chapter of the book	Comparing Cybersecurity Information Exchange Models and Standards for the Common Secure Information Management Framework	Official publications, scientific articles, and literary	Qualitative data analysis and collection method by triangulation
VIII	Journal article	Enhancing The European Cyber Threat Prevention Mechanism	Official publications, scientific articles, and literary	Qualitative data analysis and collection method by triangulation
IX	Chapter of the book	Saving Lives in a Health Crisis Through the National Cyber Threat Prevention Mechanism Case COVID-19	Official publications, scientific articles, and literary	Qualitative data analysis and collection method by triangulation

TABLE 3 Unit of analysis

Study	**Unit of Analysis**			**Viewpoint**
	Data & Tele Communications	Formation of Hybrid SA in CPS environment	Situation Centers, C2, SOCs, CERTs	
I	X	X	X	Operational environment-formation of situational awareness between C2
II	X	X	X	Operational environment-Situational awareness in maritime
III	x	X	X	Organizational responsibilities
IV	X	X	X	Privacy Issues in the context of using CPS (HERM)
V	X	X		technological-related fundamental risk impacts in CI
VI		X		Cyber Information sharing models and frameworks
VII		X		CPS and Risk Management system-comparing sharing methods and standards
VIII		X	X	National Early Warning System into the EU EWS-interoperability requirements
IX		X	X	CPS-HERM-decision making and crisis management

TABLE 4 Evolving design science process

Study	Artifact
I	Hybrid Emergency Response Model (CPS) – initial technical version
II	Hybrid Emergency Response Model (CPS) – maritime model
III	Hybrid Emergency Response Model (CPS)– the model of comparison, development needs
VI	Hybrid Emergency Response Model (CPS) – Privacy issues model
V	Hybrid Emergency Response Model (CPS) – continuity risk assessment management
VI	CPS – Features for the Cyber Information sharing
VII	CPS – Combined Continuous Risk Management model
VIII	CPS- Cross border EWS information-sharing model
IX	HERM (CPS) - Combined RIDM and CRM with AI elements
Cross-case conclusion	Proposal for the Hybrid Emergency Response Model, that enhances the formation of Situational Awareness among PPDR services.

2.2.6 Cross-case analysis and relationships between the cases

As mentioned above in TABLE 2, the research comprises different case studies that examine phenomena of the formation of situational awareness and how to develop operating procedures and processes by enhancing information sharing. The ability to gather and share information and the formation of situational awareness are linked to each other. The selected phenomena, the formation of the (cyber) situational awareness between and within public safety actors at the micro and macro level, require a broader understanding of the culture where they work daily. Due to that, the case strategy creates a usable framework to investigate information sharing comprehensively enough.

In addition, the cross-case analysis will produce a set of system requirements and features to support a model that promotes information sharing among European ECHO stakeholders. The doctoral thesis also creates a knowledge base for their purpose.

It is possible to divide selected cases into two main groups. Articles I-V present different kinds of operational environment aspects that affect to the designed hybrid emergency response model and fundamental factors that affect the implementation process. Articles VI, VII, VIII, and use case in article IX examine cyber threat information sharing models, standards, and frameworks that can use the transnational cyber-threat information sharing process as a part of the proposed Early Warning Solution HERM.

FIGURE 4 demonstrates the formation of a multiple-case study analysis. An ongoing process stopped when crucial data for the main research question was received, and the content of the problem formulation was saturated.

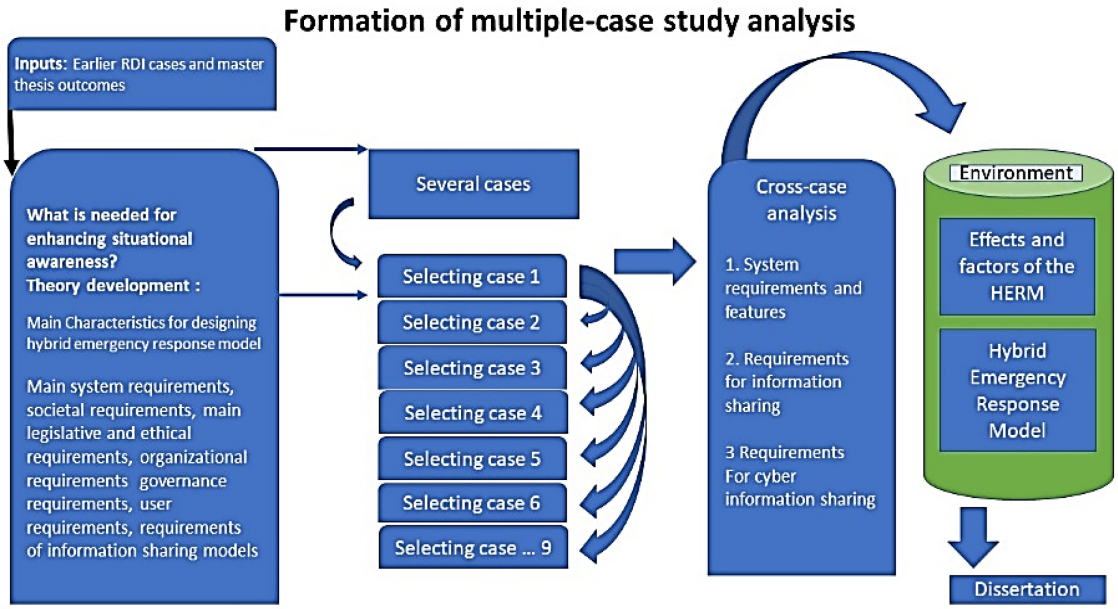


FIGURE 4 Formation of the cross-case analysis of the research

2.2.7 Relationships of the included studies

Articles are connected to each other so that the developing process is ongoing, iterative, and evolving. Article I proposes the first version of the architecture for the next-generation Emergency Response Model.

The paper describes technical examples for multi-sensor data fusion mechanisms in a cyber-physical domain and the required elements for a situational awareness system with suggestions for solving information sharing and the early warning problem. Four regional situation centers were examined by author participant observation; several professionals were interviewed. The proposed model sets ground-level knowledge for the following studies. The figure above illustrates the relationships between the articles.

Article II utilizes Hybrid Emergency Response Model in Maritime Environment. It concentrates on the daily routine and information sharing procedures in the situation and command center of The West Finland Coast Guard District called the Command and Maritime Rescue Coordination Centre (MRCC Turku). Article proposes the crucial elements for enhancing situational awareness and maritime hybrid threats detection. The research has been done in parallel with the MARISA project.

Article III handles the main factors that affect the implementation of the next-generation hybrid emergency response model with early warning features. Article suggests solving the development needs-related problems through technical, organizational, and structural choices. By comparing current emergency response processes to the proposed Smart hybrid emergency process model, effects and factors can be found that prevent the implementation of the proposed architecture.

Article IV concentrates on how privacy issues affect information sharing in the smart city context where citizens use different devices. Hybrid Emergency Response Model is one kind of Early Warning Solution, and its proposed features are linked to privacy-related data handling and information sharing. The research focused on factors that reflect the privacy-related need for a developing standardized hybrid emergency response model.

Article V seeks to identify technological risk factors and scenarios that expose vital functions of society to hybrid threats and dangers. Fundamental level risk factors that influence decision-making in society have to be identified. These threats affect critical infrastructure protection and prevent the detection of threats.

Article VI, the literature review presents important scientific articles and official materials about cyber information sharing models. The findings are discussed from the perspective of how to develop a cybersecurity information sharing system and what possible features might be included in the system.

Article VII handles similarity and dissimilarity factors regarding the essential cyber information sharing models and information management frameworks in European countries and the U.S. It will survey essential factors that affect deploying a common Early Warning System for the ECHO partners. This research aims to help other collaborators of the European ECHO Early Warning Solution and end-users by comprising valuable data for the Echo Early Warning System concept. In addition to this, the research provides data about features of existing information-sharing models and frameworks to identify and consider territorial, organizational, managerial, legal and societal dimensions. E-EWS tool will enhance coordination and information exchange in near-real-time between the members of the ECHO network. The research's sub-question handle possibilities to link US-related cyber information-sharing models to the European operational information-sharing procedures.

Article VIII explores those factors (requirements) which affect the conversion of a national EWS to a common early warning ecosystem at the EU level. A way of implementing the national cyber threat prevention system into the EU-level Early Warning System is determined in paper VIII.

Article IX concentrates on trusted information sharing and how it is possible to enhance decision-making in the context of hybrid threats by using the Hybrid Emergency Response model. The purpose was to analyze pandemic-related management procedures and occurred information-sharing challenges and risks, along with the formation of situational awareness, from the view of continuity management.

Articles V, VI, VII, and VIII belong to the European network of Cybersecurity centres and competence Hub for innovation and Operations project (ECHO) and are made in a project-worker role as a cyber security expert. Articles VI, VII, and VIII focus on information sharing mechanisms, models, and frameworks, and article IV concentrates on privacy aspects when utilizing the Hybrid Emergency Response Model. The FIGURE 5 above demonstrates how these papers are connected to each other. It is essential to notice that this is

evolving, ongoing iterative DSR (Relevance Cycle) process. Several studies may define added requirements for the subject set of requirements specifications under review.

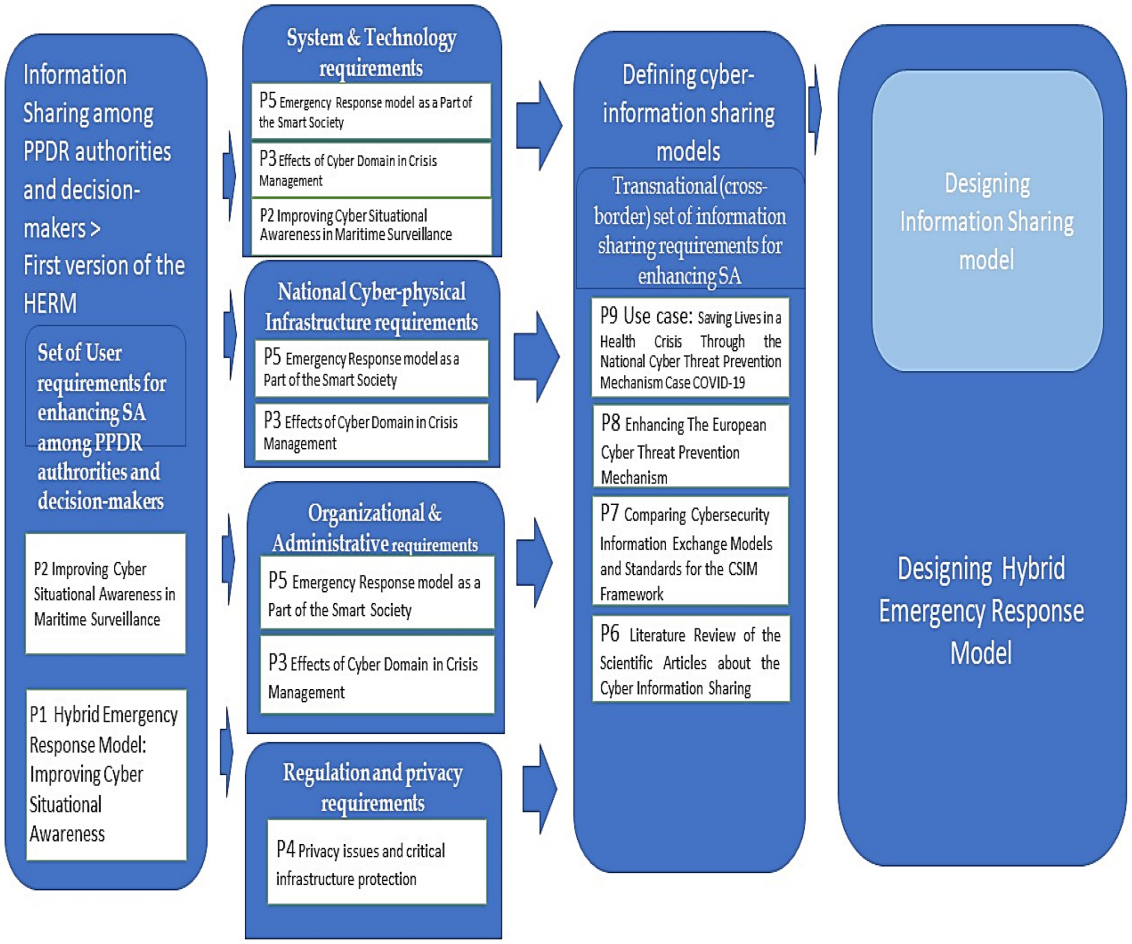


FIGURE 5 Relationships of the included papers

3 THEORETICAL BACKGROUND

This chapter handles the theoretical background, the context for the dissertation and central concepts.

When something alarming happens incidentally, it is crucial to quickly recover changes in the operational environment back to the initial state. Critically injured patients must be transferred from the accident scene to the surgical table within one hour (Lerner & Moscati, 2001). Sixty minutes is not a long time. How would it be possible to do something more to make the emergency procedures more efficient, from the first alarm to the medical first responders' arrival? There is a need to enhance information sharing from the accident site to the hospital and design information systems that generate essential data before any incidents or events occur (Simola, 2015).

From the research stated above, work has continued towards the cyber domain. The cyber domain is a crucial element in combating cyber-physical threats or hybrid threats. It is not enough to focus on the realized physical threats and the treatment of traces. The essential issue is how to react before the incident, or significant accident is realized as a physical event.

3.1 Decision-making procedures

It is said that the kitchen needs only one good cook. We live in a political environment where efficient decision-making is based on advising reports produced by advisory organizations and agencies. Those generate information for the decision-makers, but these agencies do not perform real-time operative functions that play a role in emergencies. Thus, there is a need to develop decision-making procedures that can generate and maintain situational awareness in a way that allows emergency workers to act before an incident or major accident.

Misinformation causes problems in information sharing and exchange practices, and human errors may lead decision-makers as authorities or public safety workers to the incorrect decision-making process. Harmful decisions cause extra work, harm, and cost. In the worst case, resources cannot be recovered after human error. Artificial Intelligence aided automated political procedures or processes are not a reality yet because of the legitimacy basis. The political system is in the society, but artificial solutions may support decision-makers in their daily routine. Hidden threats are threats that are not visible. Therefore fundamental threats must be eliminated.

3.2 Cyberspace in the critical infrastructure environment

Understanding cyber and hybrid threats is essential for public safety organizations, such as situation centers and emergency response centers. Small and medium-sized enterprises, as well as big enterprises, may face surprising problems when collaborating with public safety sector actors. Hybrid threats put pressure on the categorized threat classes. The cyber security domain is an essential element in the future world where the intelligent cyber ecosystem is almost everywhere. Public places and spaces will consist more technical solutions connected to each other and other environments. Technical physical and cyber layers serve a common purpose in protecting the urban environment. Citizens use mobile phones, computers, and tablets everywhere. Public broadband telecommunication systems and networks with limited data transmission capacity are often overloaded when something unexpected happens due to people having to call and share urgent information with each other at the same time. Automated predictive digitalized sensor systems create an opportunity to react faster against incidents.

Every nation has its weaknesses in infrastructure. Functioning societal functions and infrastructure are essential elements in a digitalized environment. It is not clear which sectors of society are included under the title "critical infrastructure" or what functions are included in "vital functions". Vital Functions and Critical infrastructure differ, but I do not see a need to separate them because of their fixed connections. The Cybersecurity &Infrastructure Security Agency (CISA) of the U.S. has been included 16 critical infrastructure sectors in it (Department of Homeland Security, 2013).

3.3 Human factors

What do human factors mean in this context? Defining human factors is not simple, but in this context, human as a factor means that humans affect events around you and what is happening in an emergency situation. The human may be the first cause of the incident. We have limited capacity to observe changes in

situations without making mistakes. Opposite to the human factor is the power of nature. An unexpected event may occur out of view if we don't have any technological solution to forecast it. For example, a tsunami is that kind of phenomenon. If we have some way to forecast tsunamis and we miss monitoring sensors and emergency systems, then the consequence of disaster may change as part of the human-made fault, but not directly human-made.

When the purpose is to enhance critical infrastructure protection, the crucial subject of the review is related to reducing possibilities to human-based faults and mistakes.

As M. Endsley (1995) argues, environmental and individual factors affect the formation of situational awareness; in addition to this, human capabilities vary between individuals. FIGURE 6 as follows, illustrates relationships between the concepts of Situational Awareness from Critical Infrastructure Protection to a Common Operating Picture. For a common situational understanding (CSA) or COP, possible similar mental models of individuals require the same "understanding" of the state. In other words, mental models of individuals have to be in the same state of "understanding in the group." Also, technical interfaces have to have understood each other, and the same data must be available at all levels. The difference between common situational awareness and shared situational awareness is not significant, but I have used the term "common situational awareness" to mean ongoing maintaining cyber- and the physical situational understanding in a specific group. Shared SA does not mean that shared elements for the basis of the decision are processed and concluded in the same way for the decisions; the base for the decisions is available with the same contents from the sources. Common Situational Awareness includes a more decision-oriented view and means a common decision-making process with automated decision-support elements. Common Operating or Operation Picture (COP) is connected to the specific and realized incident lifecycle.

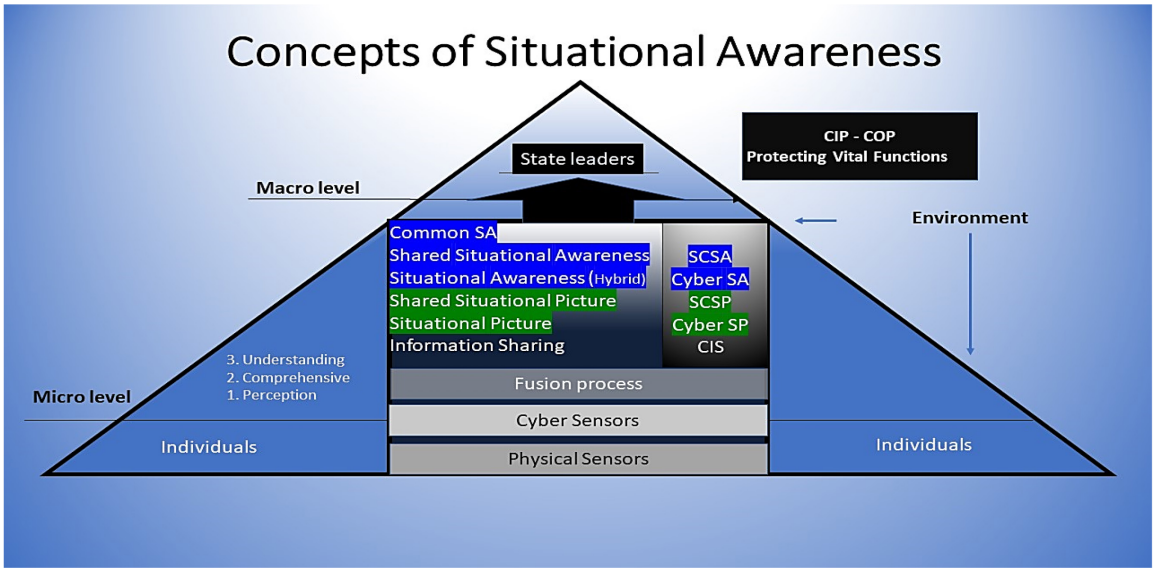


FIGURE 6 Simplistic concepts of Situational awareness (Hybrid Situational Awareness)

According to Endsley (Endsley, 2015), automatized systems may change our capabilities to observe our environment faster. Enhancing SA, predictive and preventive elements help to create a broad knowledge about the situation around us. It is essential to analyze what is to the right stage for the autonomous and intelligence systems.

Multiagent-aided intelligence creates possibilities that cannot be achieved by human cooperation. Efficiency, memory capacity, and tireless working capabilities create differences between humans and multi-agent intelligence-based systems (Wooldridge, 2009).

3.4 Central concepts

3.4.1 Artificial intelligence and intelligent multi-agent systems

As a part of the information system, Artificial Intelligence (AI) displays intelligent behavior by analyzing the environment and taking multiple autonomous actions to obtain defined aims (European Commission, 2020b). Software-based AI systems can act in the virtual world (e.g., image analysis software, search engines, shape, and face recognition systems), or AI can be attached to hardware devices (e.g., advanced robots, autonomous cars, vehicles, drones, and Internet of Things applications) (European Commission, 2020).

An Intelligent Agent (IA) is an entity that produces decisions that allow performing specific tasks for users or applications while learning while completing tasks. Perception and action are the main functions of the IA. Intelligent Agents form the hierarchical structure that comprises different levels of agents. Multi-agent system comprises several agents that interact with one another (Wooldridge, 2009). That combination may solve challenging problems in society. An agent may behave in three ways: re-actively, proactive, and socially (Wooldridge, 2009).

3.4.2 Public Protection & Disaster Relief Services

Public Protection means critical public services that provide primary law enforcement, firefighting, emergency medical, and disaster recovery services for the citizens of the political subdivision of each country. These public safety workers help protect and preserve life and property (Baldini, 2010). Disaster Relief means responding to the severe threats that cause a significant widespread threat to human life, health, property, or the environment. Public Safety and Disaster Response within certain regions can also be construed as PPDR. PPDR also consists of the military (MIL) and critical infrastructure protection (CIP) (Baldini, 2010). The Emergency Response Centre Administration provides emergency response center services throughout Finland. The Emergency Response Centres handles emergency calls from all over the country for the

rescue, police and social and health services, and the Maritime Rescue Coordination Centre (MRCC) handles emergency calls from the sea area.
They manage communications regarding the safety of people, property, and the environment and share the received information to the appropriate assisting authorities or partners such as situation centers (NENA, 2018; Ministry of Interior, 2010).

In this dissertation, Public Protection and Disaster Relief consist of a regional Emergency Response center, Law Enforcement (Southwestern Finland Police Department and the Coast Guard (MRCC) in the Southwest region of Finland), Southwest Finland Emergency Services (including rescue, safety and emergency care), Hospital District of Southwest Finland (Emergency Medical Services). In this context, PPDR services (including communication procedures) are traditional emergency services provided by the organizations mentioned above, into which cyber emergency services should be integrated. The Defence Forces have been excluded from closer review. Public safety organization is an organization that is responsible for the prevention and protection of incidents, for example, Police (Baldini 2010). Public safety authorities and PPDR authorities mean the same thing for this purpose.

3.4.3 Relevant standards and guidelines

ISO/IEC 27001 formally determines an Information Security Management System (ISMS). It is a suite for activities concerning managing information risks called "information security risks" in the standard (IsecT 2017). Information security management is an essential part of management, and the management system supports management in it. Information security ensures the confidentiality of information, as well as its availability and integrity.

ISO 27799:2016 (International Organization for Standardization, (ISO) 2016) defines guidelines for organizational information security standards and information security management practices that contain the selection, implementation, and management of controls considering the organization's information security risk environments. It defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard (International Organization for Standardization (ISO), 2016).

ISO 27032:2012 (International Organization for Standardization (ISO), 2012) is a guide to enhancing the condition of cybersecurity by drawing out the elements of its dependencies on other security domains, in particular: information, network, internet security, and critical information infrastructure protection (CIIP) (International Organization for Standardization (ISO), 2012).

ISO/IEC 9001:2015 provides practical guidance on managing the total service produced for the customer. It also enables the healthcare organization to demonstrate that it meets customer satisfaction requirements and develops customer satisfaction by managing the risks of the operating environment (International Organization for Standardization (ISO), 2015).

ISO/IEC 27002 consists of instructions such as information exchange should base on policies, procedures, and agreements (including confidentiality agreements) concerning information transfer to/from third parties, consisting of electronic information sharing (e.g., messaging) (International Organization for Standardization (ISO), 2013).

3.4.4 Situational awareness

The Ministry of Defence (2010) defines situational awareness as consisting of the following things:

- The understanding of decision-makers and their advisors concerning what has happened.
- The circumstances under which it happened.
- The goals of the different parties and the possible developments of events.
- All needed data to decide on a specific issue or an entity of issues.

Mica Endsley defines situational awareness as the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future (Endsley, 1988).

> "Situational awareness is the ability to identify, process, and comprehend the critical information about an incident, and "SA" is knowing what is going on around you. It requires continuous monitoring of relevant sources of information regarding actual incidents and developing hazards." (Endsley, 1988).

A situational picture may be a general assessment at regular intervals. A strategic situational picture consists of the detailed analysis of topics where events and their impacts are assessed. A situational picture can also be a daily or hourly drafted report of events that are made available in the information system for actors. It usually does not contain assessments of situational developments or recommendations for measures. An operational situational picture is updated in real-time as possible during a disturbance. Continuous monitoring provides an evolving "picture of events" and enables the management of the situation and the management process needed to solve the situation. (Ministry of Defence, 2010). A shared situational picture must be a reliable one that the decision-maker can trust in all its elements and that the analyses are made with the best possible expertise (Ministry of Defence, 2010).

3.5 Formation of cyber situational awareness

Helen Gill from the Unites States National Science Foundation created the term cyber-physical systems (CPS) to explain the integration of computation with physical processes where CPS, embedded computers, and networks monitor and control the physical processes. Feedback loops of physical processes affect

computations and vice versa. CPS enables to use of the next generation of "smart systems" like advanced robotics, computer-controlled processes, and real-time integrated systems (Lee & Seshia, 2015).

The term Cyber Infrastructure consists of electronic information and communications systems and services comprised of all hardware and software that process, store, communicate information, or combine all of these elements. In other words, the information contained in these systems and services belongs to the concept of CI. Processing consists of the creation, access, modification, and destruction of information. Storage includes all media types, such as paper and digitalized formats (NIST, 2014a). Cyber situational awareness is a part of situational awareness which concerns the "cyber" environment (Franke & Brynielsson, 2014). Cyber situational awareness may enhance by using data from IT cyber sensors (intrusion detection systems, etc.) that can be transferred to a data fusion process or be analyzed directly by the decision-maker (Franke & Brynielsson, 2014). Communications contain information sharing and distribution such as computer systems; control systems (e.g., supervisory control and data acquisition– SCADA systems); networks, such as the Internet; and cyber services (e.g., managed security and monitoring services) belong under the concept cyberinfrastructure.

3.5.1 Protecting Critical Infrastructure and Vital Functions of Society

Linking systems, sensors, and actuator instruments to the broader internet creates an interactive entity conceptualized as the Internet of Things (IoT) that allows things to communicate and exchange control data and other necessary information while executing applications toward machine goals (Electrical Technology, 2016). FIGURE 7 illustrates secure communication flows, electrical flows, and different domains.

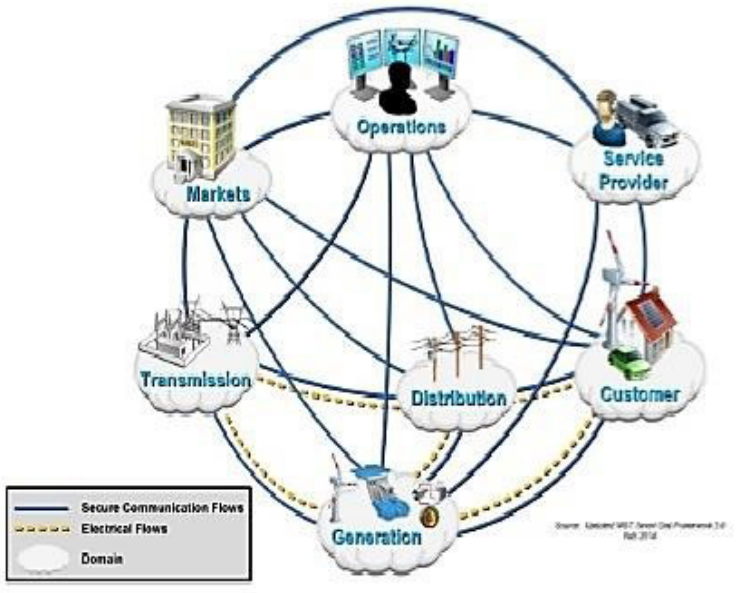


FIGURE 7 Interaction of actors in different smart grid domains (Electrical Technology 2016)

In the United States, the critical infrastructure (CI) means physical or virtual systems and assets that are so vital to the state that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health, or safety, or any combination of those matters (The White House, 2013). It is the foundation of the vital functions of society. In this dissertation, Critical Infrastructure and vital functions are not separated traditionally because the meaning of the concepts overlaps each other.

U.S Department of Homeland Security identifies 16 different sectors for the classification of Critical Infrastructure. According to the Department of Homeland Security (2013) those are Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare, and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation Systems and Water Wastewater System. Cyber threats, for example, phishing attempts, black-mailing attempts, hacking incidents, are an ever-changing threat to cyber systems across the sectors. The sector-based classification is also suitable in European countries.

3.5.2 Cyber and hybrid threats

According to the NIST (2016a) threat information is any threat-related information that might help an organization protect itself against a threat or detect the activities of an actor. Significant threat information types include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations.

TTPs describe the behavior of an actor. A tactic is the highest-level description of this behavior. At the same time, techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower level highly detailed description in the context of a technique (NIST, 2016).

Cyber threats consist of denial of service (DoS), unauthorized vulnerability probes, botnet command and control, data exfiltration, data destruction, or even physical destruction by using the alternation of critical software/data. These threats can be triggered and maintained through targeted and long-lasting mixes of malware, social manipulation, or highly developed advanced persistent threats (APT) (NIST, 2014b).

Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless cyber threats included in the cyber threat scenario are, e.g., Cyberactivism (cyber vandalism, hacktivism), Cyber-crime, Cyberespionage, Cyber terrorism, Cyber operations: pressure, Low-Intensity Conflict (LIC) or cyber warfare (Secretariat of the Security Committee, 2013). Hybrid threat means, for example, a combination of different kinds of physical and cyber threats.

3.5.3 Command and control center (C2) and decision support systems

The situation center is the place where decision-makers and authorities maintain situational awareness and make decisions to allocate, for example, PPDR-resources to the right proportion. Command and Control mean separately and collectively different things to different communities. (Alberts & Hayes, 2006). A place for command and control action may be a physically (e.g., a conference room) or virtually (e.g., telephone conference call) located and designed command and Control Center, a situation center, or Emergency Operation Room that support emergency response, business continuity, and crisis communications activities. C2 is made for managing preparations for an upcoming event or the response to an ongoing incident together and supplying them with up-to-date information (Ashish et al., 2007).

Remote operation comprises controlling and operating a system or equipment remotely. In systems engineering, monitoring means a process within a distributed system for collecting and storing state data. A PPDR monitoring station is a workstation where sensor information accumulates for end-users who need it. Monitoring systems consist of information collection, analysis, and provision for end-users, which is front-deployed knowledge.

Government Situation Centre, situated at the prime minister's office, aims to keep the state leaders and central government authorities informed continuously. The Government Situation Centre has to alert the government, permanent secretaries, and heads of preparedness and to call them to councils, meetings, and negotiations at exceptional times required by a disruption or a crisis (Ministry of defence, 2010).

The Ministry of Finance is responsible for steering and developing the state's information security in Finland (The Security Committee, 2018).

The Government situation centre's main task is to alert and call the government, permanent secretaries, and heads of preparedness to councils, meetings, and negotiations at exceptional times such as an ongoing pandemic. The ministries have to share the situational picture for their entire administrative branch with the government situation center and inform the center of all security incidents in their field of activity. In addition, authorities send security incident reports directly to the government situation center in urgent situations. As the national official focal point, the government situation center follows public sources and receives information from abroad to maintain transnational situational awareness (Ministry of Defence, 2010).

3.5.4 Intelligence solutions for public safety organizations

Open-Source Intelligence (OSINT) is described as the generally publicly available unclassified information, even limited distributed or available upon payment in any medium. It may include the systematic collection, processing, analysis and production, classification, and dissemination of information derived from openly available sources to the public. (Glassman & Kang, 2012; Morrow & Odierno, 2012; Nurmi, 2015).

Social Media Intelligence (SOCMINT) identifies social media content as a challenging opportunity for open-source investigations (Trottier, 2015). Big data contains analysis, capturing, research, sharing, storage, visualization, and information safety. Together with OSINT, Big Data produces the ability to detect standards of behavior and tendencies (Dos Passos, 2016). The availability of high-resolution worldwide satellite photography on the web has expanded open-source capabilities into areas previously available only to major intelligence services (Franke & Brynielsson, 2014). In the proposed Hybrid Emergency Response Model (Simola & Rajamäki, 2018; Simola & Rajamäki, 2017) OSINT and SOCMINT features are utilized in the automated HERM as an integrated part of an AI-driven decision support tool.

4 EFFECTS AND FACTORS OF THE NEW SOLUTION

This chapter will overview and present essential results of the articles that have been selected for the doctoral dissertation. The cases determine essential elements and a set of requirements for developing the Hybrid Emergency Response Model. Firstly, I will present the results of cases I and II that concentrate on formulating the first version of the model. The Cases Hybrid Emergency Response Model: Improving Cyber Situational Awareness and Cyber situational awareness in maritime surveillance belongs to this area.

Case III, titled Effects of Cyber Domain in Crisis Management, proposes to solve the problems of development needs through technical, organizational, and structural alternatives. Case IV handles how privacy issues affect when applying Hybrid Emergency Model in the smart city. Case V handles how the HERM can be implemented in an intelligent society where decision-making responsibilities are scattered.

Case VI analyzes cyber information sharing-related literature for the development process of the Early Warning Solution. Cases VII and VIII handle information sharing processes, models, and frameworks that have been used in classified information sharing methods and processes. Case IX handles how it is possible to use HERM to enhance situational awareness in a Pandemic situation.

4.1 Articles I and II: Fundamental knowledge about the operational environment

Understanding the environment of the research problem and knowledge base support each other in a way that the designed system developed after each case. Articles I and II concentrates on forming a model that takes into account assessed user requirements. Article I answer research questions 1, 2, and 3. Article II answers to research question 4.

4.2 Article I: HERM: Improving Cyber Situational Awareness

There is a need to follow guidelines based on user requirements and needs (Simola, 2015). It has been proved that there is a fundamental information-sharing gap between the public safety workers and different emergency response centers/ situation centers. Previous studies indicate the need for real-time information about the event with the right content. The researcher´s knowledge of the practical situations has been strengthened by doing additional empirical studies. The research project has been done from different viewpoints. Firstly at the micro-level, then from local to the regional level, and from the regional level to the national level ending up at the transnational level. Firstly, essential factors related to information sharing that affect the daily working routine of public safety authorities are introduced. Article I concentrates on the designing process of the model based on outputs of the previous studies that the researcher has done and a new knowledge base that helps in the designing process.

The purpose of the study was to design an emergency response model that enhances the formation of situational awareness. FIGURE 8 illustrates the proposed technical structure of the model. The case study is based on an empirical ethnographic research approach because the researcher had to study the culture of the actual working environment more intensely because there were dissimilarities in literature -references regarding public safety organizations' information systems.

The empirical study focused on four regional command/situation centers, the Southwestern Finland Police department, Southwest Finland Emergency Services, Hospital District of Southwest Finland, and The Finnish Border Guards in Turku. The Finnish Border Guards have their own main situational/command center in Turku, and it is called for Maritime Rescue Coordination Centre. The state manages it under the Finnish Border Guard.

Certain municipalities in southwest Finland are responsible for Southwest Finland Emergency Services and the Hospital District of Southwest Finland. The four field commanders and eight emergency dispatch workers were interviewed, and their working routines were observed in their natural work environment. It gives a better way to understand work procedures, as FIGURE 8 illustrates.

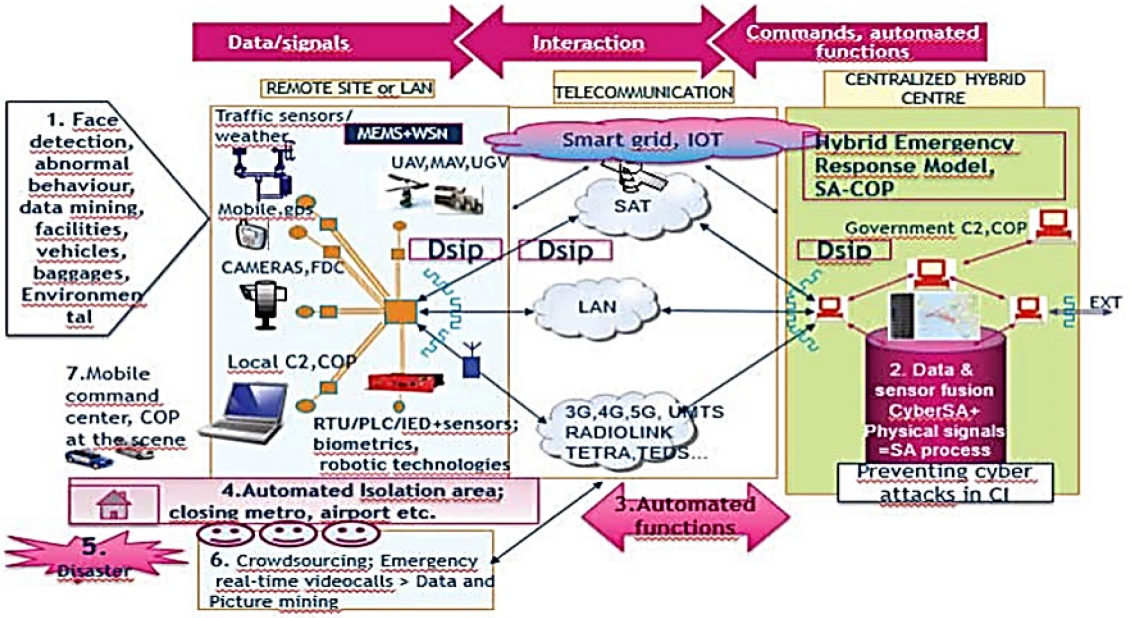


FIGURE 8 Hybrid Emergency Response Model

Findings of the research

Enhanced cyber situational awareness requires efficient information sharing and exchange with others. For example, the field command system can be used in other situation centers without cooperation. None of the regional situational centre has direct contact with the Government situation center, but the connections are handled through intermediaries. Essential situation centers should have arranged access to the government situation center´s data connections in rapidly evolving situations.

The Finnish PPDR authorities do not currently have a common command and control center with permanent personnel for major accidents. Deficient cooperation between situation centers prevents the creation of shared situational awareness and picture. Starting cooperation at the scene of an accident is not enough during a major accident. A more reliable and accurate common situational picture should be created before arriving at the accident scene. A cyber situational picture is needed if the target of the attack is a CPS. Lack of preparedness plans affects cooperation within PPDR authorities at the scene of a major accident. Reforms in the public sector and changes in PPDR organizations with legislative amendments require changes in preparedness plans. Unclear task descriptions in a case of a major accident prevent allocating resources. Complexity hierarchy levels make public safety decision-making complicated. Therefore, settling new technology faces challenges. It has to consider that individuals, groups, and work environments form an entity. Situation information does not flow if there are obstacles to information sharing.

Concentrating on organizations' tasks prevents them from seeing what other authorities are going to do at the scene of an accident. Examined situation centers cannot create direct communication connections with the Government situation

center. Mentioned deficiency prevents information flow from a local level to a higher level and creates obstacles to a higher level of preparedness. There should be a common situation center where operational commanders as different state and municipality PPDR actors and decision-makers could get together when a significant hybrid accident occurs. At present managerial personnel get together at each other's command centers depending on the type of the accident. Making large-scale built infrastructure in urban areas more resilient against different kinds of attacks and disruptions requires multifunctional cooperation between various actors in the security sector. Alert mechanisms should be multimodal (not just on operator screens), and the control system functions and communications that generate them must be designed so that cyber-attacks cannot bypass them. A common cyber situational awareness is needed for both operating CPS and emergency and crisis management.

Discussion

The research indicates the need for effective, reliable information sharing to form hybrid situational awareness. Cyber-physical system which combines separate threat signals will produce added value that is missing from the present emergency response system—in practice, establishing one system that covers Emergency Response Centre and National Cyber Security Centre Finland emergency functions.

4.3 Article II: Improving cyber situational awareness in maritime surveillance

Background

The case has been made parallel to the Maritime Integrated Surveillance Awareness (MARISA) project, and it concentrates on enhancing Situational maritime awareness in a Maritime environment. The national CBRNE strategy identifies maritime safety as one of the leading areas for development, intending to create a common maritime situational awareness among decision-makers. The overall objective of the strategy is to continuously improve the prevention of and preparedness for CBRNE threats (incident caused by chemical substances (C), biological pathogens (B), radioactive material (R), nuclear weapons (N) and explosives (E) and accidents to safeguard society and ensure vital functions for society (CBRNE strategy working group, 2017). Maritime transportation in cross-border trade has created new pressures to develop new technologies for accident prevention. Maritime safety is also a concern in managing continuity.

The Coast guard, as part of the Finnish Border Guard, ensures the security of Finland and prevents security threats at external borders (Finland and Europe). Crime prevention is one of the essential tasks that it has. The Finnish maritime search and rescue (SAR) system is part of the broader security system of the Finnish Border Guard. Coast guard services include Search and Rescue services at sea and in the air. The other main tasks are protecting coastal waters, criminal

interdiction, illegal immigration, and disaster and humanitarian assistance in operational areas. These functions may vary according to the administration, but the core functions are generally the same (The Finnish Border Guard, 2018). The Finnish Border Guard maintains readiness for management and operations during maritime incidents. The Coast Guard protects the marine environment covering almost 1,300 kilometers of territorial waters. A coherent, accurate, and sharable situational picture from the scene of an accident is needed. The accident's nature must be evaluated as soon as it occurs, and the observer must inform the state leadership of major accidents (Kaukanen & Möttönen, 2010; The Finnish Border Guard, 2018).

The main findings of the research

The main findings can be summarized as follows:

- The non-use of ship transponders affects and leads to a waste of technical and physical resources by the authorities.
- Currently, individual patrollers create the situational picture using Virve communication, VHF, and MF to collect information before arriving at the accident scene.
- The coast guard has recording cameras with data transfer features on surveillance aircraft without a visual real-time communication system. Data is possible to transfer to Maritime Rescue Coordination Centre afterward.
- Cruise ships or patrol vessels cannot share real-time data with the Maritime Rescue Coordination Centre. The use of a real-time video system is not currently possible.
- Limited data transmission capacity and the deficiency of transferring opportunities for real-time data from ships affect the correct formation of the situational picture from an accident site.
- Small ships or boats whose transponders or positioning systems are turned off and attempting to cross the Schengen border form challenges.
- The several cameras of the MRCC support border control by allowing tracking and identifying which ships are operating in the archipelago.
- Underwater surveillance is carried out in cooperation with the Finnish Navy.
- The West Finland Coast Guard District has a direct emergency number for emergencies.
- In a long-standing major maritime accident, the command and control center of the Command and Maritime Rescue Coordination Centre (MRCC) leads cooperation in multi-authority situations. It is the management and marine rescue center for the managerial personnel such as rescue and police field managers.
- PPDR authorities' coordination of crisis management needs effective coordination. Standardization is needed for technical communication solutions.

- The real-time information about available aid from voluntary associations has not been shared with the Maritime Rescue Coordination Centre.
- The area of operations of the West Finland Coast Guard District covers the region of four emergency centers and its responsibility for the security of the whole western sea area.
- Virve has only a maximum of 20 call groups per workstation.
- Due to a broad monitored area, one major emergency will relocate resources from daily routine to a more serious accident.
- All the desired call groups can be controlled with one terminal, but the groups must be shared between different workstations. This procedure helps them to analyze events better.
- The field commander and officer in charge of rescue operations decide if it is necessary to issue a major accident alert.
- The coast guard does not have a shared situational awareness system for daily cross-border cooperation.
- Operational fieldwork covers statutory tasks such as executive assistance tasks and the management of Maritime Rescue.
- International contacts of maritime rescue operations are handled in neighboring countries and, where appropriate, more widely.
- A Unique function of MRCC is coordinating the entire Finnish Border Guard's flight operations as appropriate. Airbase stations are located in Helsinki, Rovaniemi, and Turku.
- Data transmission capacity is often limited in the event of congestion, leading to needing to establish a new reliable network with high bandwidth.

The findings indicate a need to design new hybrid communication models to utilize real-time data for enhancing situational awareness. Therefore, a hybrid emergency model with intelligence capabilities needs to be designed. The designed proposal of the Hybrid Emergency Response model is a unique concept that can be transferred or expanded to the maritime environment. Using the Open-Source INTelligence (OSINT) process in a hybrid emergency model allows meaningful intelligence to be collected. Crucial open-source information consists of geospatial data. Social Media Intelligence (SOCMINT) identifies social media content in particular as a challenge and opportunity for open-source investigations.

Designed model for the maritime Situational Awareness

Separate internal and external security threats are nowadays combinations of threat types, and as a result, public safety organizations such as the Finnish Border Guard must be able to prevent virtual and physical hybrid threats that are developing upon borders and respond to them. Enhancing information sharing between the public sector, citizens, and volunteer associations, is a relevant part of this framework. It makes it possible to prevent and respond faster to the realization of threats. A new next-generation platform for the

existing emergency response information system and mechanism can lead to important new results. Organizational cooperation requires a common infrastructure and clearer and faster telecommunications connections for information sharing. The cyber domain can be used as a powerful element to enhance data fusion to create more accurate overall situational awareness. PPDR authorities can use smart emergency response functions before any threats have occurred if raw data on anomalous behavior or movements are processed and analyzed in advance, as illustrated in FIGURE 9.

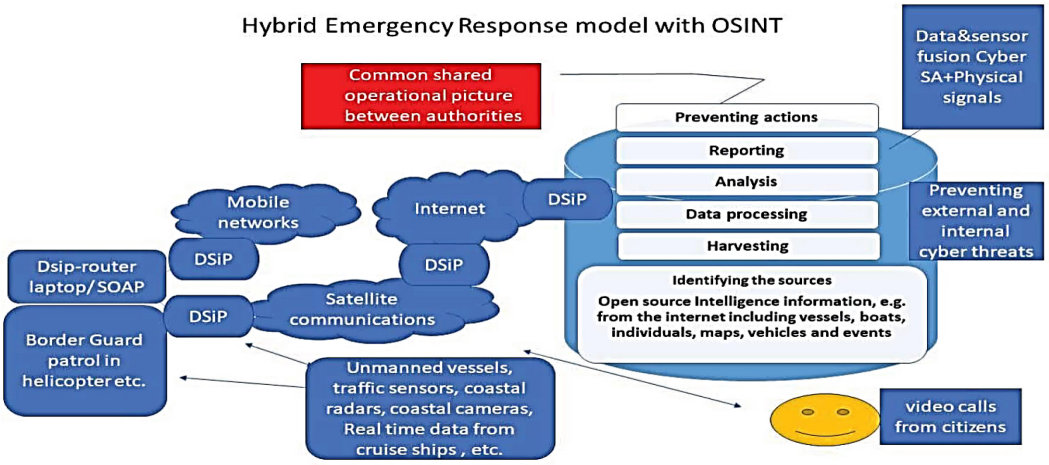


FIGURE 9 Hybrid Emergency Response Model with OSINT Features

The presented model will combine existing surveillance systems and information networks with new ones and give all concerned authorities and other stakeholders access to the information they need for their missions at sea and border areas. Combining open-source data to ensure correct and reliable information sharing is of primary importance. The essential information is processed in the desired form for the accident site command center. The next-generation emergency response system is based on active operations and automated functions. The functional information-sharing mechanism requires a direct communication connection from the situation center to the government situation center.

4.4 Article III: Effects of Cyber Domain in Crisis Management

Background

Article III identifies the key factors influencing implementing a next-generation hybrid emergency response system in critical infrastructure protection. The research suggests solving the problems of development needs through technical, organizational, and structural alternatives.

NASA, DoD, DoE, and the Department of Homeland Security have used an indicative indicator known as the Technology Readiness Level (TRL) to assess the readiness of systems under development. The Systems Development & Maturity Laboratory (SysDML) at Stevens Institute of Technology developed an indicator called the Integration Readiness Level (IRL), which facilitates handling system integration. It is possible to form a knowledge base on the technological maturity level of the emergency response services infrastructure by Combining both TRL Technology Readiness Level and IRL Integration Readiness Level scales. Tier levels 1-3 are used instead of 1-9 in this research.

By comparing current emergency response processes to the proposed Smart hybrid emergency process model, it can be found effects and factors which prevent the implementation of this architecture.

The three main categories that have been chosen for classifications are The relevant legislation for the Smart hybrid model - Technological maturity level, - Readiness level from an organizational and political view.

The main findings of the research

FIGURE 10 represents the formation of cyber-physical threats collected from different sources and the separate organizations' responsibilities that oversee these threats. There are no joint preventive cyber functions or links between the Emergency Response Centres operations and the Finnish Communications Regulatory Authority's Cyber Security Center.

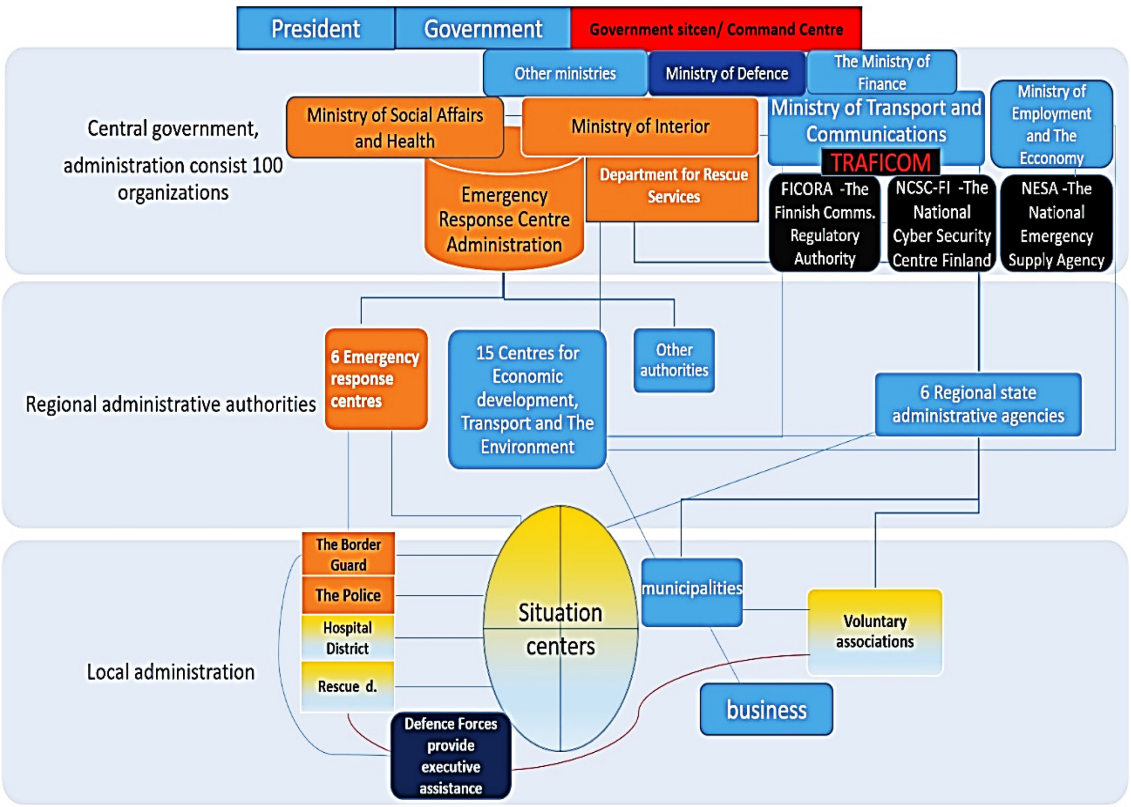


FIGURE 10 Organization's responsibilities of cyber security

There are fundamental maturity level factors that make challenging the implementation of the system. There is a difference between the new and the old model when looking at the maturity level of current national and European developments against the development process of the next generation emergency model, as clarified in TABLE 5. A prescriptive metric known as Technology Readiness Level (TRL) by NASA and integration metric called Integration Readiness Level (IRL) by the Systems Development & Maturity Laboratory (SysDML) at Stevens Institute of Technology create combined metric to form a knowledge on the technological maturity level of the emergency response services. Tier levels 1-3 are used instead of 1-9 in this research.

TABLE 5 Maturity level of emergency response systems

Maturity level		**Low**	**Med**	**High**
		1	**2**	**3**
Low (red) presents that the maturity level of the system does not correspond to the research area. Medium (green 2) presents that the maturity level is average. High (blue 3) presents that the maturity level of the system is ready for the implementation				
Research areas	**Present system**		**Next gen. HERM system**	
European legislation	1		2	
Legislation concerning technology	3		1	
Legislation concerning privacy issues	3		2	
Legislation concerning the smart hybrid model	**sum**	**7**		**5**
Technological maturity	2		3	
Smart city maturity	1		3	
Maturity of organizational integration	1		2	
Opportunities to use smart devices	1		3	
Opportunities to integrate sensor technologies	2		3	
Maturity to integrate IT-systems	1		3	
Operational reliability	2		2	
Technological maturity level	**sum**	**10**		**19**
Organizations maturity level	3		1	
Political readiness at the national level	3		1	
European policy	1		2	
Readiness level of organizational and political view	**sum**	**7**		**4**
	24		**28**	

Organizational factors prevent the execution of the new system. These factors are closely related to the legislation; for example, emergency services operate under the municipalities. The Emergency Response Centre acts under the Ministry of Interior. On the other, the Coast guard acts under the Ministry of Interior, but Defense forces act under The Ministry of Defence. Much remains to be done to make the operating environment conducive to the next generation of emergency systems. Finnish legislation has allowed law enforcement authorities to monitor citizens' digital behavior in real-time only on suspicion of a crime. Tools like OSINT, Geo-targeting, Geo-fencing with Wi-Fi, Cell Towers, and Beacons create a privacy-restricting advertisement and surveillance circuit to trace consumer behavior. These tools can be utilized only with the proposed new Hybrid Emergency Response model. That is why the maturity level of mobile technology is so low.

4.5 Article IV: Privacy issues and critical infrastructure protection

Background

Article IV handles privacy issues in smart city infrastructure where the proposed HERM operates. Identifying essential factors of privacy issues that affect the utilization of the proposed smart hybrid emergency response model generates privacy requirements for the system. In the hybrid emergency response model, proactive accident/incident management begins before any physical damage has occurred. The cyber ecosystem of the hybrid model works in many ways. Sensor networks consist of cyber and physical elements with automated functions that detect intrusions and threats in Critical Infrastructure before an emergency call has been made. Data fusion analysis combines and produces necessary command-based signals, which launch automatically processed operations like isolating an area under threat or automatic functions based on biometrics data such as thermal imaging or face recognition. Data fusion might also help avoid and reduce false alarms by fusing the information from multiple sources and sensors. The mechanism of the threat data sharing process may work with a wireless sensor and actuator network (WSAN), where signals convert to a physical process by creating a closed control loop.

The field-tested 4com -routers and DSiP -software package enables parallel use of different network technologies transparently, enabling to create of communications services platforms (Simola, Jussi & Rajamäki, 2014). This feature reduces network interference in cyber-physical operations and the need to communicate with VIRVE phones between authorities reducing. The system eliminates human error activity in the event of an accident. Automated safety measures can also remove the problems related to information sharing and commandment of power relations. The hybrid emergency response system allows people to send pictures or make video calls and provides a platform for crowdsourcing -software to screen the images and videos automatically from the

scene of an accident. The system will directly share crucial data about an accident with the field commanders and Government Situation Centres. It is relevant to allocate additional reliable data to determine discrepancies in limits. It is important to unite pieces of information to ensure the correct and reliable information is shared.

The proposed hybrid emergency response system process the essential information to the desired shape. The system consists of active physical operations and automated technical functionalities where Cyber defence operations are integrated as part of the cyber-physical emergency response services according to regional differences, authorities, and mission needs. Shopping mall sensor networks in a local city area may comprise Local Based Service -components for a geofencing place with automated functions like speed breakers, which automatically activate when the threat level (e.g., speed) has risen too high, as FIGURE 11 illustrates.

Operational preparedness affects the cooperation within PPDR authorities in the field of a major accident. Reforms in the public sector and changes in PPDR organizations with legislative amendments require updated preparedness plans.

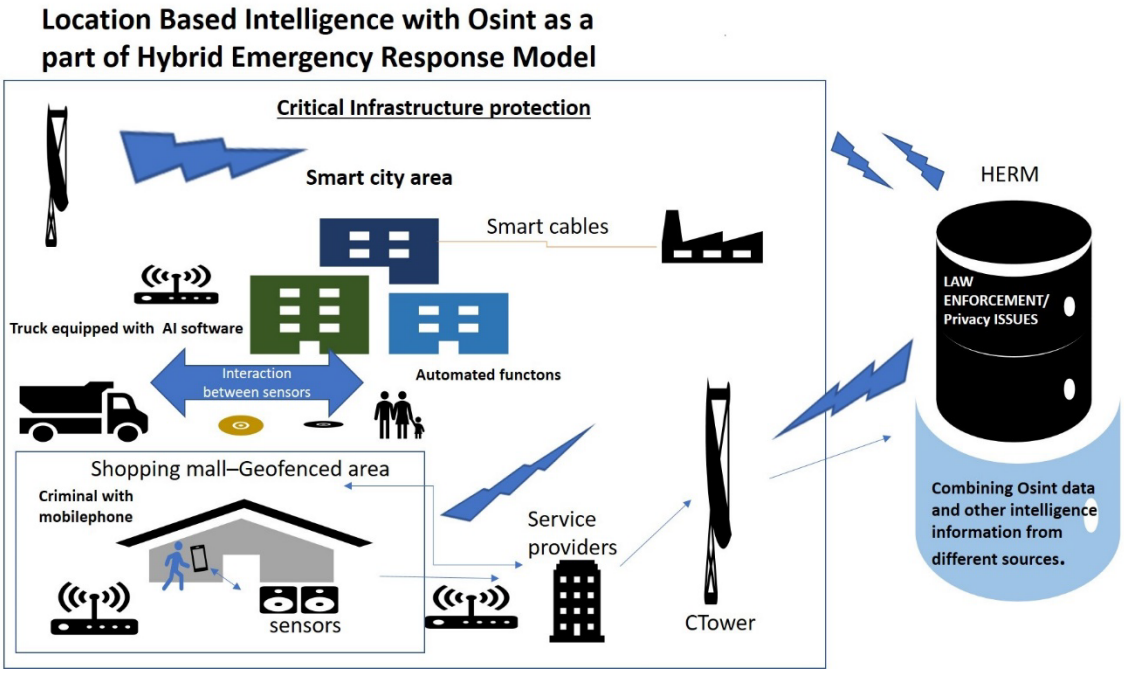


FIGURE 11 Location-based intelligence with OSINT as part of the HERM

If there are too many hierarchy levels for decision-making, information about a situation does not flow. Responsibilities for developing organization-level cybersecurity have been shared in too many factors.

Discussion about privacy issues

Using combined data from different sources can create opportunities and threats at the personal profiling level when the purpose is protecting Critical

Infrastructure. The collected privacy data cannot be used as being unauthorized, and data must also be utilized for a permitted purpose. Some political and technological factors create challenges in designing a monitoring system. The importance of privacy has risen to the surface of the social welfare and health care (SOTE) reform In Finland. The idea of the Finnish government concerning a human disease classification system based on patient records has raised protests. There is a clear trend for creating various classification systems in Europe. Still, problems arise when people are classified based on sensitive information in a situation where data management has been given to a third party. In Finland, one of the focal points of the SOTE reform is integrating patient registers and creating one joint information system. Traditional thought within Finnish decision-makers has been that the commercial operators must be kept separate from regulatory activities. Citizens are not satisfied that their behavior has been collected more widely than what has been told and for not precisely known uses. Thus, it might be essential to look at the whole cyber-physical ecosystem of Critical Infrastructure protection. The essential question is, what features and elements can be contained in the framework that protects society's vital functions?

On the other hand, digitalization and location-based technologies create opportunities and threats to citizens' private life. Power relations may change in a democratic society, and public power may centralize in a totalitarian regime. How would the sensitive information be used in different political environments? The need for a new type of standardized hybrid emergency response model forms from the following factors:

- To be able to trust, citizens must accept automatized safety functions in public places.
- Privacy legislation does not cause permanent obstacles to using sensing elements in a hybrid emergency response model.
- Organizational responsibilities have to rationalize for cybersecurity development.
- Limited observation capability restricts a human ability to work efficiently.
- Overlapping data transmission procedures limits the effective cooperation among PPDR authorities.
- Limited data transmission capacity prevents communication between the authorities.
- Preventive functions of the emergency response model on cyber threats are an essential part of the overall security in situation awareness management and Critical Infrastructure Protection.
- Confidential data must be kept safe. Therefore, continuity management needs to create between citizens and authorities on a confidential base.
- A modern Cyber-Physical System based on complex systems of communication networks. Therefore, has to consider vulnerable built infrastructures of the urban area.

- A shared common operational picture requires that real-time communication links from the local level to the state level, such as the Government Situation Centre must exist.
- If a cyber-attack becomes physical when intrusion is not detected, it may lead to interrupting the transmission of electricity, causing the telecommunications networks will conclude to function.
- Cyber preparedness and privacy policy belong to continuity management.
- The exchange of information between intelligence authorities and data protection authorities must also be ensured. When human weaknesses are left out of the information sharing procedure, data leakage to third parties becomes more difficult.
- Automatically ensured privacy protection would increase citizens' confidence in the system's activities.
- On a practical level, there is a need to integrate traditional Emergency Response Centre and National Cyber Security Centre Finland emergency functions.
- The approved intelligence legislation package is expected to improve the ability of the PPDR authorities to respond to major national and transnational hybrid threats because it allows more extended use of new decision support system technologies.
- The broader use of a new decision support system requires clarification of common rules; privacy protection should be facilitated if citizens accept common rules created in legislation.
- The micro and macro levels will be encountered if a foreign state party intervenes to interfere with the functioning of data traffic.

At the general level, the Hybrid emergency response model does not violate the citizens' privacy more than what is required to prevent a threat or solve the potential crime before it occurs because technology has to connect to the current regulation such as GDPR. Underdeveloped local urban infrastructure prevents the utilization of intelligence data collection methods, including local-based intelligence solutions—development of critical infrastructure support also privacy issues aspect. The study also indicates that the challenges to national security and vital functions and privacy issues are related to politicians and political projects. It is challenging to predict the future direction of the national political trend at the macro-level because good inter-state relations may lead to ignoring security issues. This state-level political dimension may prevent the utilization of the proposed smart hybrid emergency model.

4.6 Article V: Emergency Response model as a part of the Smart Society

Background

The paper aims to discover those fundamental technological-related risks that expose society to hybrid threats. These potential threats prevent to detect threats and affect the protection of critical infrastructure. Technical early warning solutions become useless to design if crucial risk factors are not noticed. Thus, decision-makers need reliable decision-support information that does not expose them to hazards. Implementing the presented Hybrid Emergency Response Model is the primary purpose because there is a need to combine the functionalities of situation centers, emergency response centers, and organizations to fight against cyber threats. There is no common emergency response model for all kinds of hybrid threats. The lead author of this research has innovated the next-generation emergency response model (Simola & Rajamäki, 2017).

The research area of the vital functions is defined in four main sections; the Emergency services sector, the Communication sector closely linked to the Energy Sector, and the Information sector. Firstly, it is essential to discover technological risks and scenarios that expose society's vital functions to hybrid threats and risks. After categorizing basic threats and risks, it is easier to detect fundamental level risk factors that prevent the detection of threats and prevent the protection of vital functions. We have used a combination of different methodologies to find out those factors that affect society´s decision-making. The separate risks are divided into main areas as TABLE 6 demonstrates: administrative risks, conflict risks, operational risks of the PPDR emergency services, socioeconomic risks, and infrastructure risks. The numbers A, B, C, D, and E indicate which section the subcategories are linked. Separate risks are categorized and ranked on a three risks level process. The first measure is valued at the "frequency of the phenomenon" (1 = phenomenon does not occur every year, 2 = phenomenon occurs yearly, and 3 = a phenomenon is permanent). The second value is titled the "predictability and measurability of risks" (1= phenomenon is neither predictable nor measurable, 2= phenomenon is predictable. 3 = phenomenon is predictable and measurable.) The third value is named the "impact of risk on overall security" (1= impact of the risk on one vital function, 2=impact of the risk on two to three vital functions, and 3 = impacts of risk on more than three selected vital functions.) The coefficients for the variables are titled as follows: 1 to "frequency of the phenomenon," 2 to “predictability and measurability of risks”, and 3 to "Impact of risk on overall security.

TABLE 6 Main risk classification

Main risk classification and subcategories									
A		**B**		**C**		**D**		**E**	
Administrative risks		**Conflict risks**		**PPDR services and functions related risks**		**Socioeconomic risks**		**Infrastructure related risks**	
Problems in local continuity management	C D	cyberattacks	A C E	Overloaded emergency management system	B E	Unemployment	A	Structural problems in the built urban area	A B C
Problems in cooperation between decisionmakers	B C D E	Human-made disaster or pandemic	E	Lack of human resources	A D E	Refugees	A B	Structural problems in the rural area	A B C D
Separate municipal activities	E	Cross-border radiation	C D E	Lack of resources in PPDR services	A D E	Cultural change	A	Recovery problems	A B C D
Organizational problems	B C	Physical war	A C D E	Emergency event	D E	Use of substances	B C	Secrets cyber influences	A B C D
Leadership problems in government	B C D E	Hybrid warfare	A C D E	Resource awareness of volunteers	A D E	Citizens poverty	A	Communication problems	A B C
						Unidentified people	A B C E		

Fundamental risk impacts for the HERM

The purpose of the research PV was to find out technological-related fundamental risks and challenges which are outside the official risk classification. Findings indicate that lower-level critical infrastructure risks do not cause immediate problems to the ground-level risks. FIGURE 12 shows that classified higher-level risks evidenced structural governance problems in society. The primary outcomes can be summarized so that essential human-based factors affect the whole cyber-ecosystem. The most problematic and most influential threats to domestic security and vital functions are linked to human factors such

as intentional and unintentional errors based on politicians' decisions and political projects. Balanced continuity management consists of cybersecurity maturity, operational preparedness, and decision-making reliability. Designing technical early warning solutions requires identifying fundamental risks, so that can be delivered reliable information for the decision-making process that does not expose decision-makers and society to hazards. One of the primary aims of hybrid influence is to weaken political decision-making. Despite listing the severe disturbance -threats in "Finland's security strategy for society report," similar fundamental risk types occur as the causes that have not been considered in decision-making.

Classified high level risks	Ground level-Scenario	Consequences
Cyberattacks	A) Legislation – Lack of possibilities to intervene in internal security	Lack of internal self-determination and internal sovereignty
Separate municipial activities	B) Political decisions – Lack of continuity management, short term political purposes	Line changes in security policy – development of unstable decision-making culture
Hybrid warfare	C) Energy solutions – Dependence on imported energy management, short-term political purposes	Exposure to extortion by an external actor
Unidentified people	D) Equipment for Communication systems – E.g., 5g solutions devices, network equipment.	Foreign state spying and foreign country get a role in infrastructure
	E) International public projects - Smart cable projects, gas pipeline projects	Vulnerability to sabotage - the foreign state may use cables and pipelines for hybrid influencing
	F) Decision-makers credibility- corruption, discrimination, criminal contacts to foreign state	Ability to prevent disturbances will decrease. National overall security and resilience level decreases. As a result, management of overall security becomes uncontrollable.

FIGURE 12 Classified high-level risks, scenarios, and consequences

Research indicates that structural fundamental-level threats may occur before any classified threat has been illustrated. It challenging to design new solutions concerning smart solutions if the ground base is weak. An unsecured platform causes fundamental obstacles to designing solutions for an intelligent society. Legislation sets challenges to the national politicians and authorities, but also power relations between union countries and hidden motivations of decision-makers.

4.7 Article VI: Literature Review of the scientific articles about the Cyber Information Sharing

The basis for the literature review

The research belongs to the ECHO project by developing Echo Early Warning System. The European network of Cybersecurity centres and competence Hub for innovation and Operations project (ECHO) is part of the Horizon2020 program.

The main objective of the ECHO is to strengthen the proactive cyber defence of the European Union. The literature review gathers essential scientific articles and official materials about cyber information-sharing models for the ECHO and, on the other hand, produces data about the trusted information-sharing mechanisms for the Hybrid Emergency Response model. The early warning system will work parallel with other mechanisms in the Public Protection and Disaster Relief environment. The development of the E-EWS will be rooted in a thorough review of information sharing and trust models within the cyber domain.

The literature review is based on systematic queries on four scientific databases presenting a comprehensive review of cyber information-sharing methods. Collected materials are based on scientific literature, research articles, and official publications. The results are examined from the viewpoint of how to develop a cybersecurity information sharing system and what possible features might be included in the system.

The notions of 'shared cyber situational awareness' and 'cybersecurity information sharing' create a theoretical framework by limiting the area of the literature study. It defines what to share, how to share, and with whom to share cybersecurity information.

Shared (cyber) situational awareness is closely related to trusted (cybersecurity) information sharing and exchange. In case of a hybrid incident, how can response and procedures be improved? Automated systems are more capable than human beings of processing large volumes of data. Flexible autonomy should provide a smooth and seamless transition of functions between humans and the system (Endsley, 1988).

Information sharing needs of the ECHO stakeholders are the basis for this research. The main research question is 'What are the main features of cyber exchange models?'.

The findings comprise the fundamental database for the Echo-Early Warning System based on the framework of CPS (Cyber-Physical System). It will support information sharing across organizational boundaries by providing general cyber information sharing as a reference library and securing connection management from clients accessing the E-EWS. It will combine different functions required to manage information sharing functions—including sector-specific cyber-sensitive data by covering the whole ecosystem.

Results of the literature review

Several studies were based on fundamental level public-related sources, which formed the mainframe of the research. There are few existing cybersecurity information sharing architectures and frameworks within public organizations divided into main groups. For example, Mitre (2018) categorizes information sharing models into three main models. The fourth hybrid model comprises a combination of the others, as FIGURE 13 illustrates.

I. Hub-and-Spoke means that several data producers and consumers share information; the information is sent to a central hub instead of sending information directly. The hub operates dissemination to all the other spokes as appropriate. The model can be seen as similar to e-mail distribution lists, where the senders provide a message to a mailing list service, which then delivers the message to all list members.

II. Peer-to-Peer is a group of data producers and data consumers who organize direct relationships with each other. Members share directly with each other in a mesh pattern. The group may have a single governing policy, but all sharing and exchanges happen between individuals.

III. Source-Subscriber is a single entity that publishes information to a group of consumers. For example, this is a common model in commercial environments, where the data source is a vendor and the subscribers' purchase access to the vendor's information. Source-Subscriber is also a common model for free alerts from authoritative sources (MITRE, 2018).

Despite the classification, many models are based on a hybrid structure.

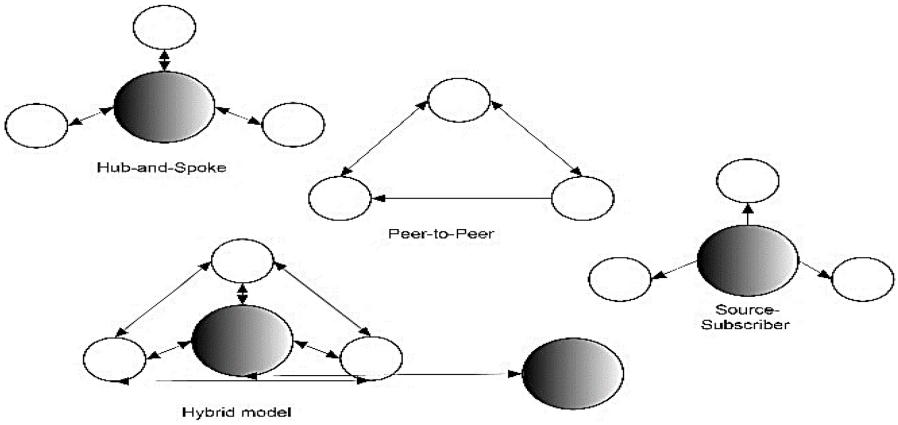


FIGURE 13 Traditional information sharing models

According to Sedenberg and Dempsey (2018), information sharing models can be divided into several categories as follows: government-centric; government-prompted—industry-centric; corporate— initiated-peer based (at the organizational level); small, highly vetted, individual-based groups; open-source sharing platforms; proprietary products; and commercialized services. Procedures and elements differ marginally from each other.

Government-Centric is a centralized model, where one central organization may share the information, exchange, or perform processing to enrich the data to others (He, Devine, & Zhuang, 2018; NIST, 2016b). The Department of Homeland Security is one kind of hierarchical Government-centric organization. The central infrastructures use open, standard data formats and transport protocols (He et al., 2018).

Sector-based Information Sharing and Analysis Centers (ISACs) are industry-centric sharing models driven by the government. Critical infrastructure owners and operators have formed non-profit, member-driven organizations to share information between government and industry. ISACs work through the National Infrastructure Protection Plan (NIPP). Information Sharing and Analysis Organizations (ISAOs) gather, analyze, and disseminate cyber threat information, but unlike ISACs, ISAOs are not sector-affiliated (Department of Homeland Security, 2013).

Corporate-based peer groups are privately sponsored cybersecurity information-sharing entities. They coordinate information sharing and exchanges without government intervention, and activities can be tailored to fit the specific needs of their members (Sedenberg & Dempsey, 2018).

Individual-based groups are small online communities of peers to share sensitive information with the goal of immediate combat attacks. This kind of group requires a high degree of trust (Sedenberg & Dempsey, 2018).

Open communities and platforms are open-source sharing platforms. Such as STIX indicators and open-source intelligence feeds are examples of this kind of format.

Essential features of cyber-threat information exchange models

The Department of Homeland Security in the US manages Automated Indicator Sharing (AIS), whose participants may attach to the Department's National Cybersecurity and Communications Integration Center (NCCIC), which permits bidirectional cyber threat indicators sharing.

Each participant has a server situated to exchange indicators with the NCCIC. Participants receive and can share DHS-developed indicators they have observed in their network defense efforts, which DHS will then share back to all AIS participants (Department of Homeland Security, 2019).

Indicator senders' identities are anonymous to other AIS participants unless they want DHS to share the source of those indicators with other participants (Department of Homeland Security 2019). Department of Homeland Security does not validate indicators because the focus is on velocity and volume. The partners inform the DHS that they will vet the AIS received indicators. The Department's goal is to share as many indicators quickly as possible (Department of Homeland Security 2019). The U.S. Government also needs useful information about indicators (Department of Homeland Security 2015).

AIS utilizes the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications for machine-to-machine communication (Department of Homeland Security 2019). STIX is a language and serialization format that enables organizations to

exchange Cyber Threat Intelligence (CTI) consistently and is machine-readable (Oasis 2017a). Trusted Automated eXchange of Intelligence Information (TAXII™) is an application layer protocol used to exchange Cyber Threat Intelligence (CTI) over the HTTPS (Oasis 2017b).

Cyber-threat information sharing governance and mechanisms

Cyber threat information is any information that may help an organization identify, assess, monitor, and respond to cyber threats and might help an organization protect itself against a threat or detect the activities of an actor (NIST, 2016). Threat intelligence reports are generally specific, prosed, and targeted threat-related information documents that have been collected, analyzed, transformed, or enriched to supply the required context for decision-making processes to provide greater situational awareness to an orgnization (NIST, 2016).

Commonly used collection-based communications describe the situation when a single TAXII client requests a TAXII server, and the TAXII server carries out that request with information from a database, as FIGURE 14 represents. A TAXII channel in the TAXII server enables TAXII clients to exchange information with other TAXII clients in a publish-subscribe model. TAXII clients can push messages to channels and can subscribe to channels to receive published messages. A TAXII server may host multiple channels per API root (Oasis 2017b). It is the main sharing mechanism for cyber threat information represented in STIX. Stakeholders may share indicators with the DHS through an ISAC or an ISAO without a TAXII client.

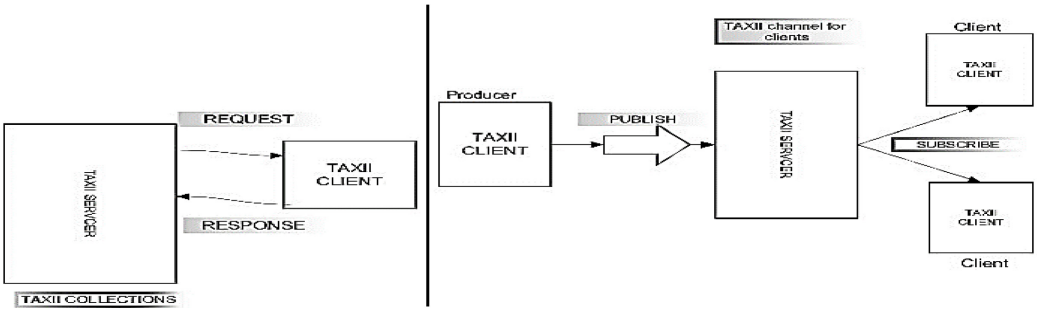


FIGURE 14 Flow of Cyberthreat Information in TAXII

Information sharing methodologies between certs and law enforcement

Collaboration between EU member states and related Network and Information Security communities (NIS) such as CERTs is an essential part of the cyber-ecosystem. It is not appropriate that small, closed groups share information without synergy with public safety organizations.

The Europol Information System (EIS) is the reference system for crimes, individuals involved, and other related data to support EU Member States, Europol, and its partners in their fight against serious crime as organized cybercrime and terrorism. For example, as a part of Europol, the European Cybercrime Centre (EC3) uses an open-source Malware Information Sharing Platform (MISP) platform (DG Home Affairs, 2014). MISP is an information-

sharing tool for malware samples and malicious campaigns related to specific malware variants. It offers architectural flexibility, allowing the utilization as a centralized platform (for example, CIRCL and FIRST instances) but also as a decentralized (peer-to-peer) platform (ENISA 2015).

There is a need to design new information management architecture and to continue improving operational capabilities and tools by focusing on automation and modernization (EUROPOL, 2019a)

There is also a need to harmonize further the technical infrastructure capability by integrating more IT systems with Europol's Identity and Access Management (IAM) landscape. The main focus is establishing a single enterprise identity, considering various networks and security standards, including IAM for Basic Protection Level (BPL) business solutions (EUROPOL, 2019b).

SIENA is made for searches on Europol's and EU member states' data. SIENA is a VPN (Virtual Private Network) designed to allow the EU member states to communicate and share intelligence information. It enables a quick and secure exchange of operational and strategic crime-related intelligence information between member states, Europol, law enforcement cooperation partners, and public safety organizations (DG Home Affairs, 2014).

National Information Exchange Model (NIEM) is used in the U.S. and enables information sharing focusing on information exchanged among organizations as part of their current or intended business practices. It is an XML-based partnership mechanism between the U.S. Departments of Justice (DOJ) and Homeland Security (DHS) (DG Home Affairs, 2014; The Criminal Intelligence Coordinating Council, 2013).

InfraGard's Secure Web Portal, hosted by the Federal Bureau of Investigation (FBI), allows confident messaging that promotes communication among members. InfraGard Members give access to the FBI's cyber incident reporting tool iGuardian, which is explicitly designed for the private sector. Membership allows peer-to-peer collaboration across InfraGard's broad membership and information-sharing and relationship-building with the FBI and law enforcement. InfraGard engages addresses threat issues related to 16 critical infrastructure sectors determined by Presidential Policy Directive-21 (PPD), the Department of Homeland Security (DHS), and the National Infrastructure Protection Plan (NIPP) (Department of Homeland Security, 2013; DG Home Affairs, 2014).

Digital Forensics XML (DFXML) is an XML language intended to represent the forensic data such as metadata of the file and detailed information about the forensic tool that did the processing, including the state of the computer on which the forensic processing was performed (Garfinkel, 2012).

The Cybersecurity Information Exchange Framework (CYBEX) is made to develop and automate cybersecurity information exchange. The CYBEX forensics operation domain supports law enforcement operations by collecting evidence by storing it in the evidence database. CYBEX provides a framework for exchanging information between a network contact point and a law enforcement

agency to offer a range of real-time cybercrime technical information related to a specific event (Rutkowski et al., 2010).

CYBEX-P and the Privacy-Preserving Cybersecurity Information Exchange mechanism are modified and developed from CYBEX and both based on robust operational and administrative structures in the information-sharing platform. The Privacy-Preserving Cybersecurity Information Exchange mechanism allows cybersecurity information sharing without revealing the organizations' identity (Vakilinia, Tosh & Sengupta 2017). CYBEX-P platform addresses the inefficiency in dealing with cybersecurity problems by an individual entity. Exchanging real-time threat data helps organizations analyze threats to predict and prevent future cyberattacks. CYBEX-P -mechanism consists of three parties (Client organization, CYBEX-P, analysts, or researchers) throughout the lifecycle of the threat data where the client organization acts as a source of threat data.

According to Sadigque et al., (2019), CYBEX-P works as the intermediary between all organizations and data analysts by sharing any external or internal threat data sources they want. Threat data may be machine-generated or curated by a security specialist. The processing server in CYBEX-P has a TPM Trusted Platform Module (TPM), which checks the software and hardware integrity running in the processing server (Sadique & al., 2019).

Making Security Measurable (MSM) of the MITRE classifies data and standardizes data formats and exchange protocols (MITRE 2013). MSM comprises cybersecurity architecture for managing and measuring where current standards are divided into processes and set to six data areas referring to a process (in parentheses): asset definition (Inventory); configuration guidance (analysis); vulnerability warnings (analysis); threat alerts (analysis); risk/attack detectors (intrusion detection); and incident report (management) (MITRE 2013). In many cases, the fundamental structure of the information-sharing mechanisms does not differ significantly. Therefore, it is suitable to continue on this issue in the conclusions.

Discussion

Cybersecurity information sharing is not precisely defined in the area of cybersecurity. The structures of information sharing models are generally very sector-specific and are created in different environments. There is a need at the EU level to determine the development of a common Early Warning Solution. Usually, the word ‘warning’ also refers to preventive functions as U.S. intelligence services operate. Combating hybrid threats requires deeper integration of governance systems in the future. Detected significant data of hybrid incidents must be able to share directly from the accident site with national participants, such as cybersecurity centers. It is essential to allocate reliable additional information to determine boundary anomalies. Combining information pieces to ensure accurate and reliable information sharing is essential. Relevant information should be processed in the format desired form by the participants. Cyber defense activities should be integrated and automated according to local capabilities, authorities, and operational needs.

The shared common operational picture means that real-time communication links from the local level to the national and EU level exist. A common cyber situational awareness is needed for operating CPS and emergency and crisis management. There should be a connection between cyber situational awareness functions and emergency management.

Factors, as follows, that may affect the requirements of system features are essential to consider in developing an early warning system at the EU level. If some EU Member States may leave the early warning system, a challenges fight against threats arises. Therefore, there is a need to involve stakeholders in the values of the western world. It may create added problems if member countries or intended future member countries begin to protest against western values after joining a common early warning solution (Edgington, 2020; Tidey, Gill & Parrock 2020). Thirdly, the ability to utilize some elements of the EUs´ Early Warning System to NATOs´ Cyber Situational Awareness Solutions is crucial. The evolution of systems has not been separated. These factors are directly linked to confidential information sharing and exchange (Ilves & al., 2016).

What other factors have to take into account in the designing of the system feature process? National Cyber Security Centres ability to cooperate with other organizations within critical infrastructure at the national level is essential. The state departments of the United States work closely together to fight against threats in cybersecurity, and the organizations of public administration in the European Union work together more formally.

The European community must solve its general problems related to cohesion before permanent and joint solutions can be built. Despite this does not prevent the designing and development work of operating models, this factor must be taken into account when developing new systems. Confidence between member states must be on a stable western basis.

There are no markable obstacles to increasing collaboration concerning the development of early warning solutions among the U.S., NATO, and the EU (Ilves et al. (2016). According to Dandurand & Serrano (2013) Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) provides a knowledge management tool for the NATO partners. The U.S. Cybersecurity Sharing Act and Europe´s directive on Network and Information Security (NIS) have similar aims. Furthermore, the EU and NATO signed a technical arrangement in 2016 to enhance information sharing between the NATO Computer Incident Response Capability (NCIRC) and the EU Computer Emergency Response Team (CERT-EU) (Ilves et al., 2016). A Joint Early Warning solution would create a practical and efficient way to respond to cross-border hybrid threat situations.

Therefore, all significant enterprises whose businesses are related to critical infrastructure should be connected to an early warning system. Legislation, bilateral agreements, data management standards, and certifications need to be brought to an acceptable level of privacy before closer cooperation on information sharing can be achieved. The knowledge holder controls the principal capital in an intelligent society. Protecting privacy and preventing crime is part of the Western tradition.

4.8 Article VII: Comparing Cybersecurity Information Exchange Models and Standards for the Common Secure Information Management Framework

Background and the formulation of the study

The study's VII primary purpose was to compare and find out differential and unite factors of existing cyber information sharing models and information management frameworks in western countries. The purpose was also to find out factors that affect the utilization of the Early Warning System for the ECHO stakeholders. The paper supports European ECHO Early Warning Solution collaborators and European politicians. It also provides attributes of existing information-sharing models to identify and consider territorial, organizational, managerial, legal, and societal dimensions of the existing information-sharing solutions, models, and frameworks. The study will form a new database for the Echo Early Warning system concept. The Echo-Early Warning System's goal is to develop security operations support tool enabling the ECHO member's network to coordinate and share information such as incidents and other cybersecurity-relevant data in near real-time within the ECHO network.

The research's sub-question focused on how it is possible to integrate cyber information sharing models from the US into Europe. The need to protect information sharing, information management, and practices within the E-ECHO consortium is essential. The research proposes an initial risk management framework for the early warning system.

The purpose is to classify information-sharing models and frameworks into their groups. Some information sharing models, frameworks, and information management frameworks are simple diagrams, some complete templates with instructions, and some information sharing models have concrete instruments and tools. The analysis aims to find out the functionalities, applicable standards, and features of information-sharing systems in the EU, USA, and NATO. The research outcome is a combined proposal of an information-sharing model and an initial risk management framework.

Define information-sharing goals

In designing early warning solutions for various national organizations of the EU member states, it is crucial to identify essential requirements that participants have to allow.

Skopik, Settanni, & Fiedler, (2016) divide a set of the main elements of security information sharing as follows:

- Coordinated cyber defense requires cooperation and economic coordination. Different data classifications are needed for multiple stakeholders.

- Legalization and Regulatory means information sharing require a legal basis. The European Union and the US member States have already set directives and regulations.

- Standardization efforts mean enabling information sharing. Standards and specifications need to standardize to comply with legal requirements (e.g., NIST, ENISA, ETSI, and ISO).

- Regional and International implementations mean that these standards and specifications, organizational measures, and sharing structures must be realized, integrated, and implemented. CERTs and national cyber security centers work on this issue.

- Technology Integration into organizations means sharing protocols and management tools on the technical layer that need to be selected and set into operation.

Identifying internal sources of cyber threat information

A first step in any information-sharing effort is identifying sources of threat information within an organization. According to the (NIST, 2016) the process of identifying threat information sources includes the following sections:

- Identify sensors, tools, data feeds, and repositories that produce threat information and confirm that the information is produced at a frequency, precision, and accuracy to support cybersecurity decision-making.

- Identify threat information that is collected and analyzed as part of an organization's continuous monitoring strategy.

- Locate threat information that is collected and stored but not necessarily analyzed or reviewed on an ongoing basis.

- Identify threat information that is suitable for sharing with outside parties and that could help them more effectively respond to threats.

Results

The main findings are that unclear allocation of responsibilities in national government ministries and departments prevents authorities from fighting together against hybrid threats (cyber-physical threats). Responsibility for developing cybersecurity is shared among too many developers. Operational work on cyber threat prevention between European public security authorities would be more standardized and with a more centralized information management system. Public safety organizations in the EU Member States need continuing risk management and proactive capabilities in their information systems to keep society's critical infrastructure protected. The sharing of responsibilities for standardization concerning information management systems and cyber emergency procedures between authorities and international organizations is unclear.

The structure of the information exchange mechanism type called ISAC often has a central hub that receives data from the stakeholders. The hub can reallocate the incoming data directly to other members or send the updated information or data to the members. In addition to that, the hub may operate as

an information-sharing “separator”, it can protect the members' identities. The focal task of the ISACs is to share information on intrusions and vulnerabilities. These types of information are usually sensitive and problematic; thus, companies often decide to keep silent about vulnerabilities. ISAC hub system relies on the hub's functionality, which makes the system vulnerable to delays and systemic failures. Important information may be hard to achieve and delays in information sharing can reduce the benefits of the information-sharing hub mechanism. In a post to all model, stakeholders share information without control.

MITREs model is one kind of hybrid information-sharing model. It is a partner for helping private or public organizations stand up and run information-sharing exchanges. The mechanism of MITRE uses automated processing of information. This work has enabled security automation in vulnerability management, asset management, and configuration management through the Security Content Automation Protocol program. Members of MITRE do not share information. Each participant sends its sensitive data to MITRE, and MITRE works diligently to ensure that member data is kept confidential

There is a need to develop Public-Private information-sharing models at the EU level because public safety organizations of the Department of Homeland Security in the USA can handle external threats more effectively. International organizations like the UN (United Nations) and NATO have formulated a co-operational working environment so that the western world could operate for a common purpose. Those organizations are the uniting factors concerning harmonizing information-sharing procedures within the EU and USA. This form of collaboration framework represents information sharing as a “square.”

The system integrity requirements mean that separate information system-related standards must process with the information-sharing methods as one wholeness when the purpose is to design a common cyber ecosystem for the western stakeholders. Interoperability should be coordinated through standards, as FIGURE 15 illustrates.

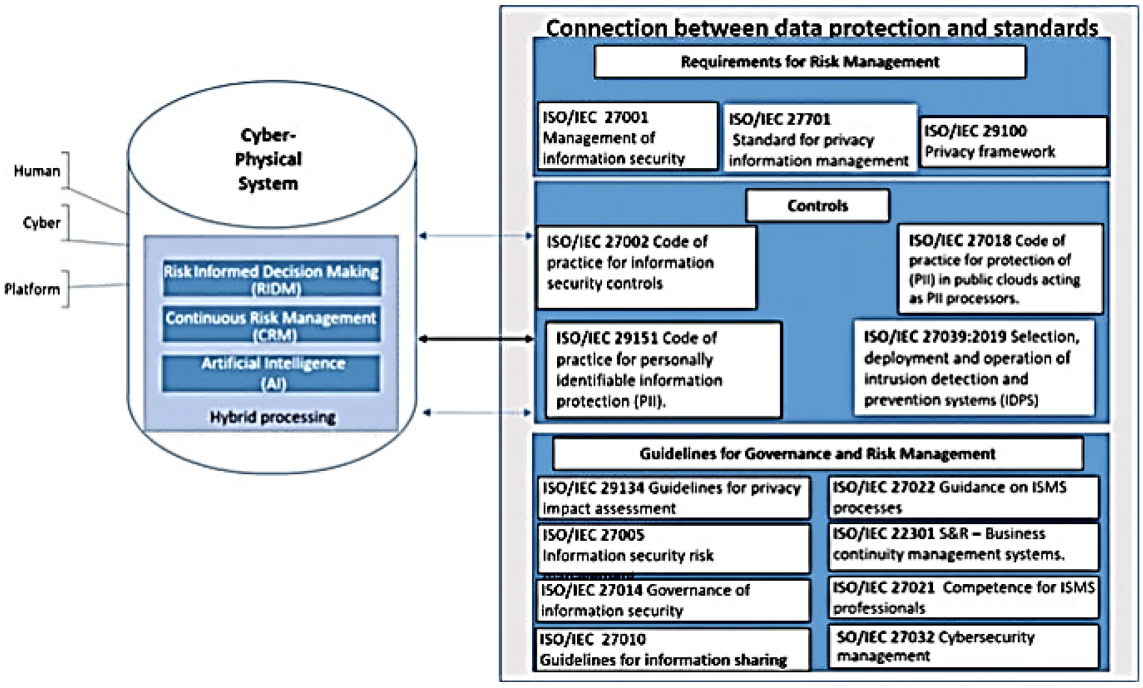


FIGURE 15 Standards supporting Continuous Risk Management in CPS

Efficient protection of critical infrastructure requires interfering with the activities of the criminal attacker. In the Cyber-Physical System, automated physical actions mean physical and cyber-defense functionalities against the attacks, but everything must be processed by following existing standards.
Privacy impact (PI) is a crucial element in all situations when the purpose is to develop a system that handles privacy identifiable information. PI could result from the processing of Privacy Identifiable information (PII).

According to ISO/IEC 29134:2017 (International Organization for Standardization, (ISO), 2017) a Privacy Impact Assessment (PIA) is a tool for addressing the potential impacts on the privacy of a process information system, program, or device. It will inform all participants who have to take action in order to treat privacy risks. PIA is an ongoing process, and the report may include documentation about measures taken for risk treatment. Measures may emerge from the use of the ISMS.

At a general level, a collaboration between the cyber-physical system and continuous risk management is required. CPS consists of three central stages for that; human, platform layer, and cyber layer, as FIGURE 15 illustrates, but in addition, the proposed framework requires considering standards and information management when the purpose is to develop common early warning solutions for the stakeholders.

At the technical level, the challenge of semantic interoperability is that information system should automatically understand the concepts arising from the actions of people and organizations. Therefore, it is important to create a common risk management framework for both. It is possible to connect different kinds of decision-making strategies to the cyber-physical framework, as the

proposal illustrates above. Legislation and regulation must be the fundamental basis for all functions and operations.

This means that the fundamental frame of the cyber-physical system is based on legislation, rules, and standards. The operations of the central EWS system must be based on transnationally accepted guidelines and standards. Semantic interoperability means that an information system can combine the information it receives from different sources and process it to preserve the meaning of the information. E.g., there are business-related differences concerning sector-specific stakeholders of the ECHO consortium.

Discussion

The paper states that separate hybrid threat prevention functionalities between the EU member states are not the only problem. A significant problem of information sharing models is related to the lack of real-time cyber information management among participants. There is an essential problem with the features of information-sharing models.

Protecting critical infrastructure, public safety organizations in European Union member states need proactive features in their information systems. Real-time communication links between the states and transnational corporations must exist for the shared common cyber situational awareness.

Legislation is not the only factor that affects to complete secure cyber-ecosystem. Developed systems need a coherent way for standardization, a common management system, and a governance model. The US public safety cyber defense organizations can combat cyberattacks but also make counterattacks (Smeets, 2019). The capability to do counterattacks is one of the most important features in protecting the western world. Therefore, Collaboration in the triangle EU-NATO-USA is essential. In addition, The United Nations acts as the fourth element. Utilizing the best features of the information-sharing models will ensure continuity of management procedures. Legislation of the EU member countries has been harmonized, but the occasional is to trust the organization's functionalities. A common continuous risk management system helps to handle the databases concerning privacy issues. Lack of standardization may cause obstacles when the aim is to catch cybercriminals or find out the state-level actor that has caused a cyber or hybrid attack.

4.9 Article VIII: Enhancing the European Cyber Threat Prevention Mechanism

Background

The study PVIII will explore those factors (requirements) which affect the conversion of a national EWS to a common early warning ecosystem at the EU level. Every EU member country has a discrete solution for monitoring and protecting the cyber ecosystem. The research will determine how to implement the national cyber threat prevention system into the EU-level Early Warning

System. Lack of cooperation with threat information sharing between EU member countries affects public safety at the international level. Separate operational functions and procedures between national cyber situation centers create challenges. The main obstacle is that European Union does not have a common cyber ecosystem related to cyber threat intrusion prevention and detection systems because some countries set privacy issues and citizens' security as topics against each other. The research will comprise a new database for the ECHO Early Warning System concept.

Concentrating only on monitoring the internet traffic does not support proactive features of early warning solutions. At least public safety authorities should have a wider possibility to access the organizations' information systems and communication because the Internet of Things (IoT) is changing using Artificial Intelligence. Electrical and telecommunication cables are placed in the same pipeline more widely. Thus, possibilities for vulnerabilities will increase.

The HAVARO, organized by TRAFICOM (the Finnish Transport and Communications Agency) and NESA (National Emergency Supply Agency) is a national early warning system that gathers threat-informed data and produces crucial information concerning the situation of cybersecurity information sharing within critical infrastructure. The HAVARO service is now under development. Instead of being a government service, HAVARO 2.0 will be jointly provided by commercial operators and the NCSC-FI. Part of the events will be processed and reported by information Security Operations Centres (SOC).

The purpose of the HAVARO 2.0 project is to create a trusted network in which the members can exchange information better than before. The HAVARO 2.0 Early Warning System will upgrade features of the existing 1.0 system by developing early-warning features to work more effectively. Existing cyber-threat sensor systems need more specialized detection features. Increasing the cyber-threat atmosphere will force stakeholders to develop a better and more efficient system. Separate forensics methods, gathering logs, gathering information, reverse engineering, and analyzing risks are not enough in the future. It is crucial to produce added value by combining different data sources and weak threat signals. HAVARO 2.0 will only be complementary to other cybersecurity services.

HAVARO 2.0 will include the GovHavaro feature (Lehto et al., 2017). That means that there will be a connection between public organizations and the HAVARO Early Warning System. This information is classified as more confidential, but sector-based sharing requires the sharing of this information to all public safety organizations and to the central government. The threat information is essential to be shared in real-time with the stakeholders if cybersecurity information related to other countries or threat information generates a common risk to vital functions at the EU level. New stakeholders of the HAVARO 2.0 have contractual relationships with SOCs, not with the NCSC.

Outcomes of the paper

Several factors are essential to notice when the purpose is to integrate the national Early Warning System to the common European Union level Early Warning

System. First, cloud services are not a secure way to store and gather threat-informed data. When customers of the early warning solution are connected to the system from all around Europe, using cloud-only service solutions is not secure because cyberattacks against virtual machines may jam the whole system. Therefore, the authors recommend using a centralized main server that produces services to EWS stakeholders. This sharing model requires using local (national) E-EWS servers where ECHO-EWS is connected. This is one kind of hybrid model, but the model is a secure part of the architecture, allowing sharing of trust-level information. It is sensible that, for example, law enforcement can gather and share trust-level information concerning vital functions of society and have the ability to be connected to the Early Warning System. It is relevant that the early warning data is shared from the central server to the affected sectors. International researchers recommend using a controlled information-sharing model, where national public safety actors share relevant data to stakeholders via a centralized EWS Center (Department of Homeland Security), as FIGURE 16 illustrates.

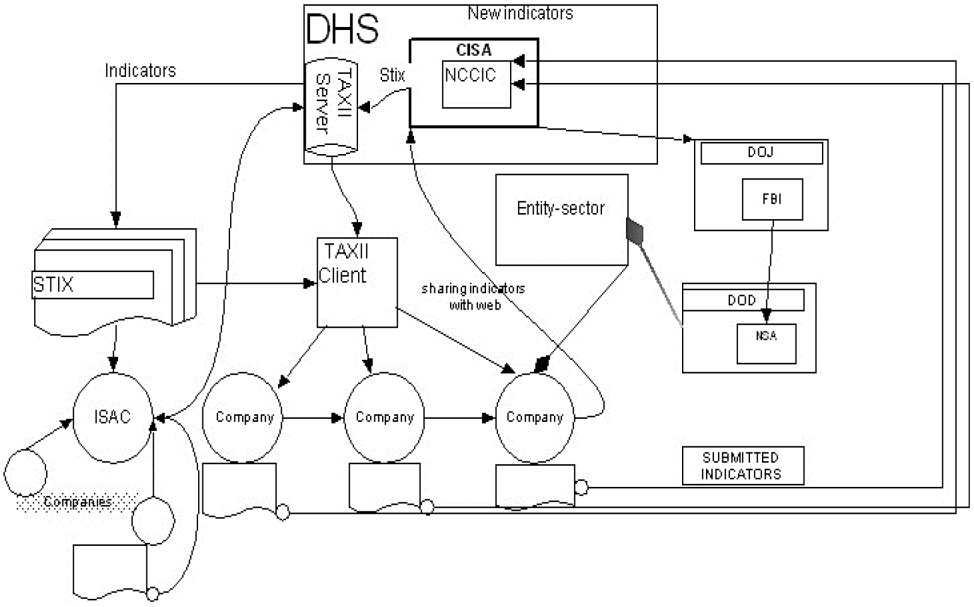


FIGURE 16 Cyber information-sharing model of the U.S. Department of Homeland Security

Two-way models also allow public safety organizations to use the gathered information to prevent hybrid threats before two or more separate phenomena cause the domino effect. Cross-border cooperation must work directly and instantly. Echo EWS will not work as a separate system but plays a crucial and parallel part in broader mechanisms, including the European -level situational awareness system of NATO. Thus, it is required to establish common taxonomies, techniques, procedures, and common ways to respond and act.

The U.S. Department of Homeland Security uses Automated Indicator Sharing (AIS) system. AIS utilizes the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII)

specifications for machine-to-machine communication. AIS participants may connect to a national early warning system in the National Cyber-security Center (NCSC) that allows bidirectional sharing of cyber threat indicators. A server housed at each stakeholder´s (community) location allows the stakeholder to exchange indicators with the National Cybersecurity Center (NCCC), as FIGURE 16 illustrates. Participants receive and can share DHS-developed observed indicators in their network defense efforts, which the national cyber situation centre will then share back to all AIS participants. Stakeholders who share indicators through AIS act anonymously unless they consent to disclose their identity (Hernandez-Ardietav & al. 2013). Official cyber-security partners will vet the indicators they receive through AIS. The government also needs useful information about indicators and other threat-informed data. Therefore, the national NCSC should share at least weekly reports with the government situation centre.

In summary, the essential outcomes of the paper are as follows:

- Preventing functions against cyberattacks but also identifying, tracing, and prosecuting a criminal/criminal group are essential features.
- It is possible to increase collaboration at organizational, tactical, strategical, and technical levels between national CERTs, NATO Computer Incident Response Capability (NCIRC), and EU Computer Emergency Response Team (CERT-EU).
- European Echo Early Warning Solution would create an effective way to respond to cross-border hybrid thread situations.
- All major companies whose businesses are involved with the vital functions of society should be connected to an early warning system.
- The National cyberthreat prevention mechanism HAVARO 2.0 is not enough. Critical information must be able to share between EU member countries because several enterprises operate internationally.
- Cross-border cyber threats force countries to exchange critical information within EU member countries and between EU and other western states.
- Operational public safety functions require a quicker response or even prediction. HAVARO 2.0 should utilize the Artificial Intelligence (AI) features to detect threats.
- The Artificial Intelligence (AI) functionalities generate added value because predictive features belong to the early warning system: it may conclude by learning from input information. The AI-based solution can make a decision without human interaction.
- Not every ECHO participant has the same opportunity to develop the national architecture for the early warning system.
- The international cyber-physical dimension of threats sets requirements of what should be the minimum cybersecurity level or requirements of cyber situation centers at the national level.

Discussion

The framework for local, national, and international information sharing should be designed with the same principles in each EU member country. FIGURE 17 illustrates the simple formation of cybersecurity information sharing and the shared cyber situational picture between countries where national HAVARO 2.0 may join. The example consists of separate national sub-hubs and one centralized hub at the European level. Stakeholders do not exchange information directly with each other. All threat-informed data is shared via the "governance" hub.

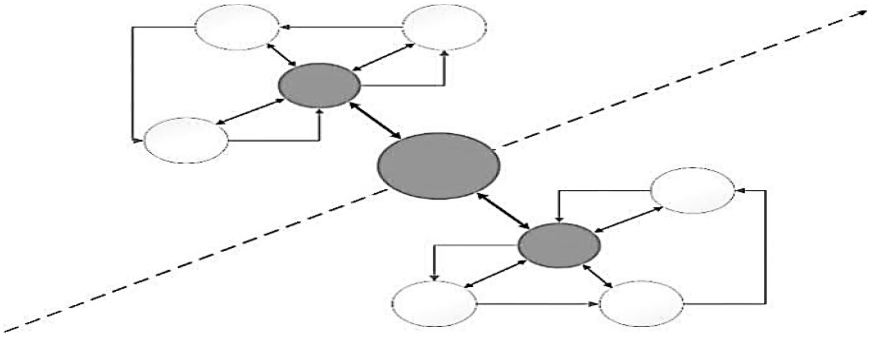


FIGURE 17 Connection between sub-hubs

National sector-based classification, where information sharing is based on Information Sharing and Analysis Centres -groups, is the optimal way to share classified information in critical infrastructure, as FIGURE 17 illustrates.

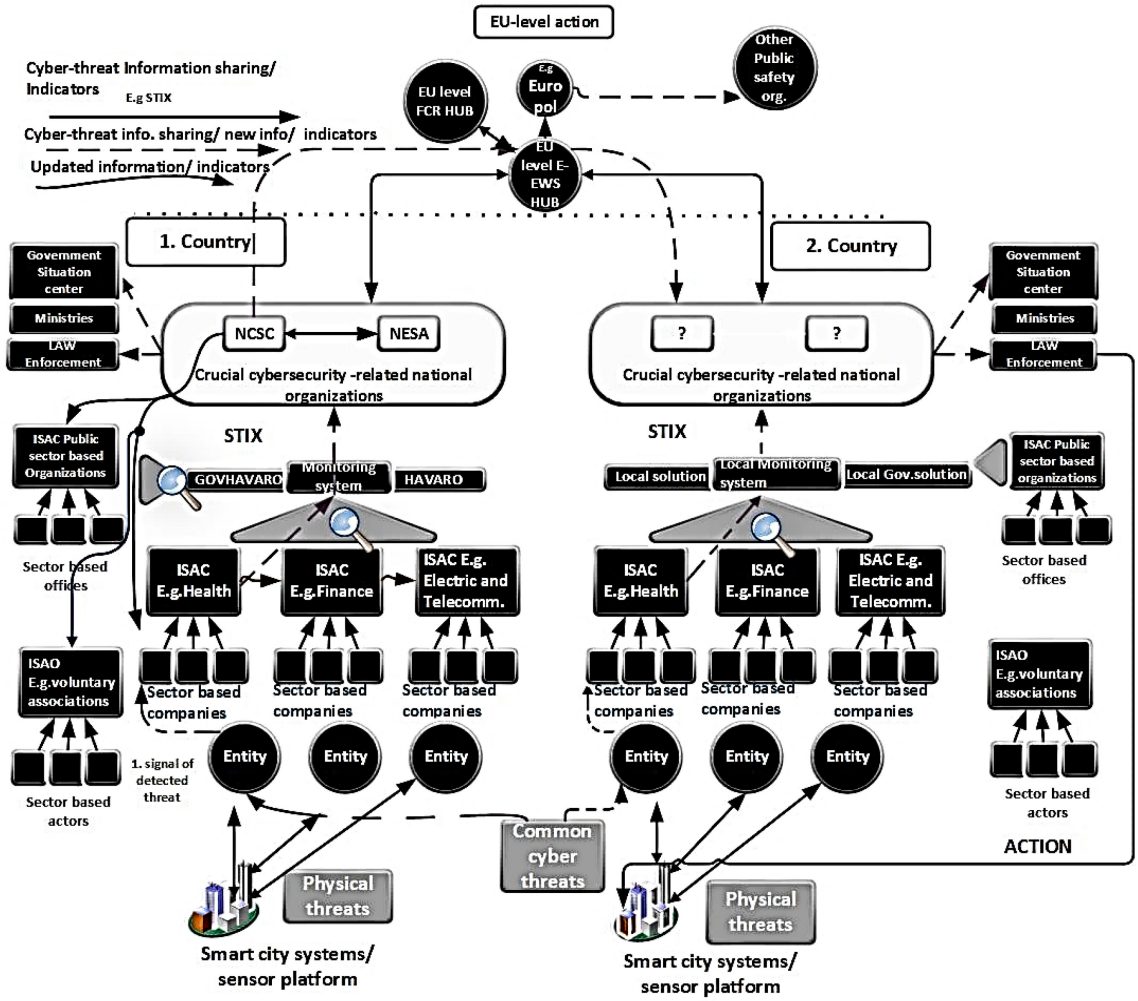


FIGURE 18 Proposed E-EWS information-sharing model with sharing mechanism

FIGURE 18 demonstrates information-sharing relationships and organizational structures concerning information sharing within a centralized hub system (countries, companies, public safety organizations, and other actors). Country-number 1 (Finland) demonstrates identifiers of the national Early Warning System (for example, HAVARO) that detect a weak signal of cyberthreat from Internet traffic in a multinational enterprise. The national cybersecurity center of country 2 has not detected a cyber threat activity. Automated Information Sharing functionalities produces crucial data for the central EWS hub, which shares relevant information in near real-time to the situation centres (CERT or CIRT team). Sensitive data will be shared directly with the international public safety organizations and/or with the governments which are associated with the cyberthreat. NCSC of Finland uses a parallel subsystem for public organizations; HAVARO consists of separate early warnings solutions named "GovHavaro" for all public organizations. Participants do not need to share information directly with each other, but there is a need to establish sector-specific communities—for example, ISAC and ISAO—that collect crucial information concerning the targeted sector of the critical infrastructure. This cybersecurity information is

monitored and handled by national CERT or CIRT, and cybersecurity centres will share all new indicators between stakeholders (ISACs). All law enforcement-related information will be shared directly via the EWS hub to the public safety authorities, such as EUROPOL or INTERPOL. Centralized EWS hub and sub-hubs are the simplest options for the national Finnish Early Warning System.
On the other hand, a big challenge will be who maintains the central hub and its governance model. Criticism concerning the use of STIX is justified, as mentioned above, and the problem needs to be rectified. More detailed guidelines, methods, standardization, and compliance with the law create a better operating environment to take advantage of automated indicator exchange.
Despite the invalidated privacy shield decision of the EU Court of Justice, there is a need to strengthen and be aware of hybrid threats from a broader perspective. Privacy issues are essential to protect. It is possible that the the privacy shield agreement needs to be changed. The agreement is significant in terms of commerce. Companies will now have to sign 'standard contractual clauses': non-negotiable legal contracts drawn up by Europe, which are used in other countries besides the U.S. (Court of Justice 2020).

4.10 Article IX: Saving Lives in a Health Crisis Through the National Cyber Threat Prevention Mechanism Case COVID-19

Background and the problem formulation

The research handles information exchange and the formation of the situational picture as a part of crisis management and how the proposed hybrid emergency response model may affect the formation of situational awareness in hybrid crises. The problems noticed in central administration and middle-level administration reflect challenges around reliable information sharing and the use of evidence-based information. The Ministry of Social Affairs and Health (STM) and the Finnish Institute for Health and Welfare (THL) have to protect citizens so that the diseases do not spread in Finland.

The research explicitly underlines the decision-making capability and formation of situational awareness of the Finnish government, the National Institute for Health and Welfare, and the Ministry of Social Affairs and Health. The paper concentrates on how to reduce the effect of dis- and misinformation in the state-level decision-making process. It is also discussed how it is possible to use a hybrid emergency response model to solve multiple problems around crisis management when several threats happen simultaneously. For example, united crises such as pandemics with cyberattacks can overload public safety organizations' workflow. If several overlapping problem-solving methods are used in crisis management, preventing the domino effect can become more challenging.

Situational awareness has been inadequate during the entire response period to the COVID-19 crisis. Even the general guidelines or information have not been shared with the citizens.

Challenges accumulate, becoming more challenging. Questions about legal jurisdiction have caused political debate. The responsibilities of officials and politicians have been unclear for some time. Secondly, by the law, public organizations' preparedness and action plans must be implemented. The political and administrative debate around the separation of powers between government ministries has caused significant problems in coordinating decision-making. We need more accurate real-time information and resources attempting to survive the challenges of daily routines around the virus pandemic while the potential for new incidents and crises increases. The overloaded patient care of hospitals makes it challenging to persist from a double major accident. The process of prioritization takes time from patient care. In addition, government resources are limited.

Sensitive patient data was stolen from the Finnish therapy center Vastaamo causing massive privacy breaches. Due to criminal activity, the social and healthcare system of Finland carried out an overloaded situation. Sensitive and personal data must be protected more effectively in the Finnish healthcare system and at the European level. Along with grave privacy breaches and the spread of misinformation through media and social media, several countries have faced the spread of misinformation that has driven divergence in people's perceptions and understanding of the facts around the pandemic. Also, decision-makers' ability to be aware of the actual situation has been difficult. False information sharing and exchange around crucial public health and safety-related issues have been a common challenge.

FIGURE 19 demonstrates the primary information sharing participants and how citizens form an understanding of the crisis from media (including social media) and state decision-makers. Foreign influencers, including the press, scientific researchers, authorities, and politicians, share their opinions. Information warfare causes pressure on citizens to find the correct information.

FIGURE 19 Formation of crisis information

The formation of an updating situational picture has been notably complex. Decision-makers (including politicians and authorities) have difficulty reaching reliable supporting data for decision-making. Thus, Finland and Europe need an early warning system that considers changing threat factors across the world more quickly. The capability to analyze raw data and find health abnormalities more quickly is an essential feature in the future.

Excellent preparation and coordinated action are required to respond against cross-border (health) threats before, during, and after the crisis. There is a need to gather data for strategic measures that must be implemented at the operational and tactical level quickly enough to stop crises like pandemics on time. Early Warning sub-solutions utilizing artificial intelligence can be the required missing part in such a rapidly evolving event process.

It is almost abnormal that an operational "power team," or even national science advisers, has not been used to advise the formation of a situational picture for the government of Finland. The EU was not acting as one front in information sharing and supporting aid to member countries under the COVID-19 pandemic.

Privacy-related threats in health services

As mentioned, the Finnish psychotherapy center lost its patient records to criminals. They can try to blackmail or otherwise influence the victims with the stolen data. There are several problems with the management and processing of health data.

Kanta is responsible for providing digital services to the social welfare and healthcare sector in Finland. According to Kela (2020), each organization associated with Kanta services has at least one Kanta-access point that can either be carried out as an organization's activity or implemented by the organization. Valvira is a national agency operating under the Ministry of Social Affairs and Health. It supervises Finnish psychotherapy service providers such as Vastaamo. Its information system belongs to the systems of Category B regulated by law. Class B patient information systems are registered with Valvira under the Customer Information Act. The law does not require an external assessment of data security.

Vastaamo itself developed its social and health care information system. Authorities monitor it only if there are security-related reasons to doubt problems or if the service provider requests it (Ranta, 2020). The criminals' activity against sensitive registers creates a need to effectively supervise information systems and information exchanging of commercial and public service providers. Data leakage threatens vital functions of society.

Problems in the crisis management

An international cross-border crisis can extend very quickly, as the COVID-19 pandemic has shown. Thus it is crucial that decision-makers effectively share essential information. The pandemic has also demonstrated that the preparedness levels of the public safety organizations are not sufficiently high. When Finland's citizens noted a lack of proper information around COVID19 at the end of February 2020, the decision-makers, such as responsible departments

under the ministries, failed to offer guidelines on how to protect against COVID-19 immediately. The Ministers of Social Affairs and Health did not know how to divide their tasks.

Managing the administration is thus becoming cumbersome. State leaders need decision-making support, such as via artificial intelligence tools, to enhance administrative efficiency. Information about the pandemic has been available to the decision-makers, but the preventive reaction has been slow. Scientific-based information from abroad has not been shared with the public.

The governments of the Nordic countries have made independent actions to prevent the spread of COVID-19. Finland changed its prevention strategy after the president interfered in the government's decision-making process. The ability of citizens to maintain situational awareness has been equally problematic. The technical solutions that had been in use for COVID-19 prevention did not enhance citizens' safety significantly.

Results

Finland's authorities of local and regional level administrations form situational awareness from the view of their territorial region. After forming a situational picture, authorities share regional instructions and guidelines with the people. So-called corona teams are responsible for regional security. Tasks are different from the government instructions at the regional level, and the government does not give absolute regional commandments, such as mandatory instructions for using masks. Continued unclear around the workflow is an essential obstacle when the aim is to share relevant information with the right audience at the right time. The labor movement or trade unionism can generate an agitating counterforce by means that are not ethically valid. The fundamental problems of social constructs have a more intensive role if the challenges to fight against the spread of crisis emerge from the citizens.

Finland does not have an operational command and control institution for suddenly evolving crises. The president leads foreign policy with the government, but there is no operational commander role for the president in the country's internal affairs. The ongoing COVID-19 crisis has shown that there is a lack of information exchange among the authorities and politicians. Thus citizens have likewise been kept unaware of the guidelines that should be followed. Information security of small- or medium-sized social and healthcare companies and public safety organizations based their oversight on self-monitoring. A single employee of the National Supervisory Authority for Welfare and Health (Valvira) supervises privacy issues in the Kanta register (National Supervisory Authority for Welfare and Health, 2020).

More challenges for health organizations are that a data breach may occur long ago before officially detected. -This may create a possibility where criminals try to affect the decision-making process by blackmail.

There are no crucial privacy issue-related barriers to using the proposed hybrid emergency response model with health sensors within a smart city infrastructure. An alarm-based early warning mechanism that automatically senses data leakage offers possibilities to improve protective functions such as

privacy protection (Simola, 2020). The proposed hybrid emergency response solution may also use flu sensors, which can transfer data in real-time from a shopping center to the Hybrid Emergency Response Center.

The early warning data, such as data of the virus particles, might then indicate a need that would allow for mall closure to be carried out immediately.

Discussion

It would be recommended that the government of Finland uses scientist experts as advisors in the decision-making process when something occurring happens regarding a whole state area. It is a general way in Europe. Decision-makers can find, for example, classified studies from foreign sources on how the coronavirus spreads and how its spread can be prevented.

First, there is a fundamental need to regulate new guidelines for the higher-level crisis management and command relationships for exceptional circumstances.

Temporary provisions should be made for emergency situations, which may require imposing restrictions on citizens. There must be one leader team whose major leader is from the central government of Finland. This leader should take control of the emergency leadership when adjutants have too much contradictory information to share. Human capabilities set limits to gathering the proper information in a time of crisis. There have been too many assistants involved in the decision-support process at the state level.

The future solution may form around artificial intelligence solutions in a way that supports decision-making. The proposed next-generation hybrid emergency model uses artificial intelligence based on a multiagent system to generate information for decision-makers. As FIGURE 20 demonstrates, the crucial factors in the hybrid risk management framework are risk-informed decision making (define risks and information), continuity risk management (handle risks continuously), and hybrid emergency response solutions (emergency operations). Decisions still are based on human thinking activity, and people are responsible for their decisions. However, it is possible to combine human-based guidelines for risks and AI-driven decision-making (Colson, 2019).

The proposed model offers two possibilities for using automation. Firstly, automated protection functions are implemented in semi-public spaces (e.g., shopping centers) and public open places (e.g., gardens). In an optimized situation, a health sensor called "flu" may begin an evacuation process if it indicates several deviations from the settled values. At the second level, an AI-aided decision support mechanism handles a massive amount of data using OSINT and produces analytical reports for state-level decision-makers. The decision-making process will enhance because the need for assistance workers will reduce in high-level decision-making.

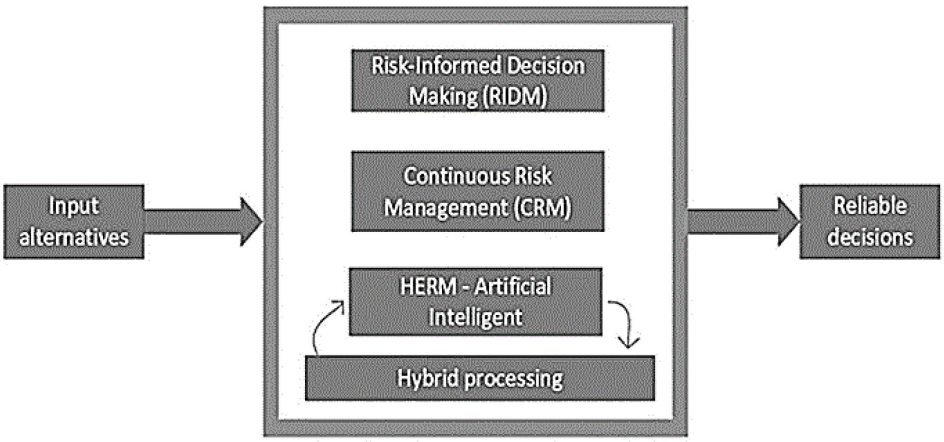


FIGURE 20 Reliable Decision-Making process

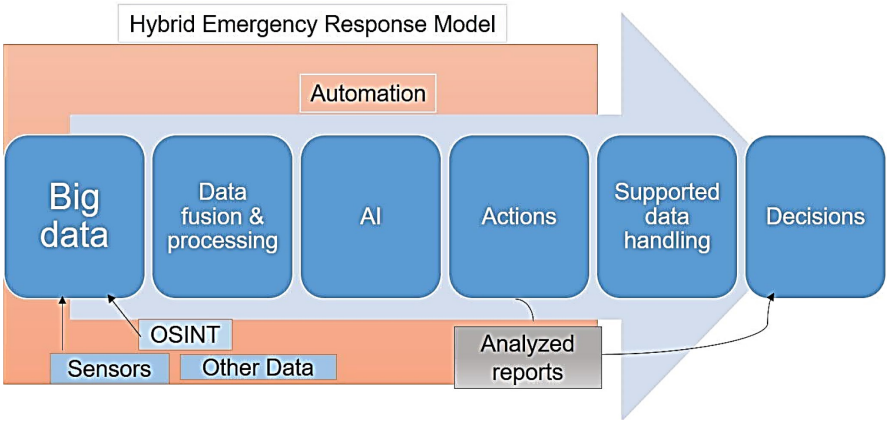


FIGURE 21 HERM with 2-level artificial intelligence features

As FIGURE 21 shows, the information sharing process of the authorities must reflect automated functions. High-level decision-makers desire to maintain control over their decision-making ability may prevent the utilization and usefulness of the proposed smart hybrid emergency model. It has been a trend that aspects and opinions of the political parties be more represented than rational-based decisions, as case covid-19 proved. Cyber preparedness, operational preparedness, and reliability of decision-making belong to controlled continuity management. The possibility of combining different level decision support functions into a single entity is real, but this does not require fusing all elements in one physical location. It is an essential requirement that a decision support mechanism is developed jointly with the crisis management system.

When the government of Finland tries to maintain situational awareness, it is not enough to use just a few sources for the data gathering. Legislation concerning privacy issues does not cause permanent obstacles to using sensors in the smart city environment as a part of the hybrid emergency response model. It is essential to rationalize organizational responsibilities for the development of overall security. Human inability to detect abnormalities in the environment

under observation and data transmission and information sharing weaknesses limits the effective cooperation between politicians and authorities. Containing preventive activities into the intelligent society as part of the emergency model is a crucial part of overall security preparedness, situational awareness, and critical infrastructure protection. In practice, the analysis of global research data on pandemics can be automated. The developed infrastructure of society and smart cities needs more accurate, standardized information systems and common guidelines for all information systems handling sensitive information.

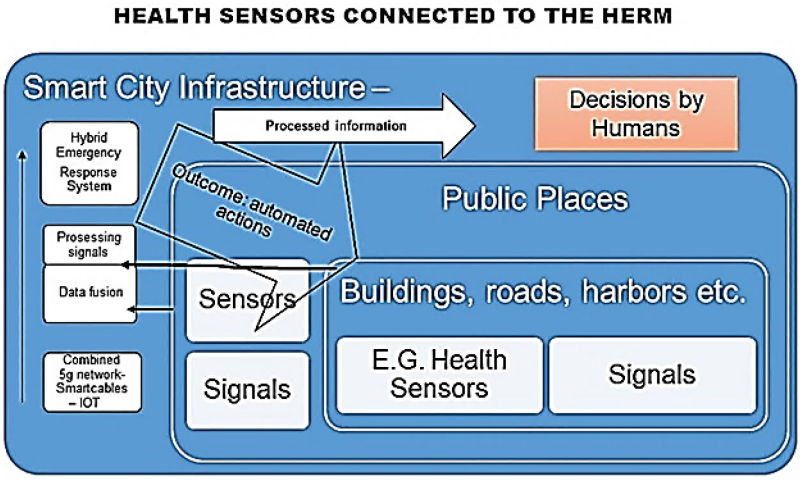


FIGURE 22 Health sensors connected to the HERM in a smart city

The challenging COVID-19 crisis requires us to change the ambition of digitalization into concrete actions. The hybrid emergency response model for smart cities offers solutions to many problems and questions. FIGURE 22 demonstrates how different elements are linked to each other. The model may use health and traffic sensors in a predictive way that supports decision-makers' daily work. The proposed model does not remove the potential realization of cyber threats, but it will enhance decision-making and common situational awareness.

5 CONCLUSIONS AND DISCUSSION

This chapter handles the answers to the research questions and discusses the limitations of the dissertation and reliability and validity issues. All sub-questions have been dealt with separately, forming a summary of the main question.

Despite the direction of the political will, our basis of the societies is not almost equal compared to each other. Every country has its ambitions to develop its smart technologies. The proposed requirements and features offer needed elements that form the framework for the European-level public safety actors and create a set of requirements for developing the system. European Union is also a security community even the union does not have a common centralized defense force. The member countries of the EU need a standardized joinable early warning emergency system for western cooperation that applies a cyber threat detection system. Cyber elements have to work coherently in different physical environments.

5.1 Answers to the research questions

The research comprises one main research question and five sub-research questions. The main research question (RQ) is

RQ How do elements of the cyber ecosystem impact in traditional Public Protection and Disaster Relief?"

Sub-questions are

RQ1. How to improve cyber preparedness level within PPDR authorities from local to national and international level as a part of PPDR services?
RQ2. How to improve and combine emergency response procedures by using the cyber security dimension?
RQ3. How do intelligent technologies affect to PPDR -organizations and central government?

RQ4. How hybrid emergency response model affects maritime security?
RQ5. What are the main obstacles to the implementation of the new system?

RQ1. How to improve cyber preparedness level within PPDR authorities from local to national and international level as a part of Public Protection and Disaster Relief services?

Articles I, II, III, V, and VI will answer this sub-question. In this context, cyber preparedness means enhancing cyber situational awareness by using digitalized information-sharing methods, processes, and procedures. Cyber preparedness-level improve by enhancing processes and procedures between the public safety organizations (Articles I, II and III). Cyber threat information has to be shared within a trusted framework that uses standardized logic, as articles VII and VIII demonstrate. Also, the relevant information has to be available in a form that every participant understands its content at every level (Article VII, VIII and IX). The information has to share in a standardized way: every participant, both public organizations and enterprises. When the purpose is to protect vital functions, Cyber-threats have to identify and detected before any incident occurs.

The proposed Hybrid Emergency Model will take into account separate threats that threaten society. —developing a proposed hybrid model with artificial intelligence elements that take into account all privacy issues is important. Cross-border threats set requirements to standardize "rules" to Public Protection and Disaster Relief service. Protocols, standardization, and regulation comprise required elements for information handling, sharing in the same way with every participant involved. These elements have to promote. Cyber situational awareness as part of Situational Awareness has to be understood in the same way in every collaborated country.

At present, we already have automated systems situated in the structure of the buildings and public areas. For example, water sprinklers start to operate when the heat has risen high enough. Transmitted data from the sensors to the sprinklers also inform the local fire brigade. That is not enough, and false alarms cause additional resource problems by using solutions that do not use artificial intelligence-based solutions. Smart platforms offer more features to detect and prevent false alarms.

The hybrid emergency response model will use Artificial Intelligence to reduce the need for human resources. AI-based multiagent systems will reduce false alarms that burden public safety services. That also affects the cyber-preparedness level when handling the cyber ecosystem as a more expansive wholeness. It also includes raw data handling and analyzing. Authorized national cyber emergency response organizations will get more tasks because of the digitalizing safety culture. Proactive AI-based multiagent elements include data gathering, handling, analyzing, and classifying by using for example OSINT -tools. Soon, all-electric and it-cables be combined in the same channel. Infrastructures of smart cities require more automated public safety features.

Local and regional stage operational PPDR services need trusted information from the cyber-threat prevention mechanism to prepare for a

potential threat. For example, the data from abroad have to reach actors at every stage. Standardized systems and data handling procedures allow forming data and sharing information to be understandable. For example, ongoing COVID-19 -time shows that regional state administrative agencies have taken a lot of regional responsibilities concerning pandemic restriction decisions under the government's guidelines. The proposed Herm will provide an efficient decision-making mechanism using AI-aided multiagent systems. The same information is available at every stage of the state. Automated "smart" features begin to operate at the same time when participants will get information about the threatening incidents. At the same time, decision-support features create reports for the decision-makers, as article IX demonstrates. European business continuity management will enhance along with international business due to the enhanced hybrid-threat information sharing within information sharing groups. Also, operational human-based work of the public safety organizations reduces at all levels.

RQ2. How to improve and combine emergency response procedures by using the cyber security dimension(domain)?

At the state level, public administration and organizations have separate cyber threat detection systems and computer emergency response teams, as articles I, II, III, and IV indicate. Most often, national Emergency Response Centres answer citizens' emergency calls without knowing what has happened. Their system is not connected to any cyber-physical warning system that could detect early warning situations before any emergency calls.

The situation center in the parliament is not gathering and sharing real-time data about the physical, cyber, or hybrid threats continuously. TRAFICOMs National Cyber Security Centre has Havaro 2.0 system that tries to prevent crucial cyber threats with centralized systems that is not proactive enough. Companies can join it voluntarily. Govhavaro is designed for public safety organizations and has a more secure mechanism for sharing sensitive threat information. As articles I and II demonstrate, there is a need to enhance interaction and transaction between the systems using a standardized (API) Application Program Interface that reduces connectivity problems. API allows combining different protocols, routines, and tools in a form that cyber information is possible to gather and share between the stakeholders. We need more advanced artificial intelligence solutions to lighten the procedures of the PPDR functions. Digital infrastructure needs to be developed in urban areas in parallel in the different EWS-participating countries. One challenge is that our public administration is quite massive for the 5.5 million people. There is a need to prioritize the use of resources.

As article VII indicates, at a general level, a collaboration between cyber-physical system and continuous risk management elements is required. Standards and information management must be considered within the proposed framework when the purpose is to design common early warning solutions for the stakeholders.

At the technical level, the challenge of semantic interoperability is that information systems should automatically understand the threatening risks arising from the actions of people and organizations. Thus, it is essential to create a common risk management framework for every organization joining the early warning solution. The crucial advance is the possibility of joining an enhanced decision-making base within the cyber-physical framework—the basic frame of the cyber-physical system based on legislation, rules, and standards. European EWS should be based on the same basic principles. The system's operations must be based on common guidelines and standards, as article VII indicates.

The requirement of semantic interoperability means that connected information systems of the hybrid emergency response model can gather and federate the data it receives from the physical and virtual sensors and process it into a united, understandable form to maintain the meaning and content of the data. The recipient unit must understand the content of the sender´s data, whether it is a human or an automated artificial intelligence system (Article VII). Cyber-physical understanding means a seamless environment of the interfaces.

RQ3. How do intelligent technologies affect to PPDR -organizations and central government?

Almost all level decision-making in society is based on human resources. Political systems that we have to require human resources. Functioning public safety sectors need a shared situational awareness. Efficient and proper content of information to share is a crucial issue when protecting critical infrastructure. When using artificial intelligence for analyzing data for decision-makers' decisions, also trusted information sharing between the authorities and confidential data stays safe. Decision-makers need reliable information that does not expose them to hazards. Artificial Intelligence-based systems reduce human weaknesses in information-sharing procedures that affect to the formation of situational awareness. Information sharing procedures will enhance by using standardized Artificial Intelligence -based solutions in the urban environment. Situational Awareness becomes an ever-updating state of understanding.

Legislation is changing, but there is no space to use artificial intelligence-based technology to reduce human resources. Articles III, IV, V, VIII, and IX prove that artificial Intelligence with a multiagent sensor system will enhance efficient decision-making at all administrative levels and stages. Despite that, technical errors may also cause crucial problems even if the system works only by using the semi-automated capacity.

Internet of Things, robotics, intelligent machines, and smart devices belong to the developed society. Intelligent system infrastructure will change public safety culture, because of changing emergency response procedures. Automation works mainly without human-based work. That leads to enhanced procedures of the public safety organizations. Automated information sharing and operating features release resources and capacity from the overloaded Virve-network to the other stakeholders. The reduced need for Virve-communication

and operational fieldwork reduced the need for human resources in separate C2 or situation centers.

Intelligent technologies will produce more accurate information for the decision-makers and personnel at the central government. The decision-support mechanism will alert decision-makers if their plan to decide something has included threats or if something is acute. Central Government will also reach all relevant data about incidents and threats immediately. A major catastrophe such as a pandemic requires immediate decisions from decision-makers, and AI-based sensor technology will offer proposals to solve the challenge. All usable and informative threat data has to be available and accessible.

RQ4. How hybrid emergency response model affects maritime security?

As article II indicates, Coast Guard patrols cannot share real-time information with other patrols or the MRCC Turku. Command and control functionalities have to be designed towards a combination of a new kind of hybrid sensor technology that uses OSINT tools and artificial intelligence solutions in order to detect threats in advance because a cyber situational picture is needed for detecting inner and outer threats including threats against information systems. For example, drug trafficking can be prevented by using more effective multiagent intelligent.

The presented model affects in many ways to maritime security, because of the centralized concept that uses, e.g., OSINT techniques to identify threats. Gathering, harvesting, processing and comping data as article II states will produce more effective tools against maritime-related risks because of the predictive features that will efficiently improve whole maritime security. Stakeholders have to trust that cross-border transportation continues despite the threats. The HERM will offer the required tools for protecting the cyber domain when processing raw data on anomalous behavior in advance. E.g., combined information from the internet, shared data from trusted collaborators via early warning hub, and other geo-information produce essential information for maritime security. For example, the identified ship may cause danger in the harbor or sea area if the contents of the cargo is abnormal, or the ship is used for a different purpose than what has been informed. The AI-aided Emergency Response Model offers added value when available human resources are limited, as article II demonstrates. MRCC Turku handles emergency calls, and the answering capacity is limited. The tasks have to prioritize when a major incident occurs.

RQ5. What are the main obstacles to the implementation of the new system?

The main obstacles are related to political views, regulation, infrastructure, technological and standardization aspects.

Article III compared current emergency response processes to the proposed Smart hybrid emergency process model. The research examined the effects and factors which prevent the implementation of the architecture. Article III indicates

that technology-related legislation sets crucial challenges, and it also indicates challenges with standardization (Article VII). Also, organizational maturity level indicates challenges that arise from organizational differences. Others operate under the municipalities, and others operate under state administration. The same governance and mandate-related challenge relate to differences in the governance of ministries. E.g., the emergency services act under municipalities and ERC acts under the ministry of interior.

As articles III, V, and VIII define separate organizational governance and the culture of governance is a crucial factor affecting the implementation process. At the local level, the meaning of organizational and sector-based issues arises because every unit depends on their organization procedures to do their fieldwork. There is a lack of co-operative synergy between the authorities, as PI indicates. Administrative, especially regulatory factors, cause part of the jurisdiction challenges. At the regional level, administrative working tasks are dominant responsibilities of work and specific issues intermingle and expand across operational boundaries. Administrative obstacles reduce situational awareness because of overlapping work descriptions at the regional levels of state administration.

At the state level, we have security-based responsibilities that have separated between different ministries. No centralized actors would be administratively responsible for cybersecurity activity or critical infrastructure protection. Local- and regional-level administrative challenges are due to the divided responsibilities at the state level, which is an essential obstacle. Organizational responsibilities should be rationalized. Another essential factor is related to the change of political power. Functioning proactive systems require a stable society. Political decision-making and continuity management have to move in the same direction. If political power changes and extremism arises, also problems arise because of the controlling features based on artificial intelligence -features (Article IV).

Also, lack of standardization prevents to implementation of the proposed system, as article VII indicates. Several standards should be introduced wider in critical infrastructure sectors. Those standards handle organizations' systems and structures, organizations' ways to share information, privacy issues, data storage and how are organizational procedures and governance organized.

Article VI indicates that a lack of leadership and cooperation between the member countries prevents a coherent implementation process. National early warning solution HAVARO is not a government service, and it will be jointly provided by commercial operators and the National Cyber Security Center. Security Operations Centers (SOC) will process and report events to the stakeholders. Trusted Networks create a community where members can exchange information among themselves.

As article VI indicates, cross-border and transnational challenges also concentrate on regulation and agreement. The privacy activists have challenged The US Privacy-Shield Agreement by arguing that U.S. national security laws did not protect EU citizens from government snooping. Lack of standardization

prevents organizations from creating common rules for information sharing and data handling.

European level E-EWS will support a national information-sharing mechanism and system for public-safety personnel to coordinate and share information in near real-time. The big challenge is the diversity of stakeholders. Therefore, system requirements cannot place too many challenging barriers to the development of the E-EWS.

5.2 Answer to the main research question RQ

5.2.1 Information sharing in practice

High-level situational awareness requires a constant flow of information about what is happening around you. Especially workable emergency services require a continuous flow of information. The formation of an accurate situational picture requires ongoing information sharing and exchange. Regardless of the administrative level, information sharing arises as one of the crucial elements when a common situational picture is needed.

It matters what content, in what form, or when the information is shared or transmitted. Information may be sent in a different format than the receiver handles it. Therefore, it is recommended that the information must stay unchanged throughout the communication chain. From the micro-level to the macro-level, real-time video is the best way to share information from the physical accident site. When we have uncut material about the events, everyone can form an understanding of what has happened.

In a basic situation, information is shared human to human by using technological systems and tools as applications. A fully automated information-sharing system does not require humans at all. Every human is a unique person with a unique understanding and mental processing capabilities (Endsley, 1995; Endsley, Mica & Robertson, 1996). Understanding regarding signals what data, messages, or pictures include varies. That leads to the misunderstood situations where the message or data sender and achiever discuss differently with each other because they may understand shared information in their way. Human-based errors and obstacles are crucial factors that affect the whole public safety atmosphere. Sometimes essential messages have not been sent (McLaughlin, Haddad, & Hume, 2016) in addition to this, it is crucial how we share information with other collaborated actors. Is it possible to share everything with everyone and how to get the message to the recipient?

Technological-based obstacles consist of various problems regarding usability. Some solutions may be so strange that humans cannot use the interface, application, or system. Sometimes collaborating organizations use the same system platform, but their systems do not communicate with each other (Articles I, II and III). As mentioned above, two main factors that affect information sharing and working environment in operating public safety work are human-

based errors and technological (technical) errors or obstacles. Technical errors also consist of broken connections between the equipment, e.g., routers. Interface-related problems prevent the flow of information, but also communication interferences are essential factors at public safety fieldworkers work (Articles I, II and III).

5.2.2 The essential elements of the cyber ecosystem

The ecosystem is defined as "a community of living organisms in conjunction with the nonliving components of their environment."

> "The Cyber Ecosystem is global and includes government and private sector information infrastructure; the variety of interacting persons, processes, information, and communications technologies: and the conditions that influence their cybersecurity." (Department of Homeland Security, (DHS), 2011)

The research indicates that essential elements of the cyber ecosystem comprise requirements and factors as follows:

- Human Factors
- Organizational and Administrative Factors
- System & Technological Requirements
- Requirements of National Cyber-Physical Infrastructure
- Transnational (cross-border) set of Requirements
- National Cyber-Physical Infrastructure
- Regulation and Privacy Requirements

When the purpose is to efficient situational awareness by information sharing methods and processes, including cyber-threat information sharing, the crucial elements can be divided from the view of the public safety authorities. As articles I and II present, the real-time video data has to be possibly shared from the site of an accident to the emergency response centre. Field-workers user needs define systems requirements for the local and regional level. In addition to this, cyber-threat information must be available at the local level, regional level, and state level in the case of a major incident. This means that knowledge about cyber-threat information enhances emergency procedures and processes. Cyber domain, including Artificial Intelligence -based multiagent system allows that sensor technology to start preventing processes before any visible threat has occurred. The system has a multiway cyber dimension that efficient public safety authorities working processes and procedures at all decision-making stages. Occurred technical requirements indicate a need to integrate ERC and National Cyber Security Centre Finland emergency functions at the state level. Information exchange between intelligence and data protection authorities has also been taken into account because of the need to respond to privacy violations. In an ideal model, privacy protection would also be ensured automatically. The fewer human resources have been used in the data handling procedure, the more possibility for data leakage to third parties becomes difficult. It could increase citizens' confidence in the hybrid emergency system's activities.

The system will bring closer separate organizational and administrative actors of all stages but also will break boundaries between different ministries. That affects, e.g., National Cyber Security Centres working culture, including information sharing procedures.

When the crucial information is available without obstacles, it will also reduce public safety costs by reducing over-resourcing and the amount of personnel. Of course, if sharable data is classified, sensitive data has its own information-sharing practices, mechanism, and models. Also, Cross-border incidents require attention related to the issue of how to prevent hybrid threats and domino effects. The proposed Early Warning system will enhance the overall situational awareness of public safety services when all participants and stakeholders implement the proposed system with the information sharing framework that is introduced in article VIII. The elements of the trusted cyber ecosystem as article VII presents require more coherent standardization and regulation concerning the legislation of the public safety actors, privacy issues, technological issues, information sharing methods, at least for the European level, not forgetting fundamental threats that challenge our political decision-making. AI-based decision-making -handling may support critical infrastructure protection, such as FIGURE 20 indicates.

Digitized systems have to integrate into government systems more thoroughly in the future. Essential gathered data about the detected hybrid incident must be directly shared with the cybersecurity centers of the national stakeholders. Thus, it is relevant to allocate more detailed and reliable data for determining limits for discrepancies. Uniting pieces of information to ensure correct and reliable information sharing is of primary essence. The critical data should be processed to the desired shape for the participants. In an early warning solution, cyber defence operations will be more integrated and automated according to local capabilities, authorities, and mission needs. The transferable cyber-physical early warning ecosystem is an opportunity to take into account, for example, regional differences, including population, educational backgrounds, average earnings and technical maturity level of infrastructure, etc. (Article IX).

Cross-border hybrid threats set requirements for how to share data (Articles VI, VII, VIII, and IX). The proposed sharing model requires using national EWS servers where European ECHO-EWS is connected. In an ideal model, there should be a European head organization that should be a responsible organization for the information sharing of the early warning data at the European level. The proposed hybrid model is a safe part of the architecture, allowing sharing of confidential, sensitive information. It is essential that, for example, the National Bureau of Investigation can gather and share trust-level information concerning detected threats in vital functions of society and have the ability to be connected to the Early Warning System. It is relevant that the early warning data is shared from the central server with the other players of the affected sectors. Multinational corporations receive threat information in advance (Articles VI, VIII). It is recommended to utilize a controlled information-

sharing model, where national public safety actors share sensitive and relevant data to sectorial stakeholders via a centralized center (Article VIII).

At present National Computer Security Centre (NCSC) of Finland has a parallel subsystem, "Govhavaro" for public organizations. It consists of differential early warning services for all public organizations. There is a need to establish sector-specific communities instead of separate participants share information freely. For example, ISAC and ISAO collect and share crucial information concerning the targeted sector of the critical infrastructure, as PVIII proposes. Cybersecurity information is monitored and handled by SOCs, CERTs or CSIRTs, and official national cybersecurity centers (EWS hub) will share all new threat indicators between sectorial stakeholders (ISACs or ISAOs). All law enforcement-related transnational information will be shared directly via the EWS hub to the public safety authorities, such as EUROPOL or INTERPOL.

Aiming to achieve the common operational picture requires that real-time information be available and information sharing connections from the local level collaborators to the national and EU level collaborators exist. Workable Cyber-physical system and emergency and crisis management maintain common cyber situational awareness. Cyber situational awareness functions and traditional emergency response service management should form a working early warning combination. The proposed Next-Generation Hybrid Emergency model combines identified requirements and uses artificial tools to generate information for decision-makers. Artificial Intelligence-based decision-support and decision-making mechanisms make the system effective. Decision-makers may utilize the produced data when the system works automatically. All presented layers are combined in the hybrid design below, and the proposed model is obtained at the transnational level when a cyber information-sharing structure in FIGURE 18 is connected to this simplified model as FIGURE 23 presents.

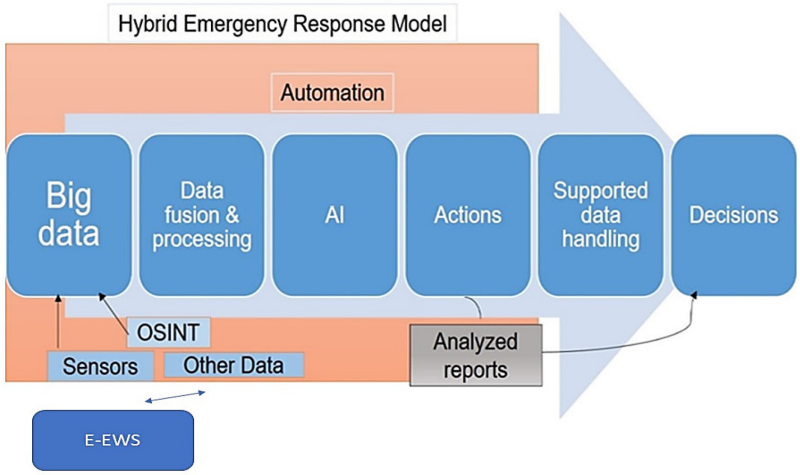


FIGURE 23 Two-way Decision Support Mechanism connected to the European EWS

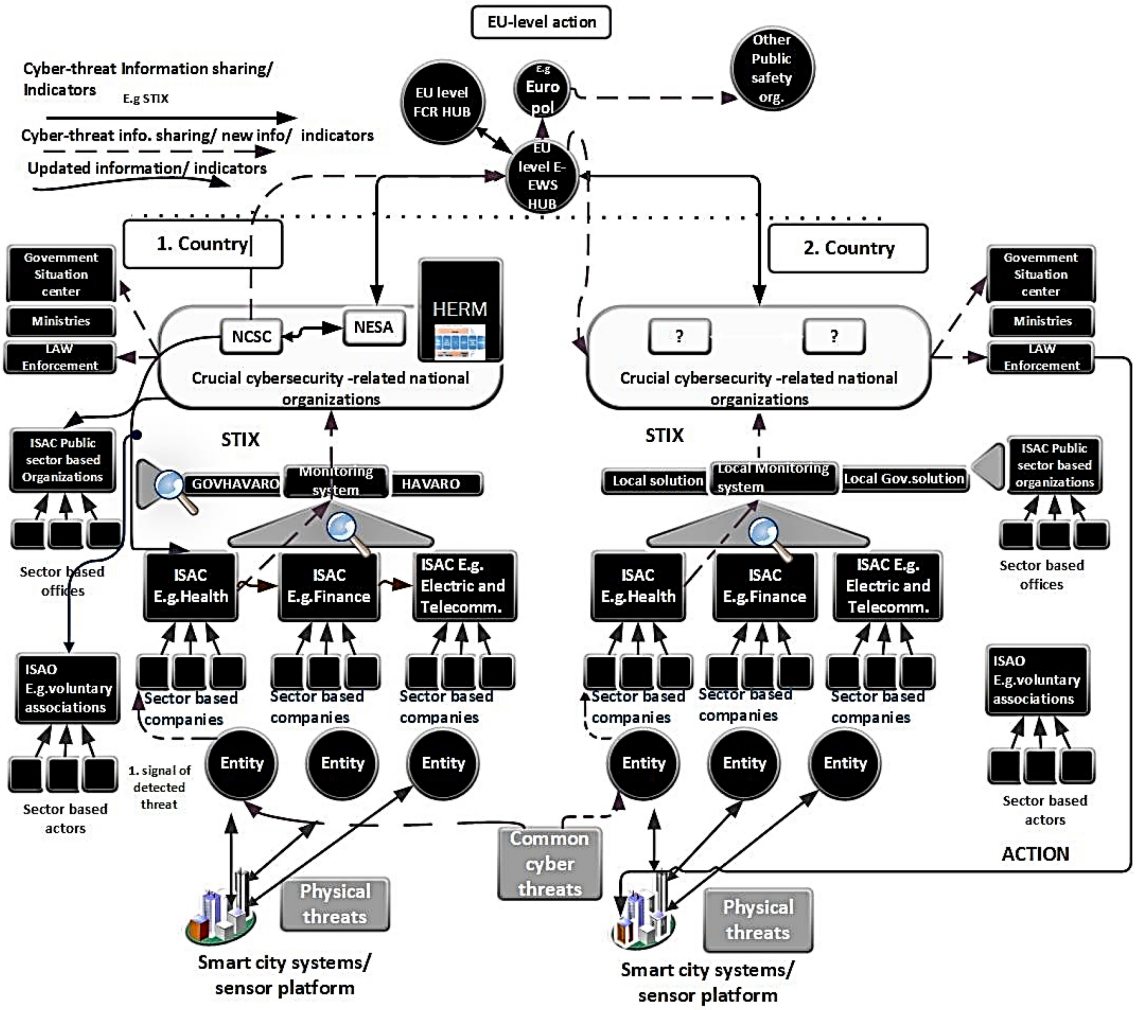


FIGURE 24 Enhanced Hybrid Situational Awareness by using HERM

FIGURE 24 illustrates that traditional information-sharing processes of the authorities' have to transform to automated or semi-automated functionalities. It is essential in the western tradition that automation or robotics do not ignore human abilities and democratic decision-making in institutions. Presently, the legislation supports politicians' desire to maintain high levels of control over their decision-making ability despite recent minor changes in legislation concerning intelligence legislation. The lack of motivation for changes may prevent the implementation of the proposed Smart Hybrid Emergency Model. It would be time to change opinions about artificial intelligence-based decisions or AI-aides automated functions in urban infrastructure. In this context, continuity management consists of the maturity of early warning technology, cyber preparedness, operational preparedness, and controlled, reliable decision-making, which belongs to the concept of "information sharing and exchange". Without information sharing, comprehensive shared situational awareness is not achieved. Supported decision functions of strategic, operational and tactical level management can be processed into a single entity without combining all elements in one physical location. Early Warning information from other

countries is easy to combine with national threat information when information-sharing procedures and mechanisms follow the same guidelines. Fundamental risk factors have to be detected before they cause domino effects thus, technical early warning solutions become useful. One crucial requirement is that a decision support mechanism is developed jointly with the crisis management system.

When the purpose is to design a common cyber ecosystem for the stakeholders, system integrity requirements mean that it is impossible to design a joint early warning system as an isolated system from information system-related standards and the information-sharing procedures, guidelines, and methods. Coherent system development needs coherent developing elements. Without common understanding of the wanted direction concerning hybrid threats prevention, it would be challenging to create "early warning umbrella" for all collaborators that are involved. Flexible Interoperability should be coordinated through standards so that Shared Situational Awareness is achievable between cross-border participants, as simplified FIGURE 23 demonstrate. European EWS should be a seamless part of the national EWS. The fundamental architecture of the early warning system needs a base that consists of joint legislation bases, guidelines, protocols, and standards. European EWS-solution has to base legislation that considers specifications of joining collaborators of countries (e.g., responsibilities of ministries). The system's operations and system-based operational work must be based on legislation, regulations, and standards. In semantic interoperability, an information system can gather information widely and process it to preserve the original meaning and contents of the information. The semantic requirement is crucial in public safety services, where a situational picture must form immediately when something abnormal happens, but semantic interoperability requires that also humans understand the content of the information and actions of the automated functions. Privacy issues affect the implementation of intelligent systems. However, the intention to protect citizens, for example, in the USA, is steering the western world atmosphere, and it is to be expected that tendency will continue to the European level. Closer cooperation on information sharing and exchange can be achieved when both transatlantic and European level legislation, bilateral agreements, data management standards, and certifications are implemented at an acceptable level of privacy.

5.2.3 The hybrid emergency response model as part of the future society

As we have seen, it is a complicated situation that public organizations and departments offer services to the private sector when the purpose is to protect vital functions. Private sector enterprises and organizations that operate within critical infrastructure use several systems that do not fulfill the information security requirements that public safety authorities require. Valtori in Finland tries to solve information technology-related problems that arise from states' information systems.

Therefore, it is not easy to combine old-fashioned mechanisms with the next-generation systems that work by using neural network solutions. If we think

about the national level of the urban areas and rural areas, we can see clearly that technological infrastructure in a rural area is not so developed as it has to be. The problematic issues concerning the undeveloped rural areas are unresolved. Lack of funding is often the reason why only urban areas develop. The same problem affects the maritime area.

Designing next-generation emergency response systems requires a coherent understanding of the political will. The highest decision-makers have to understand how fast technology develops. This also means that criminals and threat developers use more sophisticated software and tools. Due to that, it is essential to enhance cooperation between the European Union member countries. Countries that have a common culture and understanding of the security environment have to design transnational standardized systems together. It is also important to develop trusted relationships with other western countries. Polarization of the political world has been shown that stability and constancy are not essential topics nowadays. Separated western and eastern worldviews create more risks and threats than a peaceful base to construct innovative solutions for information sharing between east and west.

In cross-border threat situations, it is an essential issue with whom to share sensitive information. The importance of classifying information-sharing partners and sources arises an essential role. For example, the type of natural disaster belongs to the class that information has to share abroad from east to west and from west to east. Citizens have the right to get the correct information about the happened disaster.

In the near future, intelligent cities will be constructed in an environment where artificial intelligence-aided systems and software communicate with the traditional structures of society. Especially developed countries enhance their capability to use intelligent solutions in the smart infrastructure. The importance of used technologies for information sharing is a relevant issue when the purpose is to protect critical infrastructure and continuity management of the society.

However, the research indicates that western states have taken steps towards the digitized future. Standardized information sharing procedures mechanisms and models are crucial parts of the next-generation information sharing architecture, such as the Early Warning System titled Hybrid Emergency Response Model will be. The designing process requires that all stakeholders develop and upgrade their hybrid-threat mechanisms applying the same infrastructure in order that situational awareness reaches a consistent level. The Design Science Research requires that the proposed artifact produce added value and it solves the main research problem. It has been shown that The Hybrid Emergency Response model fulfills the requirements for enhancing Hybrid Situational Awareness among PPDR services when all presented issues are taken into account during the design process. All points of Hevner´s guidelines in TABLE 1 are fulfilled.

5.3 Reliability and validity

The doctoral dissertation generates new data for the decision-makers by creating a new model that is based on a wide range of research activities. Does the research examine the issues that it should? Mixed methods also mean quantitative measurements. Qualitative and Quantitative approaches complement each other. Several cases consist of quantitative and qualitative analysis. The purpose of the investigation is fulfilled. The research answers correspond to the research questions. Several articles were excluded because they did not provide any new relevant information on the research questions. The research approach and the methods used correspond well to the phenomenon to be examined. A combined Case study strategy with Design Science Research consists of crucial elements for developing the proposed new model. DSR requires a deeper understanding of the "formation of situational awareness in PPDR services." Therefore, the author must gather data from the actual PPDR-workers daily routine. There were no similar situation center-related studies that I have done. The selected research strategy that has been used is constructively valid. Logically we can find milestones that start from the micro-level situational awareness and ends the macro-level cyber SA. In the context of Situational awareness, Information Sharing is an essential element. Selected articles are peer-reviewed and published in classified publication forums.

External validity reflects how generalizable the study is. The research scope is possible to repeat in another region. The especially empirical part of the research consists of crucial stakeholders among regional PPDR authorities. Similar local and regional departments are located by territorial regions. The operational practices in their day-to-day work are generally similar.

5.4 Limitation and future research

The research has reached its saturation, but there is a couple of things that have to take into account. The research questions have received their answers seamlessly, but limitations arise from the view of how many PPDR-organizations have been included in the empirical review. Four situation centers from the west coast were selected for the doctoral dissertation. The other four could have been selected from a different region. Despite that, sufficient coverage has been achieved due to the extensive use of literature and official publication. People have also been interviewed very extensively.

Future research could include a technical section of features that creates a more accurate model of the proposed issues. Research can be expanded to include a broader range of organizations; for example, defence forces is out from closer review. It is crucial to notice that this designed model is only a proposed model, not ready to use solution. Therefore, technical choices, for example, selected routers, are examples of valued equipment. It is essential to understand

the ecosystem of the proposed model and what are those essential elements and factors are connected and affect it

YHTEENVETO (SUMMARY IN FINNISH)

Maailmanlaajuinen Koronavirus pandemia on osoittanut varhaisvaroitusjärjestelmän tarpeellisuuden niin kansallisesti kuin globaalistikin. Voidaanko varoitus- ja hälytystoimintoja yhdistää ja millä tavalla? Miten päätöksentekijät voisivat saada olennaisen tiedon päätöksenteon tueksi kriisin hetkellä ja ennen kriisiä tarkemman tilannekuvan muodossa? Tämän väitöskirjan tarkoitus on osoittaa olennaisimmat tekijät ja vaikuttimet sekä kehitystarpeet liittyen julkisten turvallisuusorganisaatioiden toimintaan liittyen tilannetietoisuuden ja tilannekuvan ylläpitoon, erityisesti hälytystoiminnoissa ja osoittaa näille haasteille ehdotelma seuraavan sukupolven hälytysmallista. Tällä hetkellä kyberturvallisuusulottuvuutta ei hyödynnetä kriittisen infrastruktuurin suojelussa juuri lainkaan ja eri turvallisuusorganisaatioiden synerginen toiminta on puutteellista. Esitelty varhaisvaroitusjärjestelmä ottaa huomioon menetelmät ja keinot, joilla kyberfyysinen järjestelmä voitaisiin mahdollistaa siten, että reagoivasta hätäkeskusjärjestelmästä tulisi pikemminkin ennakoiva ja estävä kuin reagoiva.

Seuraavan sukupolven Hybrid Emergency Response Model auttaa päätöksentekijöitä yhteisen tilannekuvan muodostamisessa tavalla, joka tehostaa ja parantaa yhteiskunnan elintärkeiden toimintojen suojauksen ennakoivaa reagointikykyä myös sellaisten uhkien osalta, jotka ovat vasta muodostumassa. Kyberturvallisuus ei ole enää erillinen saareke perinteisten uhkien takana, vaan yhdistelmäuhat eli hybridiuhat tarvitsevat entistä tehokkaampaa hybridivastetta. Dominoefekti pitää kyetä estämään riittävän tehokkaalla hybridiuhkien ennaltaehkäisyllä. Tässä ratkaisussa älyteknologialla on oma erityinen roolinsa.

REFERENCES

Alberts, D. S., & Hayes, R. E. (2006). Understanding Command and Control. DoD command and control research program. Center for Advanced Concepts and Technology (ACT).

Ashish, N., Kalashnikov, D. V., Mehrotra, S., Venkatasubramanian, N., Eguchi, R., Hegde, R., & Smyth, P. (2007). Situational awareness technologies for disaster response. In H. Chen, E. Reid, J. Sinai, A. Silke & B. Ganoz (Eds.), Terrorism informatics: Knowledge management and data mining for homeland security. Springer.

ATLS (Ed.). (2008). Advanced trauma life support for doctors (student course manual) (8th ed.). USA: American College of Surgeons.

Baldini, G. (2010). Report of the workshop on "Interoperable communications for Safety and Security" with recommendations for security research. (No. JRC60381). Publications Office of the European Union. doi:10.2788/19075.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. MIS Quarterly, 11(3), 369-386.

Colson, E. (2019). What AI-driven decision-making looks like. Retrieved from https://hbr.org/2019/07/what-ai-driven-decision-making-looks-like

Court of Justice of the European Union. (2020). The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield

CBRNE strategy working group. (2017). National CBRNE strategy 2017. (No. 32). Ministry of the Interior.

Dandurand, L., & Serrano, S. O. (2013). Towards improved cyber security information sharing. Paper presented at the 5th International Conference on Cyber Conflict.

Department of Homeland Security. (2011). Blueprint for a secure cyber future - the cybersecurity strategy for the homeland security enterprise. DHS.

Department of Homeland Security. (2013). NIPP 2013 - partnering for critical infrastructure security and resilience. U.S.: DHS.

Department of Homeland Security. (2015), Automated Indicator Sharing (AIS) FAQ, Retrieved from https://www.uscert.gov/sites/default/files/ais_files/AIS_FAQ.pdf

Department of Homeland Security. (2019). Automated indicator sharing (AIS). Retrieved from https://www.us-cert.gov/ais

DG Home Affairs. (2014). UINFC2 project. Deliverable D.1.3: Law enforcement agents' requirements. European Union.

Dos Passos, D., S. (2016). Big data, data science, and their contributions to the development of the use of open-source intelligence.11(4)

Edgington, T. (2020). Brexit: All you need to know about the UK leaving the EU, BBC News, viewed 20 September 2020, <https://www.bbc.com/news/uk-politics-32810887>.

Electrical Technology. (2016). Internet of things (IOT) and its applications in the electrical power industry. Retrieved from

http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html
Endsley, M. (1988). Design and evaluation for situation awareness enhancement. Paper presented at the Proceedings of the Human Factors Society 32nd Annual Meeting, 97-101.
Endsley, M. R. (1995). Toward a theory of situation awareness. Human factors. (37), 32-64.
Endsley, M. R. (2015). Autonomous horizons, system autonomy in the air force – A path to the future. (No. 1).Air Force Office of the Chief Scientist.
Endsley, M. (1988). Design and evaluation for situation awareness enhancement. Paper presented at the Proceedings of the Human Factors Society 32nd Annual Meeting, 97-101.
Endsley, M., & Robertson, M. (1996). Team situation awareness in aviation maintenance. Paper presented at the Human Factors and Ergonomics Society Annual Meeting. doi:40. 10.1177/154193129604002107
European Commission. (2020a). Joint Communication to the European Parliament and the council - The EU´s cybersecurity strategy for the digital decade. Brussels: European Commission.
European Commission. (2020b). On artificial intelligence - A European approach to excellence and trust. Brussels: European Commission.
EUROPOL. (2019). Secure information exchange network application (SI-ENA). Retrieved from https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-sien
Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. Computers & Security, 46, 18-31.
Garfinkel, S. (2012). Digital forensics XML and the DFXML toolset. Digital Investigation, 8, 161-174.
General Secretariat of the Council. (2014). European Union maritime security strategy. Brussels: European Commission.
Glassman, M., & Kang, M., Ju. (2012). Computers in human behavior; intelligence in the internet age: The emergence and evolution of open-source intelligence (OSINT).28(2), 673-682.
He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. Risk Analysis, 38(2), 215-225. doi:https://doi.org/10.1111/risa.12878
Hernandez-Ardieta, J. L., Tapiador, J. E., & Suarez-Tangil, G. (2013). Information sharing models for cooperative cyber defence. Paper presented at the The 5th IEEE International Conference on Cyber Conflict (CyCon), Tallinn, Estonia. 1-28.
Hevner, A. (2007). A three-cycle view of design science research. Scandinavian Journal of Information Systems, 19(2) Retrieved from https://aisel.aisnet.org/sjis/vol19/iss2/4

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In R. Sharda, & S. Voss (Eds.), Design research in information systems: Theory and practice. Springer Science and Business.
Hughes, J., Randall, D., & Shapiro, D. (1993). From ethnographic record to system design. Some experiences from the field. Paper presented at the Computer Supported Cooperative Work (CSCW), 123-141.
Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and NATO global cybersecurity challenges: A way forward. Washington: PRISM, NDU.
International Organization for Standardization (ISO). (2012). ISO 27032:2012 information technology — security techniques — guidelines for cybersecurity.
International Organization for Standardization (ISO). (2013). ISO/IEC 27002:2013 Security techniques — code of practice for information security controls. Retrieved from https://www.iso.org/standard/54533.html
International Organization for Standardization (ISO). (2015). ISO 9001:2015 quality management systems - requirements. Retrieved from https://www.iso.org/standard/62085.html
International Organization for Standardization (ISO). (2016). ISO 27799:2016 health informatics — information security management in health using ISO/IEC 27002. Retrieved from https://www.iso.org/standard/62777.html
International Organization for Standardization (ISO). (2017). ISO/IEC 29134:2017 guidelines for privacy impact assessment. Retrieved from https://www.iso.org/standard/62289.html
IsecT. (2018). ISO/IEC 27005:2018 information technology — security techniques — information security risk management (third edition). https://www.iso27001security.com/html/27005.html. Updated 2018.
Kananen, J. (2013). Case-tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulun julkaisuja.
Kaukanen, J., & Möttönen, M. (2010). Border guard headquarters - MARITIME SEARCH AND RESCUE MANUAL 2010. Ministry of the Interior.
Kela. (2020). Tekniset liittymismallit kanta-rekisteriin-tecnical instruction. Helsinki: Kela.
Lee, E., Ashford, & Seshia, S., Arunkumar. (2015). Introduction to embedded systems, a cyber-physical systems approach (2nd ed.) Lee&Seshia.
Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). 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.
Lerner, E. B., & Moscati, R. M. (2001). The golden hour: Scientific fact or medical ?urban legend?? Academic Emergency Medicine, 8(7), 758-760. doi:10.1111/j.1553-2712.2001.tb00201.x

McLaughlin, E., Haddad, M., & Hume, T. (2016). Brussels attacks: Order to close metro sent to wrong address - CNN.com.
Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Thousand Oaks: Sage Publications.
Ministry of Defence. (2010). Security strategy for society, government resolution. Helsinki: Ministry of Defence.
Ministry of Interior. (2010). The Finnish Emergency Response Centre Operations act. 2010. (692/2010)
MITRE. (2018). Trusted automated eXchange of indicator information — TAXII™ enabling cyber threat information exchange
Morrow, J., & Odierno, R. (2012). Open-source intelligence, ATP 2-22.9, army techniques publication. Washington: Headquarters, Department of the U.S. Army.
NENA. (2018). NENA/APCO next-generation 9-1-1 public safety answering point requirements. USA: NENA and APCO. Retrieved from https://www.nena.org/resource/resmgr/standards/nena-req-001.1.2-2018_ng-psa.pdf
NIST. (2014a). Guidelines for smart grid cybersecurity - volume 3 - supportive analyses and references. U. S. Department of Commerce.
NIST. (2014b). Guidelines for smart grid cybersecurity national institute of standards and technology, volume 1 - smart grid cybersecurity strategy, architecture, and high-level requirements. The U.S. Department of Commerce. doi:10.6028/NIST.IR.7628r1 Retrieved from DOI Retrieved from http://dx.doi.org/10.6028/nist.ir.7628r1
NIST. (2016). Guide to cyber threat information sharing. No. NIST Special Publication 800-150). Gaithersburg: National Institute of Standards and Technology.
National Supervisory Authority for Welfare and Health. (2020). Organizational structure. Retrieved from https://www.valvira.fi/web/en/valvira/organisational structure
Nunamaker, J., Minder Chen, J. R., & Purdin, T. (1991). Systems development in information systems research. Journal of Management Information Systems (3), 89-106.
Nurmi, P. (2015). OSINT - avointen lähteiden internet-tiedustelu. Helsinki: Aalto yliopisto.
Ojala, L., Solakivi, T., Kiiski, T., Laari, S., & Österlund Bo. (2018). Merenkulun huoltovarmuus ja suomen elinkeinoelämä - toimintaympäristön tarkastelu vuoteen 2020. .Huoltovarmuusorganisaatio.
Ojasalo, K., Moilanen, T., & Ritalahti, J. (2009). Kehittämistyön menetelmät. uudenlaista osaamista liiketoimintaan. Porvoo: WSOYpro.
Patton, M. (2002). Qualitative evaluation and research methods (3rd ed.). London: Sage Publications.
Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., Takahashi, T., . . . Adegbite, S. (2010). CYBEX - the cybersecurity information

exchange framework (X. 1500). Computer Communication 40, 59-64. doi:10.1145/1880153.1880163.
Sadique, F., Bakhshaliyev, K., Springer, J., & Sengupta, S. (2019). A system architecture of cybersecurity information exchange with privacy (CYBEX-P) doi:10.1109/CCWC.2019.8666600
Safety Investigation Authority. (2017). Turku stabbings on 18 august 2017/ puukotukset turussa 18.8.2017. Helsinki: SIA.
Secretariat of the Security Committee. (2013). Finland´s cyber security strategy - government resolution. Ministry of Defense.
Sedenberg, E. M., & Dempsey, J. X. (2018). Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs
Simola, J. (2020). Chapter 10 - privacy issues and critical infrastructure protection. In V. Benson, & J. Mcalaney (Eds.), Emerging cyber threats and cognitive vulnerabilities (pp. 197-226) Academic Press. doi: https://doi-org.ezproxy.jyu.fi/10.1016/B978-0-12-816203-3.00010-1
Simola, J., & Rajamäki, J. (2018). Improving cyber situational awareness in maritime surveillance. Paper presented at the 17th European Conference on Cyber Warfare and Security ECCWS 2018, Oslo, Norway. 480-488.
Simola, J. (2015). The effects and factors of the real-time video in PPDR services (master's thesis). Laurea University of Applied Sciences

Simola, J., Jokinen, E., & Rajamäki, J. (2015). How situational awareness can be improved by using real-time video? case: Simulated natural disaster at the viksu 2014 camp.
Simola, J., Lehto, M., & Rajamäki, J. (2021). Emergency response model as a part of the smart society. Paper presented at the European Conference on Cyber Warfare and Security (ECCWS2021).
Simola, J., & Rajamäki, J. (2014). Using a real-time video to allocate public protection and disaster relief resources in the rescue service process - natural disaster in young voluntary firefighter´s camp. Paper presented at the 5th European Conference of COMPUTER SCIENCE (ECCS '14), Geneva, Switzerland. 56-62.
Simola, J., & Rajamäki, J. (2016). Common cyber situational awareness: An important part of modern public protection and disaster relief. Paper presented at the 10th International Conference on Computer Engineering and Applications (CEA '16), Barcelona, Spain. 54.
Simola, J., & Rajamäki, J. (2017). Hybrid emergency response model: Improving cyber situational awareness. Paper presented at the 16th European Conference on Cyber Warfare and Security, University, College, Dublin, Ireland. 442-451.
Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. computers and security., 154-176.

Smeets, M. (2019). NATO allies need to come to terms with offensive cyber operations. Retrieved from https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations

Tidey, A, Gill, J & Parrock, J. (2020). EU warns Turkey of quick sanctions if dialogue over Eastern Mediterranean drilling fails. EURONEWS. viewed 20 September 2020, https://www.euronews.com/2020/10/02/eu-leaders-break-deadlock-over-belarus-sanctions

The Finnish Border Guard. (2018). Finnish Border Guard maritime SAR suitable equipment. Retrieved from http://www.raja.fi/sar/en/equipment

The Criminal Intelligence Coordinating Council. (2013). National criminal intelligence sharing plan. Building a national capability for effective criminal intelligence development and the nationwide sharing of intelligence and information. (No.2). USA: CICC.

The Security Committee. (2018). Security strategy for society. Helsinki: The Security Committee.

The White House. (2013). Critical infrastructure security and resilience, presidential policy directive. Washington: The White House.

Trottier, D. (2015). Open-source intelligence, social media and law enforcement: Visions, constraints and critiques. 18(4-5), 530-547.

Vakilinia, I, Tosh D & Sengupta S (2017). Privacy-preserving cybersecurity information exchange mechanism. In Proceedings of the 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS). pp. 1-7.

Wooldridge, M. (2009). An introduction to multiagent system (2nd ed.). United States: John Wiley & Sons.

Yin, R. K. (2014). Case Study Research Design and Methods (Fifth ed.). Los Angeles: SAGE Publications.

ORIGINAL PAPERS

I

HYBRID EMERGENCY RESPONSE MODEL: IMPROVING CYBER SITUATIONAL AWARENESS

by

Jussi Simola & Jyri Rajamäki, 2017

Conference proceeding of the 16th European Conference on Cyber Warfare and Security ECCWS, Dublin, Ireland. p,.442-451

https://urn.fi/URN:ISBN:978-1-911218-44-9

Hybrid Emergency Response Model: Improving Cyber Situational Awareness

Jussi Simola and Jyri Rajamäki
Laurea University of Applied Sciences, Research, Design and Innovations, Finland
simolajussi@gmail.com
jyrirajamaki@laurea.fi

Abstract: Cyber threats have increased in spite of formal integration in Europe and the world. Therefore, authorities need to respond to growing challenges. As major terror attacks, hybrid warfare and major accidents e.g. in USA, Belgium, Ukraine and France have shown preparation for different kind of threats is challenging. Finnish Public Protection and Disaster Relief (PPDR) authorities and politicians have recognized the importance of a common situational awareness in preparation for the future. Cyber situational awareness is a part of situational awareness which concerns the "cyber" environment. Such situational awareness can be reached, e.g., by using data from IT sensors that can be fed to a data fusion process or be interpreted directly by the decision-maker. This study was conducted on the ground by visiting in four situation and command centers of PPDR services located in Southwestern Finland. The main purpose of the study was to create smart hybrid emergency response -model based on intelligent emergency management system and find out local and state level factors which affect to utilization of system. The aim was also to research the level of preparedness in regional administration including local PPDR departments. The main results can be summarized so that unclear allocation of responsibilities in government departments prevent authorities from fighting together against cyber and physical threats. Responsibilities for developing cybersecurity has also been shared for too many factors. The operational field work of the PPDR authorities should be more standardized and management should be more centralized. Unclear emergency procedures between authorities and lack of co-operation between situation centers with limited data transmission capacity prevent to create common situational awareness. In the future, a common cyber situational awareness is needed for both operating cyber physical system and for emergency and crisis management. PPDR services and decision makers In Finland need a common multifunctional hybrid emergency response-model to be able to prevent various threats until bureaucratic and organizational barriers have been removed. Need for common cyber ecosystem to control crossboarding threats is growing.

Keywords: cyber security, hybrid emergency response, PPDR, situational awareness, early warnings

1. Introduction

European Public Protection and Disaster Relief (PPDR) services such as law enforcement, firefighting, emergency medical and disaster recovery services have recognized that the lack of interoperability of technical systems limit the cooperation between the PPDR authorities. *Also The military (MIL) and critical infrastructure protection (CIP) faces similar challenges.*

As major terror attacks, hybrid warfare and major accidents e.g. in USA, Belgium, Ukraine and France have shown preparation for different kind of threats is challenging. Recent major accidents have indicated that lack of human resources affects to disaster recovery.

The main purpose of the study was to create smart hybrid emergency response -model based on intelligent emergency management system and find out local and state level factors which affect to utilization of system. The aim was also to research the level of preparedness in regional administration including local PPDR departments.

Another topic is to find out different agencies' level of preparedness of applying new technologies, especially in the cyber domain.

2. Theoretical framework

2.1 Situational awareness

According to Endsley (Endsley 1988), a general definition of situational awareness is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future". From a technical viewpoint, situational awareness comes down to compiling, processing and fusing data, and such data processing includes the need to be able to assess data fragments as well as fused information and provide a rational estimate of its information quality (Franke,

Brynielsson 2014). The cognitive side of situational awareness concerns the human capacity of being able to comprehend the technical implications and draw conclusions in order to come up with informed decisions (Franke, Brynielsson 2014). Referred to Endsley (1988, 2015), humans are not as good at processing large volumes of data, quickly and consistently, nor of sustaining attention for long periods of time. Figure 1 illustrates the level of autonomy increases as the capability of the system increases for performing various components of any given functions. Flexible autonomy should provide smooth, simple, seamless transition of functions between human and the system (Endsley 2015).

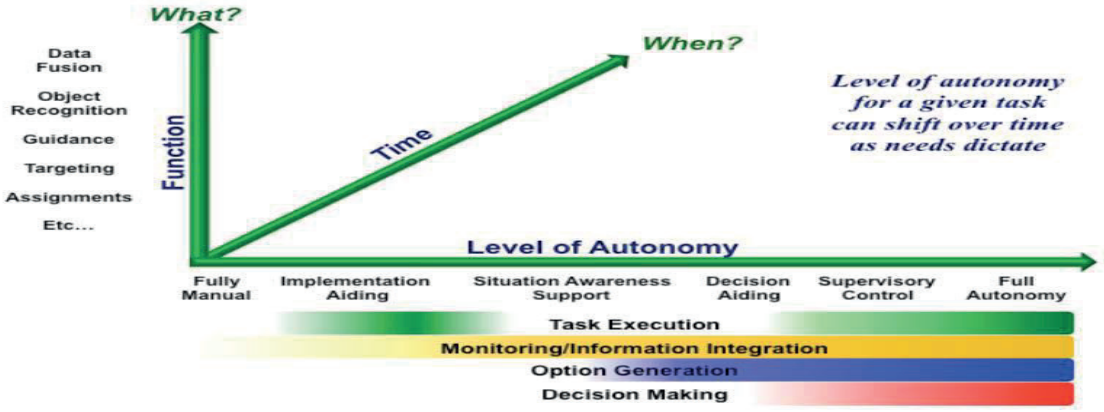


Figure 1: Level of autonomy

2.1.1 Cyber situational awareness

According to Franke and Brynielsson (Franke, Brynielsson 2014), cyber situational awareness is a subset of situational awareness, i.e., cyber situational awareness is the part of situational awareness which concerns the "cyber" environment. Such situational awareness can be reached, for example, by the use of data from IT sensors (intrusion detection systems, etc.) that can be fed to a data fusion process or be interpreted directly by the decision-maker (Franke, Brynielsson 2014).

2.2 Structural and organizational changes in Finnish PPDR

The term public protection and disaster relief (PPDR) or Public Safety organizations are responsible for the prevention of and protection from events that could endanger the safety of the general public (Baldini 2010). According to Baldini (Baldini 2010), The main public safety functions include law enforcement, emergency medical services, border security, protection of the environment, firefighting, search and rescue (SAR) and crisis management.

The structural changes within public sector, such as the regional administration reform, the Emergency Response Centre (ERC) reform and so called social welfare and health care reform have influenced public sector employee´s work processes over the past ten years. In addition, technological development has occurred rapidly (Hanni 2013). Changes in PPDR organization´s due to legislation have developed a need to create special operational working methods (Aine et al. 2011). The Finnish Security Intelligence Service (Supo) is an operational security authority engaged in close cooperation with international security and intelligence services. Supo moved directly under the Ministry of the Interior in 2016. Earlier the Finnish Secure Intelligence Service operated under the National Police Board (The Finnish Security Intelligence Service 2015).

2.3 Command and control system

A Command Center is any place that is used to provide centralized command for some purpose. An Incident Command Center would be located at or near an incident to provide localized on-scene command and support of the Incident Commander. Mobile Command Centers may be used to enhance emergency preparedness and back up fixed command centers. Command Centers may include Emergency Operations Centers (EOC) or Transportation Management Centers (TMC) as well.

Supervisory Control and Data Acquisition (SCADA) systems are basically Process Control Systems (PCS) that are used for monitoring, gathering, and analyzing real-time environmental data from a simple office building or a

complex nuclear power plant. PCSs are designed to automate electronic systems based on a predetermined set of conditions, such as traffic control or power grid management (Gervasi 2010).

2.3.1 Distributed systems intercommunication protocol—DSiP

DSiP forms multiple simultaneous communication channels between the remote end and the control room: if one communication channel is down, other channels will continue operating. DSiP makes communication reliable and unbreakable by using various physical communication methods in parallel. Applications, equipment and devices can communicate over a single unbreakable data channel. Satellite, TETRA, 2G/3G/4G, VHF-radios and other technologies can be used simultaneously. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication (Ahokas et al. 2010).

2.4 Critical infrastructure protection

Critical Information Infrastructure means any physical or virtual information system that controls, process, transmits, receives or stores electronic information in any form including data, voice or video that is vital to the functioning of critical infrastructure. Critical infrastructure (CI) includes energy production, transmission and distribution networks, ICT systems, networks and services (including mass communication), financial services, transport and logistics, water supply, construction and maintenance of infrastructure, waste management in special circumstances. That smart network will integrate information and communication technologies with the power-delivery infrastructure (Ministry of the Interior 2016, Ahokas et al. 2010).

2.5 Emergency communications

European authorities communicate with each other in Virve -network. There is a need to create new trusted network with wide bandwidth. The transmission capacity is often limited in an overload situation.

Enhancing common operational picture has been noticed also in The United States. Need to transmit live video but also different kind of sensor data from scene of the accident has become main areas for development of information systems. The 9-1-1 Center of the future with FirstNet systems will receive incoming Data calls from the machines and sensor systems including automatic crash notification (ACN), break-in alarms, and body health monitors. Use of both systems ensures multi-media capabilities throughout the entire call process (National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) 2016, National Public Safety Telecommunications Council 2015).

2.6 A smart grid system and internet of thinks

Internet of Things connects systems, sensors and actuator instruments to the broader internet. IOT allows the things to communicate, exchange control data and other necessary information while executing applications towards machine goal (Electrical Technology 2016).

Cybersecurity risks should be addressed as organizations implement and maintain their smart grid systems (National Institute of Standards and Technology 2014). A smart grid system may consist of information technology which is a discrete system of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. A smart grid system may also consist of operational technologies (OT) or industrial control systems (ICS) like SCADA systems, distributed control systems (DCS), and other control system configurations (National Institute of Standards and Technology 2014, CHONG, KUMAR 2003).

Industrial Internet of Things (IIOT) collects data from connected devices (i.e., smart connected devices and machines) in the field or plant and then processes this data using sophisticated software and networking tools. The entire IIOT requires a collection of hardware, software, communications and networking technologies (Electrical Technology 2016).

2.6.1 Integration of safety functions

Decision Support Engine (DSE) is a facilitator intended to help authorities and other decision makers that compiles key information from raw data using system rules and knowledge. It captures data from different

sensors e.g. surveillance cameras (Ahmed et al. 2012). Face detection camera (FDC) is also one kind of decision support engine itself. Data processing for event detection follows next in order to identify events in current surveillance context (NEC Corporation). To understand the current surveillance state depends on the output of combined event detection units.

2.7 Situational awareness at national level

The Ministry of Finance of Finland is responsible for the steering and development of the state's information security (Ministry of defence 2010). Government situation centre ensure that the state leaders and central government authorities are kept informed continuously as illustrated in Figure 2. In Finland, the Government situation centre was set up in 2007, and it has the duty to alert the government, permanent secretaries and heads of preparedness and to call them to councils, meetings and negotiations at exceptional times required by a disruption or a crisis.

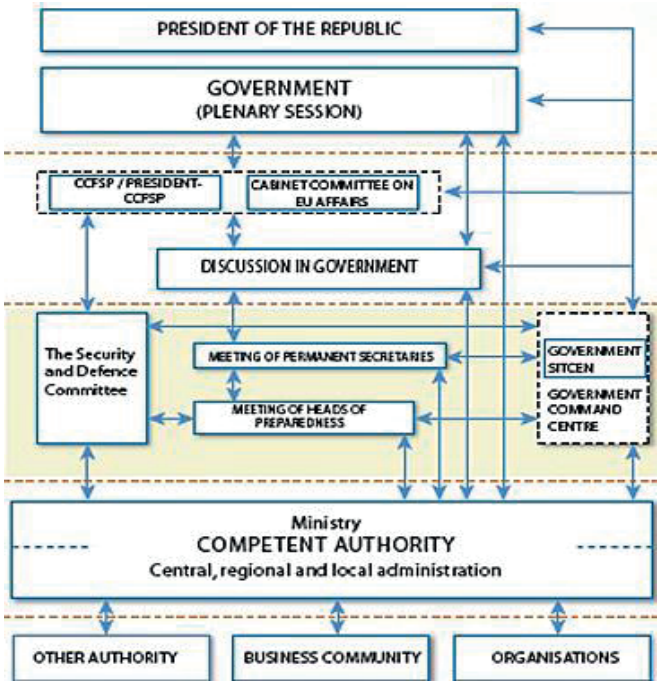


Figure 2: Management of disturbances in Finland

2.8 Cyber situational awareness at national level

Ministry of Transport and Communications is responsible for safeguarding the functioning of electronic ICT systems. The Ministry of Finance is responsible for safeguarding the state administration's IT functions, information security, and the service systems common to the central government (Secretariat of the Security Committee 2013). The Security Committee coordinates cyber security preparedness, monitors the implementation of the Cyber Security Strategy and issues recommendations on its further development. (Secretariat of the Security Committee 2013). The Finnish Communications Regulatory Authority (FICORA) working under steering control the Ministry of Transport and Communications. The National Cyber Security Centre Finland (NCSC-FI) operates within the Finnish Communications Regulatory Authority (FICORA) and offers an increasingly diverse array of information and cyber security services. In its role as a statutory supervisory and steering authority with a responsibility for information security tasks, NCSC-FI gathers information. FICORA's other operations yield more information governed by legislation on events relating to incidents, deviations and disturbance situations (Finnish Communications Regulatory Authority 2014). The information gained from nationally or internationally detected information security incidents, deviations and threats (incident response function, CERT) is combined with the information gained from inspections of information systems and telecommunications arrangements (information assurance function, NCSA) and the information received in the role as a supervisory and steering authority. Combined, this information is used to produce NCSC-FI's combined cyber security situational picture, as illustrated in Figure 3. (Finnish Communications Regulatory Authority 2014).

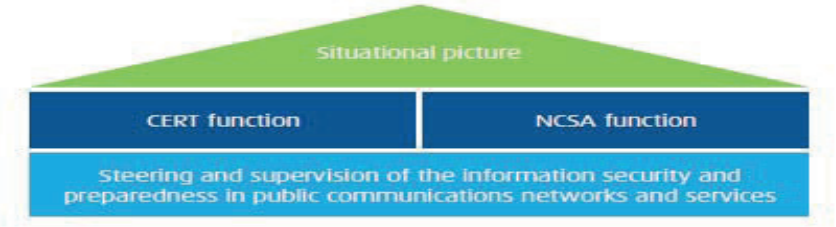


Figure 3: Producing of Finnish national cyber security situational picture (Finnish Communications Regulatory Authority 2014)

2.8.1 Alert and detection system HAVARO

HAVARO is an alert and detection system which FICORA has created in partnership with the National Emergency Supply Agency (NESA) in 2012. The National Emergency Supply Agency (NESA) is a public organization working under steering control the Ministry of Employment and the Economy. NESA is responsible for planning and measures related to developing and maintaining security of supply.

The system monitors information security incidents only, it is incapable of monitoring the communication of individual users. Red observations indicate that the system has observed harmful traffic, which points to a likely information security breach in the organization.

2.8.2 Cyber-Physical Systems

The term cyber-physical systems (CPS) was coined by Helen Gill at the National Science Foundation in the U.S. to refer to the integration of computation with physical processes. In CPS, embedded computers and networks monitor and control the physical processes. Feedback loops physical processes affect computations and vice versa. CPS are enabling next generation of "smart systems" like advanced robotics, computer-controlled processes and real-time integrated systems (Lee, Seshia 2015).

Modern infrastructures include not only physical components, but also hardware and software. These integrated systems are examples of cyber-physical systems (CPS) that integrate computing and communication capabilities with monitoring and control of entities in the physical world. Figure 4. presents a CPS that consists of two physical layers (platform layer and human layer) and a cyber layer between them. The current trend is that the cyber layer is expanding.

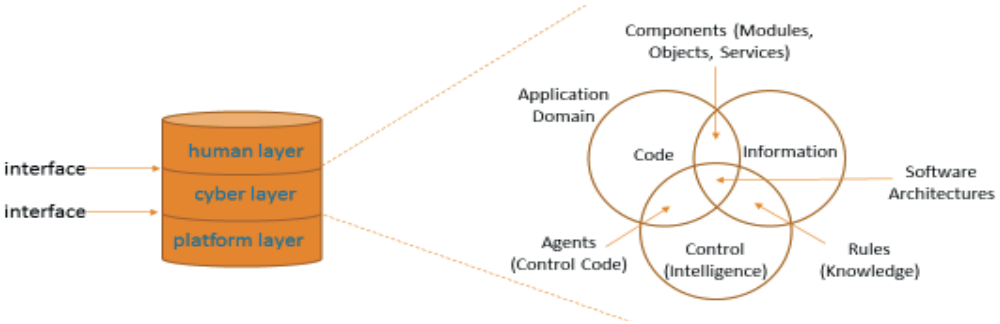


Figure 4: Layers of cyber-physical systems modified from (Hevner, Chatterjee 2010)

Many CPS applications are safety-critical which means that their failure can cause irreparable harm to the physical system under control and to the people who depend on it. In particular, the protection of our critical infrastructures that rely on CPS, such as the electric power transmission and distribution, industrial control systems, oil and natural gas systems, water and waste-water treatment plants, healthcare devices, and transportation networks play a fundamental and large-scale role in our society and their disruption can have a significant impact to individuals, and nations at large. Increasingly many CPS are operated under automated controls and a sophisticated cyber-attack can exploit weaknesses to its advantage.

2.8.3 Critical infrastructure and cyber threats

Cyber threats include denial of service (DoS), unauthorized vulnerability probes, botnet command and control, data exfiltration, data destruction or even physical destruction via alternation of critical software/data. These threats can be initiated and maintained by a mixture of malware, social engineering, or highly sophisticated advanced persistent threats (APTs) that are targeted and continue for long periods of time. Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications (National Institute of Standards and Technology 2014).

3. Research background, method, process

This case study is carried out by the guidance of Yin (2014). Case study illustrates the attempt to produce an profound and detailed information about the object under research.

Four regional command/situation centers were selected to be researched in an empirical study: Southwestern Finland Police department, Southwest Finland Emergency Services, Hospital District of Southwest Finland and The Finnish Border Guards in Turku. The Finnish Border Guards have their own main situation/command center in Turku and it´s called for Maritime Rescue Coordination Centre. The situation center of the Southwestern Finland Police department and the command centre of the The Finnish Border Guard are managed by the state. Southwest Finland Emergency Services and Hospital District of Southwest Finland act under the municipality. The field commanders of the situation centers were interviewed in their own work environment.

The materials collected for this case study are based on observations, interviews, scientific publications, collected articles and literary material. Participant observation makes it possible to get close to the actors. It illustrates the identities of actors' diversity (Viinamäki, Saari 2007), observation is made on the field and the results are recorded and saved as notes. One prominent data collecting method used was focus interviews (Brannen 2004). Eight emergency dispatch workers were interviewed.

4. Case study findings

Regional situation centers use different systems and therefore the same system can be used in two situation centers without cooperation with each other. None of the regional situation center has direct contact with the Government situation centre, but the connections are handled through intermediaries. For rapidly evolving situations access to the Government situation centres', data connection should be arranged to the essential situation centers.

As recent major accidents have indicated that lack of human resources affects to disaster recovery. PPDR-actors cannot start operations, if there is a human factor preventing the flow of information. Preventing post-accident after the disaster may be delayed. Recent violent acts at local and state level (from local to national level) have shown this to be reality. The communication activities of Intermediaries have been one of the major problems in recent major accidents. In Brussels, Belgium federal police request to close the metro and the main railway stations did not reach the responsible chief of the railway police because phone networks were down. A request to close railway station was sent to the responsible authority´s personal e-mail instead of work mail. Responsible authority did not see the message until after the attacks (McLaughlin et al. 2016). The November 2015 terror attacks also did not cause a total closure of the Paris Metro or other public arenas (The Guardian 2016, Steafel et al.). Therefore workable cyber environment with automated functions must be seen as a common objective of organized societies. The main issue regarding reliable decision support analysis to decision-makers is related to at which point in chain-reaction the human action is more harmful than useful (Endsley 1988, Endsley 2015, Endsley 1995).

4.1 Emergency situations

The lack of cooperation between situation centers prevent to create common situational awareness and picture. Starting cooperation at the scene of the accident, as Figure 5 illustrates, is not enough during a major accident in a modern cyber-physical system.

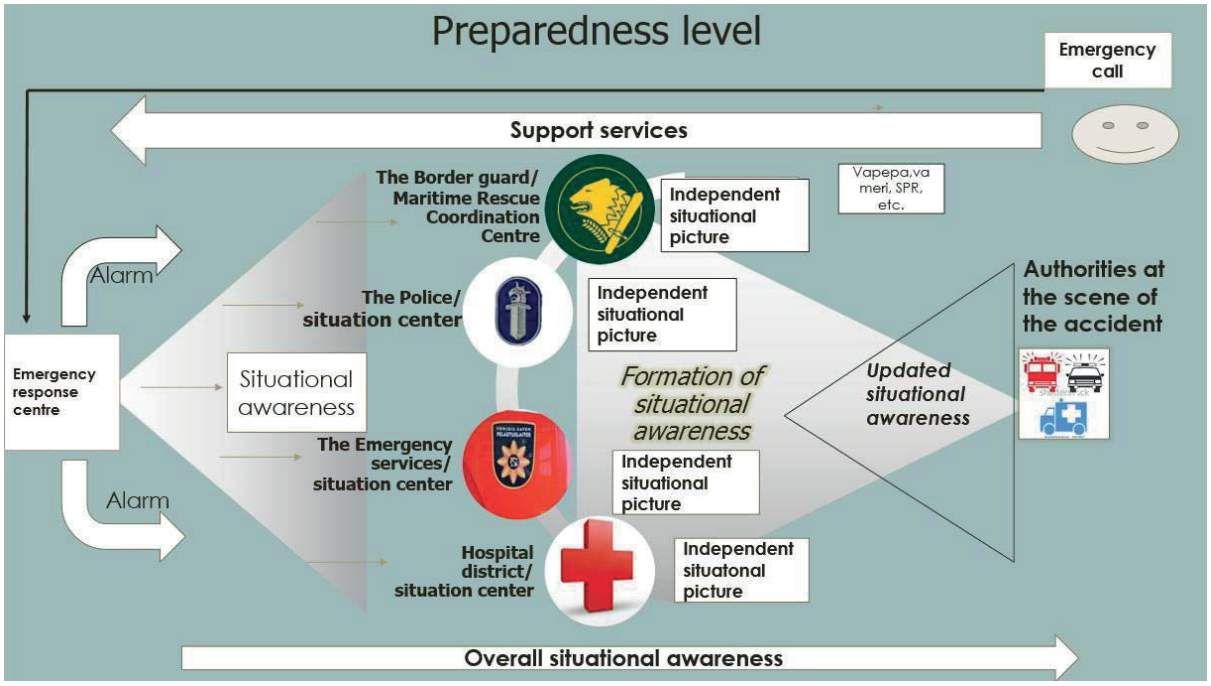


Figure 5: Formation of situational awareness

The officer in overall charge of the situation is responsible for maintaining the situational picture and for coordinating the operations. Unless otherwise agreed the officer in charge of the rescue operations comes from the rescue service region where the accident or dangerous situation occurred. Field commander and officer in charge of rescue operations decide together if it is necessary to make a major accident alert. For example The Turku University Hospital has its own command center which is set up in a case of a major accident. Leading medical director, managing dierector and other managing personnel get together in their command center depending on the type of a major accident. Communication between situation center and command center in the Turku University Hospital exists via online camera. This practice is too slow when there is a need to create a common situational picture. The differencies of rescue operations illustrate the facts that it would be important to see all the resources available. However, a reliable and correct common situational picture should be created before arriving to scene of the accident. If the scene is a modern CPS, also a cyber situational picture is needed.

As shown in a picture of smart hybrid centre model 6. proactive accident/ incident management begins before any physical harm has occurred. Sensor networks consist cyber and physical elements. Cyber environment of Hybrid model works many ways. It detects intrusions and threats in critical infrastructure before any emergency call has been made. Data fusion analysis combine and produce important signal based on commands, which launch automatic process like isolating area under threat or robotic functions based on biometrics data like thermal imaging or face recognition. Data fusion also might help with the false alarms by fusing the information from multiple sources, also false alarms can be avoided by combining sensors. The processing device (controller) sends commands to a wireless sensor and actuator network (WSAN) which then converts them into input signals for the actuator, that acts with a physical process, thus forming a closed control loop.

The field tested DSiP solution with 4com routers (Simola, Rajamäki 2014) enables parallel use of different network technologies in a consistent and transparent way, enabling communications services platforms to be created. In cyber physical operations, this feature reduce network jamming. The hybrid model reduces necessary of communication with Virve phones between authorities. It also eliminates errors of human activity, when an accident situation is on. Automated safety measures can also bypass the problems related to the commandment of power relations. Hybrid emergency response system allows people to send pictures or video calls from the scene of the accident. Smart System allows crowdsourching software screens the images and videos automatically. Relevant data from the major accident will be directly shared to the field commanders and Governments command centre. To determinate discrepancies of limits is relevant to allocate additional reliable data. Combining pieces of information to ensure the correct and reliable information to be shared is of primary importance. The essential information is processed to the desired shape for the accident site command center.

The system is based on active operations and automated functions. Cyber defense operations are integrated and automated according to local capabilities, authorities and mission needs.

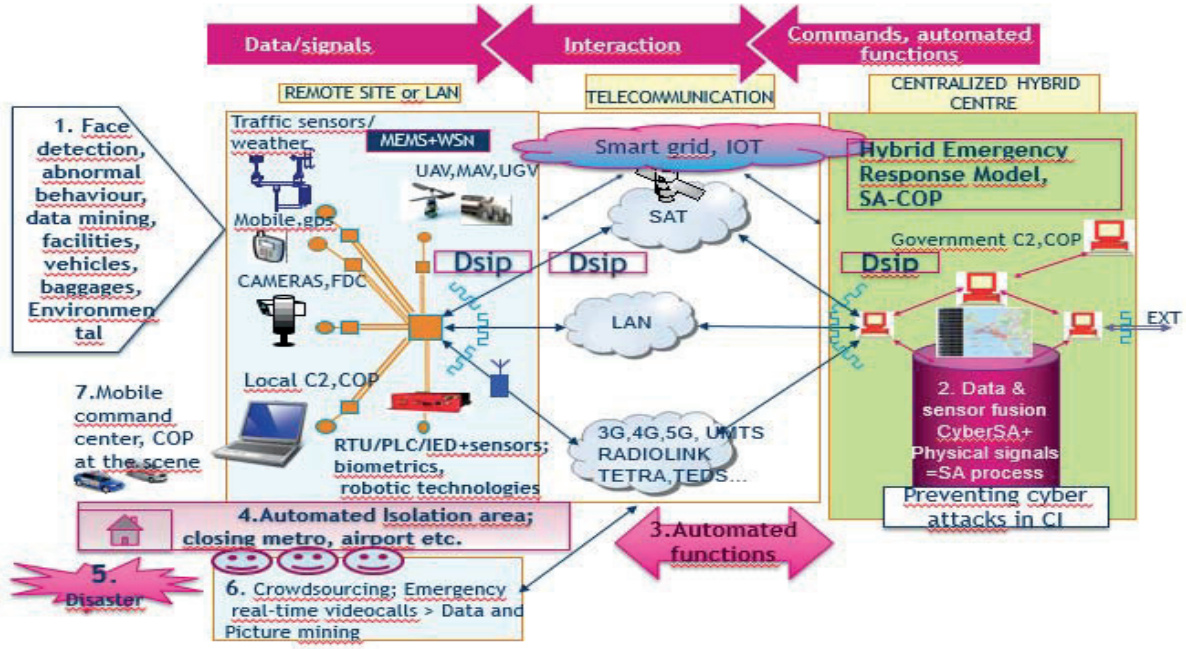


Figure 6: Smart hybrid centre model

Lack of preparedness plans affect to cooperation within PPDR authorities at the field of a major accident. Reforms in public sector and changes in PPDR organizations with legislative amendment require changes in preparedness plans. At present managerial personnel get together at each other's command centers depending on the type of the accident.

Today, too many hierarchy levels in and between organizations exist. Therefore, settling new technology faces challenges. If there are too many hierarchy levels, information of situation does not flow or, at least, it is slow (Rajamäki, Viitanen 2014). Responsibilities for developing cybersecurity has been shared too many factors (Ministry of the Interior 2016, Ministry of defence 2010, Finnish Communications Regulatory Authority 2014, Kauppinen 2015, National Cooperation Network for Disaster Risk Reduction 2012).

5. Discussion

Both the European and the American regulations aim at achieving cyber resilience enhancing cooperation between public and private sectors in order to improve capacities, resources and processes to handle cyberphysical threats in critical infrastructures. But that´s not enough. There is a need for common cyber ecosystem to control crossboarding threats.

Traditional thought within Finnish decision-makers has been that the commercial operators must be kept separate from regulatory activities. In U.K. The Home Office-led Emergency Services Network (ESN) will replace the existing Airwave mobile radio system. ESN will be delivered using commercial network. The police communications network enabling officers to access key databases, to take electronic fingerprints and witness statements, and to stream live video while on the move (Nasir 2016, Travis 2015).

6. Conclusions

The need for a new type of hybrid emergency response model reflects the following factors; A human is an individual with limited observation capability. Overlapping and limited data transmission and lack of real time data capabilities prevents the effective cooperation between security authorities. No one of the situation centers of this case study has a possibility to direct communication connection to the Government situation centre. Fight against cyber threats is an essential part of the overall security in SA management. Instead of separate situation centers, there should be a common regional situation center where different state and municipality PPDR actors and decision-makers could get together when a major accident occurs.

Often, urban built infrastructures represent a critical node within the intertwined networks of an urban area. Substantial part of our CPS today relies on complex systems of communication networks. There is just as much of a need to take in to account the equally vulnerable built infrastructures of modern urban areas. (Davis et al. 2006).

As Figure 7 shows, a situational awareness (SA) system itself is a CPS, cyber SA being a subset of it. Situational awareness is a prerequisite for CPS to be resilient. According to Franke and Brynielsson (Franke, Brynielsson 2014), cyber SA cannot be treated in isolation, but it is intertwined with and a part of the overall SA. Cyber SA indeed concerns awareness regarding cyber issues but these need to be combined with other information to obtain full understanding regarding the situation.

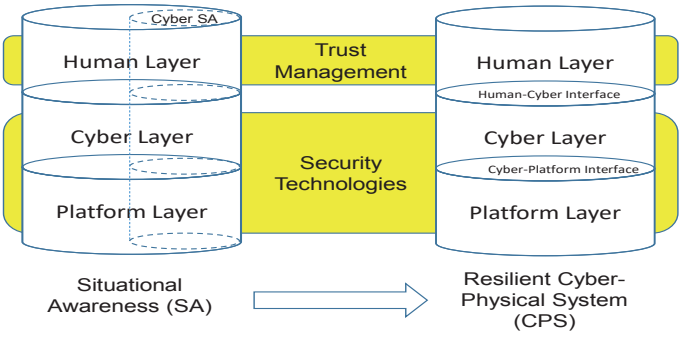


Figure 7: Situational awareness as a prerequisite of the resilience of a cyber-physical system

In the future centralized hybrid emergency model with emergency response functions is necessary. Shared common operational picture means that real time communication link from local level to state level exist. At the moment flow of real time data is not been transmitted to the Government command centre. E.g. if a cyber attack interrupted electricity transmission, telecommunication networks discontinue operating. Cyberattack become physical, if intrusion has not been detected. Hybrid warfare need hybrid responses. The government departments of Finland must take into considerations that cyber preparedness is not a separate part in the continuity management. In practice this means that there is need to integrate e.g. Emergency Response Centre and National Cyber Security Centre Finland emergency functions.

References

Ahmed, D.T., Hossain, M.A., Shirmohammadi, S., Alghamdi, A., Pradeep, K.A. and El Saddik, A. (2012) Utility based decision support engine for camera view selection in multimedia surveillance systems DOI 10.1007/s11042-012-1294-7.

Ahokas, J., T. Guday, T. Lyytinen and J. Rajamäki (2010) Secure and Reliable Communications for SCADA SystemsAnonymous *INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS*.

Aine, A., Nurmi, V., Ossa, J., Penttilä, T., Salmi, I. and Virtanen, V. (2011) *Moderni kriisilainsäädäntö.* Helsinki: WSOYpro.

Baldini, G. (2010) *Report of the workshop on "Interoperable communications for Safety and Security" with recommendations for Security research.* Publications Office of the European Union DOI 10.2788/19075.

Brannen, J. (2004) Working qualitatively and quantitatively. In: Seale C., Gobo G., Gubrium J.F. and SILVERMAN D. eds., *Qualitative Research Practice* London: Sage Publications, pp. 312-326.

Chong, C. and KUMAR S. (2003) Sensor Networks: Evolution, Opportunities and Challenges, *IEEE*.

Davis, R., Ortiz, C., Rowe, R., Broz, J., Rigakos, G. and Collins, P. (2006) An assessment of the preparedness of large retail malls to prevent and respond to terrorist attack. (No. 216641).

Electrical Technology (2016) *Internet of Things (IOT) and Its Applications in Electrical Power Industry.* ET. [viewed 11/8/2016]. http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html.

Endsley, M.R., (1995) Toward a theory of situation awareness. Human Factors, no. 37, pp. 32-64.

Endsley, M.R. (1998) Design and evaluation for situation awareness enhancement. Anonymous *Proceedings of the Human Factors Society 32nd Annual Meeting*.

Endsley, M.R. (2015) *Autonomous Horizons, System Autonomy in the Air Force – A Path to the Future.* Air Force Office of the Chief Scientist.

Franke, U. and Brynielsson, J. (2014) *Cyber situational awareness: A systematic review of the literature*. In: *Computers & Security*, pp. 18-31-46 DOI 10.1016/j.cose.2014.06.008.

Finnish Communications Regulatory Authority (2014) *National cyber security centre: Action plan 2014-2016*.

Gervasi, O. (2010) Encryption Scheme for Secured Communication of Web Based Control SystemsAnonymous *Encryption Scheme for Secured Communication of Web Based Control Systems*.

Hanni, J. (2013) *The quality and amount of information for emergency situations management.*

Hevner, A. and Chatterjee, S. (2010) *Design science research in information systems*. In: *Design Research in Information Systems: Theory and Practice.*Springer Science and Business.

Kauppinen, T. (2015) *CYBER SECURITY OF SUPPLY, FIIF JAM SESSION.* National Emergency Supply Agency, 22nd September 2015.

Lee, E., Ashford and Seshia, S., Arunkumar (2015) *Introduction to Embedded Systems, A Cyber-Physical Systems Approach.* 2nd ed. Lee&Seshia ISBN 978-1-312-42740-2.

Mclaughlin, E., Haddad, M. and Hume, T. (2016) *Brussels attacks: Order to close metro sent to wrong address - CNN.com.* Available from: http://edition.cnn.com/2016/05/12/europe/belgium-brussels-attacks-metro-email/.

Ministry of the Interior (2016) *National Risk Assesment 2015.* Helsinki: Ministry of the Interior ISBN 2341-8524/ISBN 978-952-324-060-5 (PDF).

Nasir, R. (2016) LTE to replace TETRA network for UK emergency services – Networking.

National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) (2016) *NENA/APCO Next Generation 9-1-1 Public Safety Answering Point Requirements.* USA: NENA and APCO.

National Cooperation Network for Disaster Risk Reduction (2012) *National Platform for Disaster Risk Reduction.* Helsinki: Ministry of the Interior.

National Institute of Standards and Technology (2014) *Guidelines for smart grid cybersecurity National Institute of Standards and Technology, Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements.* U.S. Department of Commerce DOI. DOI 10.6028/NIST.IR.7628r1.

National Public Safety Telecommunications Council. (2015) *FirstNet and Next Generation 9-1-1 High-Level Overview of Systems and Functionality.*

NEC Corporation. *Face Recognition: Technologies: Biometrics: Solutions & Services | NEC.* [viewed:11/15/2016]. Available from: http://www.nec.com/en/global/solutions/biometrics/technologies/face_recognition.html.

Ministry of defence (2010) *Security strategy for society, Government resolution.* Helsinki: Ministry of Defence; ISBN ISBN: 978-951-25-2235-4 pdf.

Rajamäki, J. and Viitanen, J. (2014) Near border information exchange procedures for law enforcement authorities. International Journal of Systems Applications, Engineering & Development, 8, 2015-2020.

Secretariat of the Security Committee (2013) *Finland´s Cyber Security Strategy - Government resolution.* Ministry of Defense.

Simola, J. and Rajamäki, J. (2014) Using a real-time video to allocate public protection and disaster relief resources in rescue service process - Natural diaster in Young voluntary firefigter´s camp *5th European Conference of COMPUTER SCIENCE (ECCS '14) 72007-127*. Geneva, Switzerland.

Steafel, E., Mulholland, R., Sabur, R., Malnick, E., Trotman, A. and Harley, N. Paris terror attack: Everything we know on Saturday afternoon - Telegraph. *The Telegraph* (11/27/2016).

The Finnish Security Intelligence Service (2015) *The Year Book.* Helsinki: Ministry of the Interior.

The Guardian (2016) Paris attacks inquiry finds multiple failings by French intelligence agencies.

Travis, A. (2015) Questions over limited range of new £1bn emergency services network. *The Guardian*.

Viinamäki, L. and Saari, E. (2007) *Polkuja soveltavaan yhteiskuntatieteelliseen tutkimukseen.* Helsinki: Kustannusosakeyhtiö Tammi.

Yin, R.K. (2014) *Case Study Research, Design and Methods.* 5th ed. Thousand Oaks: Sage Publications.

II

IMPROVING CYBER SITUATIONAL AWARENESS IN MARITIME SURVEILLANCE

by

Jussi Simola & Jyri Rajamäki, 2018

Proceedings of the 17th European Conference on Cyber Warfare and Security
ECCWS 2018. 28-29.6.2018. Oslo, Norway, 424-431

https://urn.fi/URN:NBN:fi-fe2018090334419

Improving Cyber Situational Awareness in Maritime Surveillance

Jussi Simola and Jyri Rajamäki
Laurea University of Applied Sciences, Research, Design and Innovations, Finland
simolajussi@gmail.com
jyrirajamaki@laurea.fi

Abstract: Maritime surveillance has become one of the main areas in managing overall situational awareness. For example, the growing importance of maritime traffic in cross-border trade has created new pressures to develop new technologies for accident prevention. Maritime safety is also a matter of concern for continuity management. Automatic ship alarm systems, coastal radars and coastal cameras are not alone sufficient equipment to build maritime awareness. The Universal Shipborne Automatic Identification System (AIS) is a ship transponder system that is currently used by most actors in the commercial shipping industry. Ships equipped with an AIS transponder send out a packet every few seconds with data about the ship and its journey. The transponder transmits and receives information on VHF channels. This globally used tracking system is highly vulnerable to hacking. A major maritime traffic problem arises if transponders are switched off. Hybrid threats need coordinated hybrid responses; therefore, a cyber situational picture is also needed. The cyber dimension is an essential part of the management of situational awareness. This study was conducted on the ground by visiting four situation and command centers of the Public Protection and Disaster Relief services located in Southwestern Finland. The main results can be summarized so that the failure to use ship transponders affects misuse of the authorities' technical and physical resources. Also, the lack of real time data from ships with limited data transmission capacity affects the correct formation of the common situational picture—for example, from the site of an accident. The technical communication solutions of the PPDR authorities should be more standardized and management should be more centralized. A hybrid emergency model with emergency response functions is necessary. Currently, the flow of real time data is not being transmitted, for example, from cruise ships to the Maritime Rescue Coordination Centre. The developed Hybrid Emergency Response model is a unique concept that can be transferred to the maritime environment. By using the OSINT (Open Source INTelligence) process in the hybrid emergency model, it is possible to gather meaningful intelligence data related to maritime security. Essential open source information has geospatial dimensions. The main purpose of the study is to enhance maritime safety and create a common intelligent maritime emergency management system for public safety organizations.

Keywords: cyber security, hybrid emergency response, PPDR, OSINT, early warnings

1. Introduction

European governments and the European Public Protection and Disaster Relief services—such as law enforcement, firefighting, medical emergency, disaster recovery and military services, but also voluntary associations like civil protection activity or voluntary firefighters—have recognized that the lack of interoperability of technical systems limits cooperation between authorities.

At the EU level, for example, the Common Information Sharing Environment (CISE), the European Coast Guard Functions Academy Network II (EFGA NET 2), the Early Warning for Increased Situational Awareness (EWISA), Safety Authorities in the Arctic Countries (SARC) and Maritime Integrated Surveillance Awareness (MARISA) are all currently being developed together by the European Commission and EU/EEA Member States (The Finnish Border Guard, 2017, Marisa, 2017).

A domestic strategy plan such as the National CBRNE strategy demonstrates that maritime safety is one of the main focus areas when the purpose is to develop a common situational maritime awareness for different authorities and decision-makers. The overall aim of the strategy is to continuously improve the prevention of and preparedness for CBRNE threats and incidents in order to safeguard society and secure the functions vital to society. CBRNE threats refer to hazardous incidents caused by chemical substances (C), biological pathogens (B), radioactive material (R), nuclear weapons (N) and explosives (E) as well as by the misuse of expertise related to these (CBRNE strategy working group, 2017).

The Finnish Border Guard (including the coast guard services) acts under the authority of the Ministry of the Interior but can be incorporated fully or in part into the defense forces when required by defense readiness. The Finnish Defence Forces also monitors sea areas to detect and locate accidents, abnormal events and emergency phases in conjunction with the surveillance of territorial integrity and participates in SAR operations by providing access to its special expertise, personnel and equipment (Kaukanen, Möttönen, 2010, Ministry of the Interior, 2005).

The Finnish Border Guard ensures the security of Finland and prevents security threats directed towards Finland and Europe at external borders. The Finnish Border Guard has many important tasks. Crime prevention is one of the most important areas. It also takes care of people's safety in the border area and on islands.

Coast guard services may include search and rescue (SAR) at sea and in the air, the protection of coastal waters, criminal interdiction, illegal immigration and disaster and humanitarian assistance in operational areas. These functions may vary according to the administration, but the core functions are generally the same. The Finnish maritime search and rescue (SAR) system is one part of the wider security system of the Finnish Border Guard. The Finnish Border Guard has immediate readiness for management and operations during maritime incidents. The Coast Guard also promotes the protection of the maritime environment and it covers 1,250 kilometers of territorial waters (The Finnish Border Guard, 2018; Kaukanen & Möttönen, 2010; Ministry of the Interior, 2005).

Maritime safety has become one of the main discussion areas between public safety authorities and decision-makers in Europe. Overall situational awareness requires different kinds of technical solutions that can combine and produce correct real time data to support correct decisions. Hybrid threats require a coordinated hybrid response. Therefore, a cyber situational picture is an occasional factor when authorities need to create a common situational picture—for example, from the scene of an accident. If oil tankers were to collide in the Gulf of Finland, the ships could spill up to 30,000 tons of oil into the sea. It is important that the nature of the accident is evaluated as soon as it occurs, and the observer must immediately inform the state leadership of major ship accidents.

2. Theoretical framework

2.1 Maritime situational awareness and new automated and unmanned technology

According to the Ministry of Defence (Ministry of Defence, 2010) situational awareness means the understanding of decision-makers and their advisors of what has happened, the circumstances under which it happened, the goals of the different parties and the possible development of events, all of which are needed to make decisions on a specific issue or range of issues. A general definition of situational awareness is the perception of the elements in the environment within time and space, the comprehension of their meaning and the projection of their status in the near future (Endsley, 1988). "Situational awareness is the ability to identify, process and comprehend the critical information about an incident. It is knowing what is going on around you. Situational awareness requires continuous monitoring of relevant sources of information regarding actual incidents and developing hazards" (Homeland Security, 2008).

According to Franke and Brynielsson (2014), cyber situational awareness is a subset of situational awareness, i.e. cyber situational awareness is the part of situational awareness that concerns the cyber environment.

Communications include sharing and the distribution of information: computer systems; control systems (e.g. supervisory control and data acquisition, SCADA); networks, such as the Internet; and cyber services (e.g. managed security services), which are all part of the cyber infrastructure.

The European Union has funded many unmanned maritime situational awareness projects. It has been seen as a future goal to develop and produce automatic solutions for the maritime environment. Unmanned systems, vessels and aerial vehicles will gradually replace human resources. Such technological development also means that information systems are more vulnerable to different types of threats, such as cyber threats. Therefore, advanced solutions are needed to prevent different kinds of threats. Maritime actors, such as shipbuilders, shipping companies and harbors, would need to ensure that their autonomous vessels are protected against attacks by hackers or pirates. In other cases, new technology faces big problems because the responsibility for maritime traffic is shifting from human actors to automated functions.

Maritime surveillance is understood as the process of watching, monitoring, recording and processing the behavior of people, objects and events in order to control activity. The aspects of maritime surveillance discussed in this paper include border control, safety and security, customs, fisheries control and environmental protection (Kaukanen & Möttönen, 2010).

2.2 Organizational influences in Finnish maritime security

The structural changes within the public sector, such as the regional administration reform, the Emergency Response Centre (ERC) reform and ongoing social welfare and health care reform, have influenced the work processes of public sector employees over the past ten years. Due to the regional administrative reform, preparedness plans also need to be changed.

The Baltic Sea Maritime Incident Response Group (Baltic Sea MIRG) project was established by the Finnish Border Guard as the responsible maritime search and rescue authority in cooperation with Finland's Emergency Rescue Services. MIRG is an international project led by the Finnish Border Guard. The purpose of this is to create a MIRG coordination model and operational guidelines for international MIRG operations and to support the harmonization of MIRG services in Europe (Finnish Border Guard - Finnish Transport Safety Agency, 2016).

The Finnish Border Guard is the lead SAR authority and responsible for coordinating all SAR activity. It has a direct emergency number for emergency situations. Under the Maritime Search and Rescue Act (Ministry of the Interior, 2005), the Finnish Border Guard:

- Is responsible for planning, developing and supervising all SAR activity as well as coordinating cooperation with other public authorities and volunteers.
- Coordinates and conducts search and rescue operations.
- In the event of an emergency, is responsible for coordinating radio communications and facilitating telemedical assistance services between medical care providers and vessels.
- Works to prevent accidents and emergencies.
- Is responsible for the Maritime Assistance Service (MAS).
- Is responsible for receiving all distress signals received from maritime, aviation and private emergency transmitters and conveying such signals to the relevant national authority as well as the national coordination of all COSPAS-SARSAT matters.
- Provides SAR leadership training and other SAR-related education and training.

The Finnish Border Guard takes part in search and rescue operations in its control area by providing the equipment, personnel resources and expert services needed for search and rescue operations if the scale or special nature of the incident makes this necessary. Participation in search and rescue may not endanger performance of the border guard functions and the country's military defense services.

The Finnish Border Guard may perform functions in its control area that are needed to find and assist persons who have got lost in open country or are otherwise in need of immediate assistance there. The responsibility for leading searches for missing persons rests with the police. Separate provisions are laid down on Finnish Border Guard functions as part of the maritime search and rescue service (Ministry of the Interior, 2005a; Ministry of the Interior, 2005b; Ministry of the Interior, 2009).

The Finnish Border Guard may, using its vessels, aircraft and other special vehicles, provide urgent ambulance transport in its control area that the authorities or ambulance service enterprises otherwise handling ambulance transport are unable to perform because they lack the vessels, aircraft or other special vehicles (Ministry of the Interior, 2009; Ministry of The Interior, 2005).

In its control area, the Finnish Border Guard may provide the kind of special transport that the State is required to provide in order to ensure a person's personal safety when no other State authority can provide such transportation. The Finnish Border Guard may also, upon request, give executive assistance to some other authority in its control area that is required by law to perform a control function (Ministry of the Interior, 2005).

2.3 Intelligence solutions for public safety organizations

OSINT is defined as the systematic collection, processing, analysis and production, classification and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security. It is any unclassified information, in

any medium, that is generally available to the public, even if its distribution is limited or only available upon payment (Glassman & Kang, 2012; Morrow & Odierno, 2012; Nurmi, 2015).

Most information has geospatial dimensions. Examples of geospatial open source include maps, airborne imagery, atlases, gazetteers, port plans, gravity data, aeronautical data, navigation data, geodetic data, human terrain data (cultural and economic), environmental data, commercial imagery, LIDAR, hyper and multi-spectral data, geo-names and features, urban terrain, vertical obstruction data, boundary marker data, geospatial mashups, spatial databases and web services. Most of the geospatial data mentioned above is integrated, analyzed and syndicated using geospatial software such as a Geographic Information System (GIS) (Morrow & Odierno, 2012; Nurmi, 2015; Trottier, 2015; Vetter, 2015; Wood, 2016).

Social Media Intelligence (SOCMINT) identifies social media content in particular as a challenge and opportunity for open source investigations (Trottier, 2015). Big data includes processes of analysis, capture, research, sharing, storage, visualization and safety of information. Associated with OSINT, Big Data is the ability to map standards of behavior and tendencies (Dos Passos, 2016). The availability of worldwide satellite photography, often of high resolution, on the web (e.g. Google Earth Pro) has expanded open-source capabilities into areas formerly available only to major intelligence services.

2.3.1 Centralized cyber threat detection

One way of examining cyber security content automation is through the generalized functional model in use by the standards community. As illustrated in Figure 2, the security functions contained in this model generally represent the first wave plus a portion of the second wave. Security content automation standards that can facilitate the exchange of information with and among functions are annotated adjacent to each function, input or output. In general, the functions left to right can be organized into “preincident detection” (asset inventory, configuration guidance analysis, vulnerability and threat analysis) (National Protection and Programs Directorate, 2011).

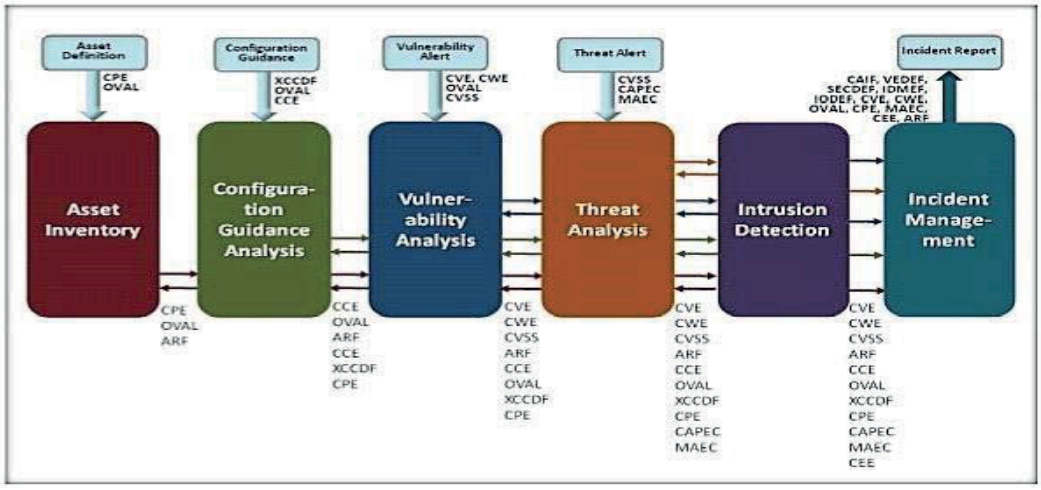


Figure 1: Centralized threat detection system

2.3.2 Multi-layer maritime intelligence system Kingfisher

Kingfisher is based on a multi-sensor, multi-layer maritime intelligence system that combines a variety of information sources to expose the covert movements of vessels and boats. Utilizing Satellite Automatic Identification system (S-AIS) data, Synthetic Aperture Radar satellite imagery, electro-optical satellite imagery, Vessel Monitoring Systems (VMS), coastal radar, open source intelligence (OSINT) and weather patterns, the system is one of the most developed in maritime cyber-physical ecosystems (ISI, 2017).

2.4 Emergency maritime communications

European authorities communicate with each other through the Virve network. There is a need to create a new and trusted network with a wide bandwidth. Transmission capacity is often limited in an overload situation, therefore there is a need to develop new hybrid communication models to utilize real time data.

Shipping in the Baltic Sea, for example, is continuously monitored using AIS tracking. By analyzing historical data regarding vessels, the identity, type, position, speed and traffic intensity can be mapped in detail and provide important input to marine spatial planning. Along with more precise information about the monitored ships and the results of port state controls, AIS data can also make it easier to assess different short- and long-term effects of shipping on the marine environment. There are several AIS tracking websites on the internet that citizens can visit and use (SIME, 2014).

The use of emergency services with the COSPAS-SARSAT satellite system requires an emergency transmitter. Locating an emergency transmitter in emergency situations is much more accurate and faster if the emergency transmitter also includes GPS positioning. Figure 1. illustrates how the COSPAS-SARSAT system works (Secretariat of the Cospas-Sarsat Programme, 2016).

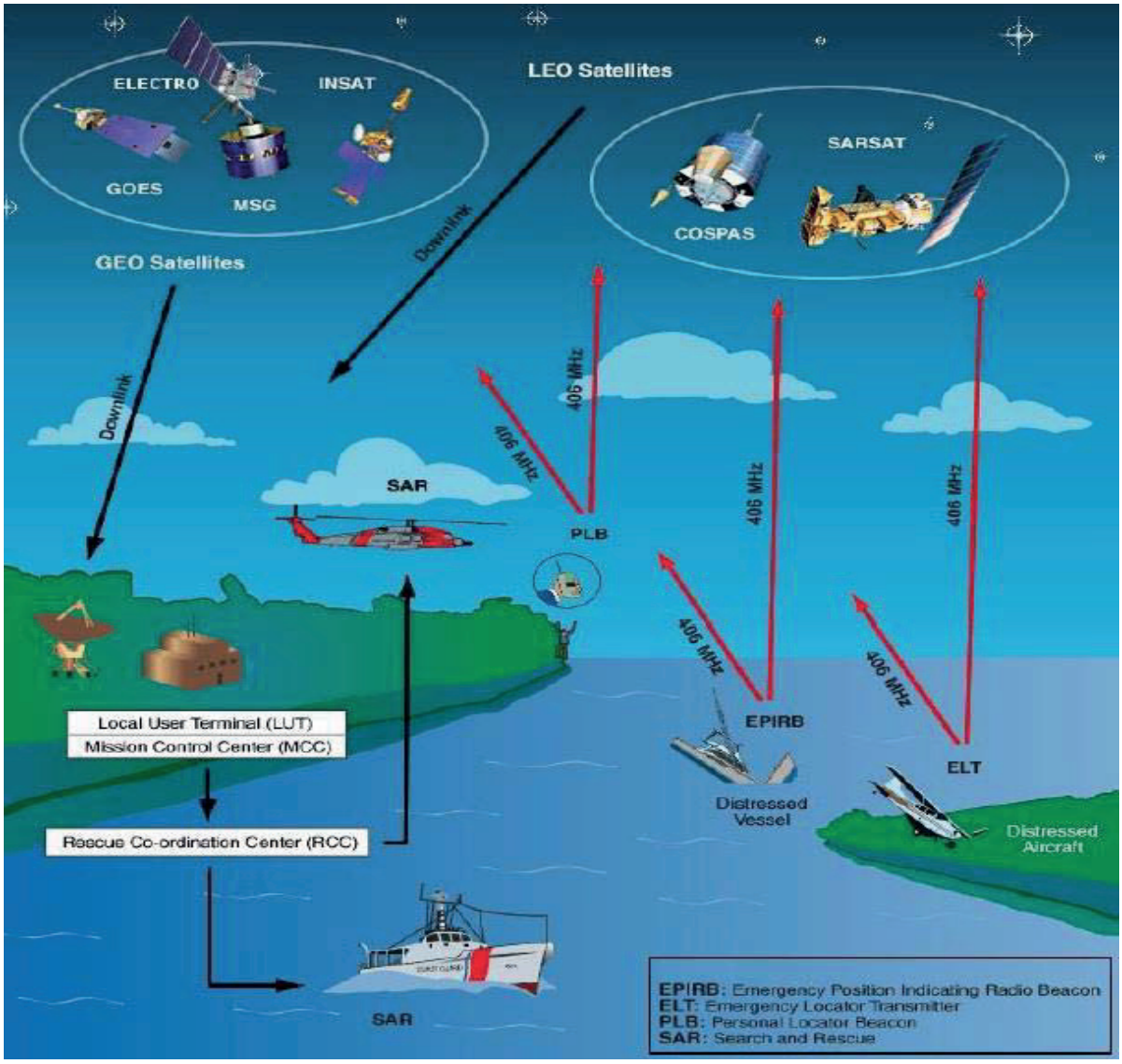


Figure 2: Basics concept of the COSPAS-SARSAT system

2.4.1 SAR suitable equipment

The Finnish Border Guard's vessels and aircraft are used in 70 per cent of all maritime SAR activity in Finland (The Finnish Border Guard, 2018). Patrol vessel *Turva* started operations in 2014. The vessels underwater activities center provides the ability to create an underwater situational picture. Vessels are also identified at the request of other authorities in relation to their needs. With its sensors, *Turva* brings more performance to METO cooperation. The underwater activities center is used to conduct underwater activities. The DP2 classified standby system enables efficient and safe operation at the side of the accident. *Turva's* equipment includes different kinds of systems, such as a 3D radar, thermal camera, searchlight and scanning sonars and modern

ROV equipment. In connection with the use of ROV equipment, the two *Turva* crews have continuous preparedness to use divers. The *Super Puma* together with *Turva* provide quick access to additional information, such as information about identifiable objects or target areas. NVG functions, the Virtual Horizon system and the HVLA (Helicopter Visual Landing Aid) system enable safe cooperation (Simola et al., 2015).

2.5 Distributed Systems Intercommunication Protocol (DSiP)

DSiP enables multiple simultaneous communication channels between the remote end and the control room: if one communication channel is down, other channels will continue to operate. DSiP makes communication reliable and unbreakable by using various physical communication methods in parallel. Applications, equipment and devices can communicate over a single unbreakable data channel. Satellite, TETRA, 2G/3G/4G, VHF radios and other technologies can be used simultaneously. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication. The latest innovation is an all-in-one solution DSiP-router-laptop (Rajamäki & Villemson, 2009; Simola & Rajamäki, 2015).

3. Research background, method and process

PPDR authorities are tasked with the challenge of providing the first response in life-critical circumstances. The ability to create the right situational awareness and reliable communication with each other are the most important issues between the PPDR, military and voluntary services.

The West Finland Coast Guard District has its own main situation and command center in Turku and it is called the Command and Maritime Rescue Coordination Centre (MRCC Turku). The approach of this case study handles mainly the West Finland Coast Guard District and the Command and Maritime Rescue Coordination Centre and their relationship to each other's situation centers and emergency response centers.

This case study is carried out with the guidance of Yin (2014). The case study illustrates the attempt to produce profound and detailed information about the object being researched. The materials collected for this case study are based on observations, interviews, scientific publications, collected articles and literary material. Interviewees were chosen on the basis of their expertise in their specialist roles: they operate or have operated in public safety organizations. One of the interviewees has been a technical developer in public safety organizations. The interviews were recorded and analyzed using the qualitative content analysis method.

The case study's empirical research approach is due to the fact that the researcher had to study more deeply the culture of the situational centers and the actual working environment of employees working in the field. Participant observation makes it possible to get close to the actors.

4. Case study findings

The Finnish Border Guard uses mainly Virve telephones for communication between authorities, but VHF and MF connections are also widely used in the coastal area. They have a direct emergency number for emergency situations. In addition, the emergency calls placed by citizens can be redirected from the Emergency Response Centers to the MRCC Turku. Their own command and control center (the Command and Maritime Rescue Coordination Centre) reserves cooperation in multi-authority situations if a long-standing major accident occurs. In a situation such as this, managerial personnel such as a rescue manager or a police field manager meet in the control and command room to work with each other. The Command and Maritime Rescue Coordination Centre (MRCC Turku) is their management and marine rescue center. The management relationships may be unclear in such cases, therefore it is important to meet. Different authorities do not receive real time information about available aid from voluntary associations, not even the Maritime Rescue Coordination Centre.

The West Finland Coast Guard District is responsible for security in the whole sea area in Western Finland. They have a situation and analysis team that is there for half of the day. The same group has three customs officers who work with them daily. It is a daily operational mode.

The area of operations of the West Finland Coast Guard District covers the emergency area of four emergency centers. Virve has only a maximum of 20 call groups per workstation. This means that the monitored area is quite wide and one major accident will relocate resources from daily routine to a more serious accident. It is possible to control all the groups that they want with one terminal device, but they have to share the groups

between the different workstations. This procedure helps them better analyze events. The field commander and officer in charge of rescue operations decide together if it is necessary to issue a major accident alert. The coast guard does not have a shared situational awareness system for cross-border cooperation. Currently, the situational picture of an individual patroller is based on the Virve communications and background information that has been collected before via radio communication, for example. There is no possibility to use visual real time data communication systems, but the surveillance aircraft has a good camera that records events and transfers data to the MRCC. The use of real time video is not currently possible. The flow of real time data is not transmitted, for example, from cruise ships or from patrol vessels to the Maritime Rescue Coordination Centre. Small ships or boats that are attempting to cross the Schengen border create additional challenges, especially in situations where the transponders are switched off. They have a certain number of cameras in the archipelago and in places they support border control. The cameras allow tracking and identifying which ships are operating there. Underwater surveillance is carried out in cooperation with the Finnish Navy.

Operational field work covers statutory tasks involving the leading positions of other authorities as provided by the law on the Border Guard (Border Guard Act) such as executive assistance tasks and the management of Maritime Rescue. It includes, for example, that oil spills and initial actions for the fight against oil spills belongs nationwide to them, also in the Gulf of Finland. Concerning sea rescue, international contacts are handled in neighboring countries and, as the case may be, more broadly. A special function is the coordination of the entire Finnish Border Guard's flight operations as appropriate. Airbase stations are located in Helsinki, Rovaniemi and Turku.

In Turku, there is also a surveillance aircraft. Aviation operations are coordinated by a field commander in Turku. If the Gulf of Finland coast guard has a sea rescue mission, they can use aerial vehicles in Helsinki. Helicopters are widely used by other authorities in their tasks, such as to transfer patients to hospitals and to search for fire. They practice and participate in multiauthority exercises, major accident exercises and rescue exercises. There are several maritime rescue authorities in Finland that, using their own special expertise, take part in the task and, accordingly, border control takes part in other tasks and helps with the equipment if necessary.

5. Discussion

Computing technology in most control centers, situational centers and emergency response centers is based on sequential computing and the infrastructure based on human capabilities and activities. To support the next-generation hybrid smart control center monitoring, analysis and control functions, the parallel computing infrastructure needs to be implemented with proper prioritizing and scheduling different real time simulation tasks.

Government agents, utility executives, policymakers and technology providers must agree on a common goal and take actions to accelerate the process towards final deployment, and legal and organizational barriers have to be removed. Given the scale of the effort required and the enormity of the challenges ahead, collaboration among different sectors is essential and should be developed through various channels in order to ensure and accelerate the success of the future smart control centers.

6. Conclusion

Limited data transmission and the lack of visual real time data capabilities prevent the formulation of an accurate situational picture in MRCC Turku. Coast Guard patrols cannot share real time information with other patrols or the MRCC Turku. There is a need to strengthen the entire maritime intelligence ecosystem. The greatest need for new sensor technology is at sea (Lemponen, 2012). There is also a need in command and control functions to design a combination of a new kind of hybrid sensor technology that uses OSINT tools in order to detect threats in advance because a cyber situational picture is needed. For example, drug trafficking can be prevented by more effective hybrid-based intelligence.

Effective cooperation between security authorities needs a common technology for all authorities. Municipal actors relying on municipal technical resources is not sustainable because cooperation between the Finnish Border Guard and emergency services has developed, especially at the site of the scene of maritime accidents. Organizational cooperation requires a common infrastructure and clearer and faster connections. The DSiP telemeter includes mobile communication, IT systems and a command and control center. The DSiP solution is already in use with the Finnish Border Guard, but its potential could be better utilized (Hult, 2012).

Open source intelligence is an applicable emergency response tool for public safety authorities. The presented hybrid model will offer an updated emergency response management model to PPDR services. Currently, new information systems are already out of date when they are introduced.

A dynamic cyber-physical ecosystem or infrastructure is needed in order to respond to a rapidly evolving maritime alert situation. It is obsolete to manage public safety organizations as separate public safety actors. The internal and external security atmosphere can no longer be separated in the traditional sense. Threats have changed into combinations of threat types and, as a consequence, public safety organizations like the Finnish Border Guard must be able to prevent new kinds of hybrid threats and respond to them. Improving the flow of information between the public sector and citizens, including volunteer associations, is also a relevant part of this framework. It must be possible to prevent and respond faster to the realization of threats. A modelling platform for a smart emergency response model can lead to important new results. The cyber domain can be used as a powerful dimension to enhance data fusion to more accurate overall situational awareness. By processing raw data on anomalous behavior in advance, PPDR services can use smart emergency response functions before any threats have occurred, as illustrated in Figure 3.

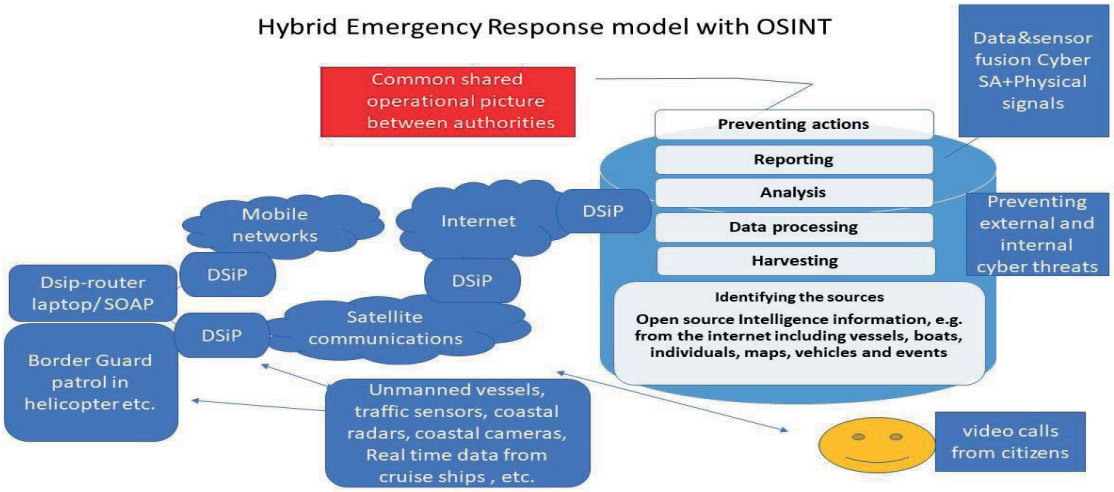


Figure 3: Hybrid Emergency Response model with OSINT

The next generation hybrid model will integrate existing surveillance systems and networks with new ones and give all concerned authorities access to the information they need for their missions at sea. Combining pieces of open source information to ensure correct and reliable information is shared is of primary importance. The essential information is processed in the desired form for the accident site command center. The next generation emergency response system is based on active operations and automated functions. At the very least, a direct communication connection without unnecessary intermediaries must exist from the situation center to the government situation center.

References

Act on Cooperation between the Police, Customs and the Border Guard, 687 (2009).

Border Guard Act, 578 (2005).

Border Guard Administration Act, 577U.S.C. (2005b).

The Border Guard in Figures - the Finnish Border Guard. Retrieved from https://www.raja.fi/facts/the_border_guard_in_figures

CBRNE strategy working group. (2017). National CBRNE strategy 2017. (No. 32). Ministry of the Interior.

Cospas-Sarsat Programme (2016). Cospas-Sarsat system data. (No. 42). Canada: Secretariat of the International Cospas-Sarsat Programme.

Dos Passos, D. (2016) “Big data, data science and their contributions to the development of the use of open source intelligence. Systems & Management, 11 p 392–396

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors Society 32nd Annual Meeting, 97–101.

Finnish Border Guard and Finnish Transport Safety Agency. (2016). Baltic Sea MIRG - European maritime traffic risk assessment on ship fires. Ministry of the Interior.

The Finnish Border Guard. (2018) Finnish Border Guard maritime SAR suitable equipment. Retrieved from http://www.raja.fi/sar/en/equipment

The Finnish Border Guard. (2017). According to the website: https://www.raja.fi/projects/horizon2020 Ministry of the Interior.

Franke, U. and Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. Computers & security (pp. 18-31-46 DOI 10.1016/j.cose.2014.06.008

Glassman, M., & Kang, M. J. (2012). "Intelligence in the internet age: The emergence and evolution of open source intelligence (OSINT)", Computers in human behaviour, 28, pp 673–682.

Homeland Security. (2008) National response framework. Washington, DC: FEMA publications warehouse.

Hult, T. (2012) Public Protection and Disaster Relief services ICT-systems developing and integration. Thesis

Kaukanen, J. and Möttönen, M. (2010) Border guard headquarters - MARITIME SEARCH AND RESCUE MANUAL 2010. Ministry of the Interior.

Lemponen, I. (2012) Vedenalainen datasiirto – langallisten ja langattomien tiedonsiirtojärjestelmien nykytila ja kehitysnäkymät. http://www.doria.fi/bitstream/handle/10024/85020/Lemponen_IM.pdf?sequence=1

MARISA. (2018) "MARISA - Maritime Integrated Surveillance Awareness" [online], Marisa Project, https://www.marisaproject.eu/

The Maritime Search and Rescue Act, 1145U.S.C. (2005a).

Ministry of Defence. (2010) Security strategy for society, government resolution. Helsinki: Ministry of Defence

Morrow, J. and Odierno, R. (2012) Open source intelligence, ATP 2-22.9, army techniques publication. Washington: Headquarters, Department of the U.S. Army.

National Protection and Programs Directorate (NPPD). (2011) Enabling Distributed Security in Cyberspace - Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. United States: Department of Homeland Security.

Nurmi, P. (2015) OSINT - avointen lähteiden internet -tiedustelu. Helsinki: Aalto yliopisto.

ISI. (2017) Kingfisher – multi sensor, multilayer, maritime intelligence system. Retrieved from https://www.imagesatintl.com/solutions-services/maritime-situational-awareness/

Rajamäki, J. and Villemson, T. (2009). Designing emergency vehicle ICT integration solution. Proceedings of the 3rd International Conference on Communications and Information Technology, Athens, Greece. 83–90.

SIME. (2014) Mapping shipping intensity and routes in the Baltic Sea using historical AIS data. (No. 5). Göteborg: Havsmiljöinstitutet.

Simola, J. and Rajamäki, J. (2015) How a real time video solution can affect the level of preparedness in situation centres. Paper presented at the Second International Conference on Computer Science, Computer Engineering and Social Media (CSCESM), Lodz, Poland. https://doi.org/10.1109/CSCESM.2015.7331824

Simola, M., Aheristo, M., and Puustinen V. (2015) Vartiolaiva Turva tilannekuvan tuottajana- Rannikon Puolustaja

Trottier, D. (2015) "Open source intelligence, social media and law enforcement: Visions, constraints and critiques." European Journal of Cultural Studies, 18, pp 530–547.

Vetter, M. (2015) Open source intelligence techniques and the dark web Retrieved from www.itproportal.com/2015/10/30/open-source-intelligence-techniques-and-the-dark-web/

Wood, M. Graham. (2016) Social media intelligence, the wayward child of open source intelligence.

Yin, R. K. (2014) Case study research, design and methods (5th ed.). Thousand Oaks: Sage Publications.

III

EFFECTS OF CYBER DOMAIN IN CRISIS MANAGEMENT

by

Jussi Simola & Martti Lehto, 2019

Proceedings of the 18th European Conference on Cyber Warfare and Security
ECCWS 2019. 4.-5.2019. Coimbra, Portugal. p.365-371

http://urn.fi/URN:NBN:fi:jyu-202001071042

Effects of Cyber Domain in Crisis Management

Jussi Simola and Martti Lehto
University of Jyväskylä, Faculty of Information Technology, Finland
juhemisi@student.jyu.fi
martti.j.lehto@jyu.fi

Abstract: There is fundamental need in EU-level to develop common alarm procedures and emergency response models with preventive functions which work well from local to national level and from national to international level. European Public Protection and Disaster Relief (PPDR) services such as law enforcement, firefighting, emergency medical and disaster recovery services have recognized that lack of interoperability of technical systems limits cooperation between the PPDR authorities. Also, the military (MIL) and critical infrastructure protection (CIP) faces similar challenges. Recent major accidents have indicated that lack of human resources affects to disaster recovery. PPDR-actors cannot start operations, if there is a human factor preventing the flow of information. Preventing a domino effect after a disaster may be delayed. There is a need to understand how public safety authorities can act in a preventive manner so that a potential accident or offense can be prevented in advance. This paper´s goal is to find out main factors which affect to implementing of the next generation hybrid emergency response system for critical infrastructure protection. Early detection of any threat and rapid response to neutralize the threat may help to save human lives and vital functions before any disaster occurs. By comparing present emergency response processes to the next generation Smart hybrid emergency process model, it can be found effects and factors which prevent to implement this architecture. For example, legislation, organizational changes, lack of using cyber dimension and emergency procedures effects to combine different kind of PPDR -functions. Cyber dimension as a part of situational awareness raises its value for the continuity management. For traditional purposes, PPDR services are being seen as separate physical operational functions. This study proposes to solve the problems of development needs through technical, organizational and structural alternatives. The main issue regarding dividing reliable decision support information to decision-makers is related to at which point in chain-reaction a human action is more harmful than useful. It has been seen in earlier empirical studies that human activities may prevent to manage functions of essential emergency response procedures during a disaster. It´s necessary to create emergency response model, that will be functionally capable and modern combining cyber and physical elements in a right proportion.

Keywords: critical infrastructure protection, cyber-physical threats, emergency response, PPDR, continuity management

1. Introduction

European decision-makers like politicians have recognized, that it´s not enough to start emergency response procedures in traditional way at the scene of an accident or a catastrophe. Nowadays hybrid attacks against critical infrastructure are based on combination of different kind of threats. Human factors, technological communication problems and lack of interaction between different PPDR actors show challenges at the scene of an accident. It´s necessary to take into account these things before starting to build the next generations emergency response model.

Thanks to the rapid development of information systems, national legislation has also faced new challenges. On the other hand, practiced policy in Europe has been based on the image of the world that free movement between countries should be facilitated in Europe. The obstacles to free movement were reduced in the Schengen area until the terrorism that came with the Middle East refugee wave forced the European decision-makers to change the political lines. Terrorist attacks in the United States, Australia, France, Belgium, Germany, Sweden and Finland have changed the weighting of security issues.

The EU's internal and external border control have been intensified and the conditions for asylum applications have been revised. EU information systems projects have become increasingly multinational. Security has been perceived as a common EU affair, no longer a separate national task. The importance of legislation is emphasized when building common IT structures and platforms for information systems. National legislation may become an obstacle, especially in situations where other partner countries have implemented laws that support new IT solutions. The outline of the paper is as follows. After the introduction section 2 presents theoretical framework and central concepts of the paper. Section 3 handles research background, objectives and methods. Section 4 handles findings. Section 5 include discussion and section 6 conclusions.

2. Theoretical framework and literature review

In the future it´s not enough to develop separate technological solutions for critical infrastructure protecting. In EU-level there is a need to reach common situational picture when cross-boarding threat like cyberattack has occurred. Smart nations or European union needs cooperation between smart cities, because without smart cities smart nation cannot form. Thus smart information systems are being developed, it´s important that there is already infrastructure where to connect the system. Every smart city should be construct from a long-term view. Smart city needs urban built environment. This case study aims to find out those factors which affect to implementation of the Hybrid Emergency Response Model. There are separate situation centers, emergency response centers and organizations fighting against cyber threat´s, but there is no common emergency response model for all kind of hybrid-threats. The author of this research has innovated next generation emergency response model (Simola & Rajamäki, 2017). It´s necessary to research things that are setting barriers to implementation process.

The proposed cross-boarding intelligent emergency management system will provide next generation emergency response model for state decision-makers and PPDR-authorities. The model will combine different data sources, analyze them and produce predictive emergency actions before an alarming accident has occurred. Developed Hybrid Emergency Response -model is one kind of concept which can be expanded to the maritime surveillance environment.

2.1 Data protection regulation in EU countries

The EU General Data Protection Regulation (GDPR) harmonize data privacy laws across Europe. The law is technology neutral and applies to both automated and manual processing if the data is organized in accordance with pre-defined criteria (European Commission, 2016b). The purpose is to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. GDPR applies to all businesses offering goods and/or services to EU. That means that the organizations do not have to reside in the EU area or even in Europe. If you are holding private information about an EU citizen whom you provide services, GDPR applies (European Commission, 2016b).

Personal data cover e.g. name, address, email address, an internet protocol address, location data on a mobile phone and a cookie ID, the advertising identifier of your phone. In some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies. Directive presents mostly a continuation of earlier Data Protection Directives efforts (European Commission, 2016b).

Eu directive named the ePrivacy 2002/58 has been amended by Directive 2009/136, which introduces several changes, especially in what concerns cookies, that are now subject to prior consent. The directive does not apply to issues concerning criminal law and state security, public security and defense. The interception of data is covered by the new EU Data Retention Directive the purpose of which is to amend E-Privacy Directive (IBP, 2014)

The EU Data Protection Directive 2016/680 or Law Enforcement Directive regulates on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. This proposal applies cross-border and national processing of data by member states' competent authorities for the purpose of law enforcement. This comprise e.g. the prevention, investigation, detection and prosecution of criminal offences, the safeguarding and prevention of threats to public security (European Commission, 2016a).

2.2 Central concepts

2.2.1 Smart city, nation and infrastructure

Internet of Things connects systems, sensors and actuator instruments to the broader internet. IOT allows the things to communicate, exchange control data and other necessary information while executing applications towards machine goal (Electrical Technology, 2016). Fig. 1. Illustrates secure communication flows, electrical flows and different domains (Updated NIST Smart Grid Framework 3.0, Feb 2014).

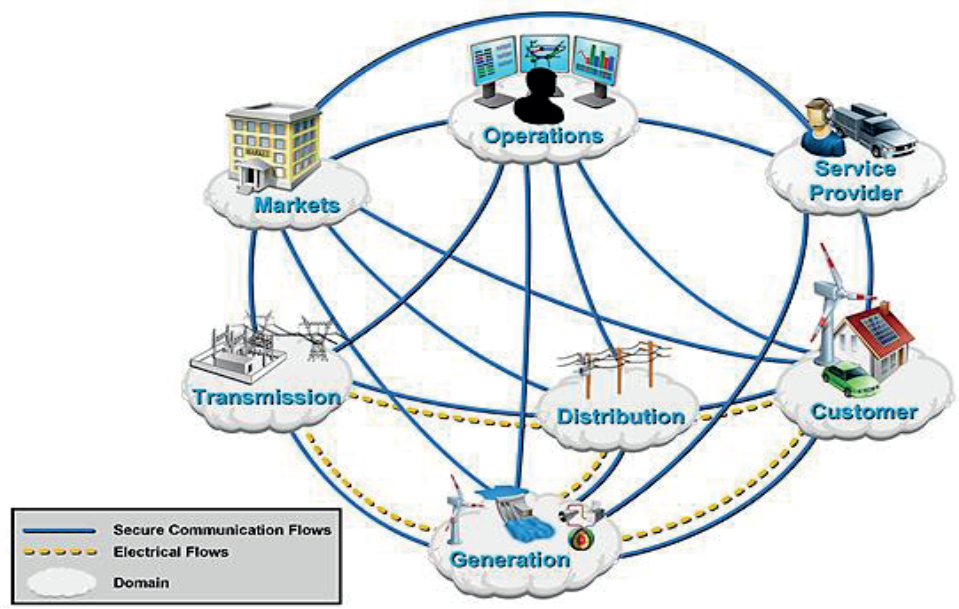


Figure 1: Interaction of actors in different smart grid domains

Cybersecurity risks should be addressed as organizations implement and maintain their smart grid systems (National Institute of Standards and Technology, 2014). A smart grid system may consist of information technology which is a discrete system of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. A smart grid system may also consist of operational technologies (OT) or industrial control systems (ICS) like SCADA systems, distributed control systems (DCS), and other control system configurations (CHONG & KUMAR, 2003; National Institute of Standards and Technology, 2014). Industrial Internet of Things (IIOT) collects data from connected devices (i.e., smart connected devices and machines) in the field or plant and then processes this data using sophisticated software and networking tools. The entire IIOT requires a collection of hardware, software, communications and networking technologies (Electrical Technology, 2016).

Critical Information Infrastructure means any physical or virtual information system that controls, process, transmits, receives or stores electronic information in any form including data, voice or video that is vital to the functioning of critical infrastructure. Critical infrastructure (CI) includes energy production, transmission and distribution networks, ICT systems, networks and services (including mass communication), financial services, transport and logistics, water supply, construction and maintenance of infrastructure, waste management in special circumstances. That smart network will integrate information and communication technologies with the power-delivery infrastructure (Ahokas, Guday, Lyytinen, & Rajamäki, 2010; Ministry of the Interior, 2016).

2.2.2 Sensors for monitoring, buildings, bridges and other structures

The development of more robust and advanced smart sensors could help provide valuable information about the health of various structures, including bridges, tunnels, buildings like shopping malls and water distribution systems. Sensors can provide valuable insight on the structural health and condition of bridges or buildings. In the future building can monitor the activities of all individuals inside the building. In the future buildings, bridges and shopping malls are part of smart city and smart grid (NIST, 2012).

2.2.3 Location based sensors

Retailers of malls may use indoor or/and outdoor navigation technologies to provide location-based services using mobile ‘‘push’’ notifications to provide advertisements. Technologies are currently available to not only locate a customer but are also be able to establish history of a path taken by a typical customer during the day (Kini & Suomi, 2018; Rachel, 2013). Advertisement networks are able to locate and custom-deliver an advertisement to customer with or without customer’s permission. With this technology it is possible to provide personalized marketing based on the consumer’s location. If mobile users give permission (opt-in) to the companies whose brand, products and services they like, companies send them personalized advertisements when they are shopping (Yiu, Jensen, Møller, & Lu, 2011).

2.2.4 Cyber infrastructure and cyber physical systems

The term cyber-physical systems (CPS) was coined by Helen Gill at the National Science Foundation in the U.S. to refer to the integration of computation with physical processes. In CPS, embedded computers and networks monitor and control the physical processes. CPS are enabling next generation of "smart systems" like advanced robotics, computer-controlled processes and real-time integrated systems (Lee & Seshia, 2015). Cyber Infrastructure Includes electronic information, communications systems, services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information or any combination of all of these elements. Processing includes the creation, access, modification and destruction of information. Storage includes paper, magnetic, electronic, and all other media types (National Institute of Standards and Technology, 2014). According to Franke and Brynielsson (2014), cyber situational awareness is a subset of situational awareness, i.e., cyber situational awareness is the part of situational awareness which concerns the "cyber" environment. Such situational awareness can be reached, e.g. by the use of data from IT sensors (intrusion detection systems, etc.) that can be fed to a data fusion process or be interpreted directly by the decision-maker (Franke & Brynielsson, 2014). Communications include sharing and distribution of information, e.g. computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) which are part of cyber infrastructure.

2.2.5 Cyber and hybrid threats

According to DHS & Office of Emergency Communications (2016) cyber threats can be illustrated in many ways. Potential Risks to emergency response system components may be formed from devices or equipment, network infrastructure and connections or data applications and services. In spear-phishing attack means that a criminal finds a webpage for his target organization that supplies contact information for the company. Using available details to make the message seem authentic, the criminal drafts an email to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator. The email asks the employee to log into a false page that requests the employee's username and password or click on a link that will download spyware or other malicious programming (Rouse, 2017). Data breaches mean data has stored on user device and it is accessed, manipulated or stolen. Users may download malicious software "malware" (e.g., botnets, viruses, spyware, trojans and rootkits). It is called "Man-in-the-middle attack" when wireless link between the user device and the tower may be susceptible and allow attackers to steal data or monitor conversations. In Denial-of-service (Dos) attack, criminals overload towers or other key network resources with requests for network access, damaging or destroying the operability of the targeted infrastructure and straining the capacity and resiliency of the network. Insider threats: Employees or other authorized personnel may produce insider threats when they use their access to steal, corrupt, or destroy data. In malicious applications attackers create applications that appear to be safe but allow them to steal, corrupt or modify data, eavesdrop on conversations, or acquire data on the location of victims and/or first responders (DHS & Office of Emergency Communications, 2016). Hybrid threat means for example combination of different kind of physical and cyber threats.

2.2.6 PPDR services

The term "Public Protection" is used to describe critical public services that have been created to provide primary law enforcement, firefighting, emergency medical and disaster recovery services for the citizens of the political subdivision of each country. The term Public Safety and Disaster Response, within certain regions, can also be construed as PPDR. The military (MIL) and critical infrastructure protection (CIP) are also included in the term (Baldini, 2010).

The Emergency Response Centre Administration provides emergency response center services throughout Finland. The duty of the Emergency Response Centre Administration is to receive emergency calls from all over the country for the rescue, police and social and health services; handle communications relating to the safety of people, property and the environment; and relay the information they receive to the appropriate assisting authorities or partners (National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO), 2016; The emergency response act, 2010).

2.2.7 Emergency response management information systems

Traditional Emergency Response System should consist of at least basic components like a database, data analysis capability, normative models and interfaces. E.g. personnel in Emergency Response Center use Emergency Response system. It is one kind of DSS system. Decision support systems are used to track key incidents and the progress of responding units, to optimize response activities and to act as a mechanism for queuing ongoing incidents (Ashish et al., 2007; Endsley, 1988; Endsley, 1995).

Situation center means the place where PPDR authorities make decisions to allocate resources to the right proportion. The words Command and Control individually and collectively mean different things to different communities (Alberts & Hayes, 2006). C2, situation center or Emergency Operation Room is a physical or virtual location designed to support emergency response, business continuity and crisis communications activities. PPDR authorities meets at the C2 -room to manage preparations for an impending event or manage the response to an ongoing incident. By gathering the decision makers together and supplying them with the most current information can be made better decisions (Ashish et al., 2007). In systems engineering, monitoring means a process within a distributed system for collecting and storing state data. A PPDR monitoring station is a workstation or place in which sensor information accumulates for end users who need it. Monitoring systems include information collection, analysis and provision for end-users, which is front-deployed knowledge. Government Situation Centre ensure that the state leaders and central government authorities are kept informed continuously (Ministry of defence, 2010).

2.2.8 Open Source Intelligence as a part of the HERM

OSINT is defined as the systematic collection, processing, analysis and production, classification and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security. It is any unclassified information, in any medium, that is generally available to the public, even if its distribution is limited or only available upon payment (Glassman & Kang, 2012; Morrow & Odierno, 2012; Nurmi, 2015).

3. Research background, objectives and methods

At present public safety authorities (PPDR) do not use cyber dimension in their daily routine at all. The problem is that public safety authorities have separate Cyber security organizations with own administrations. Organizations which have responsibilities for cyber security operations are separated from PPDR services. As a part of FICORA, The National Cyber Security Centre Finland (NSCS-FI) produce information of Cyber threats for stakeholders, but that data does not reach e.g. emergency response centers or situation centers. Separate organizational cyber security functions, methods and procedures prevent effective response for cyber physical threats. Combining Open Source Intelligence data (Morrow & Odierno, 2012) and traditional intelligence sources overall situational awareness arises. Hybrid threats need coordinated hybrid responses, therefore also a cyber situational picture is needed.

3.1 Method and process

3.1.1 Case study research strategy

Empirical approach helps to understand PPDR authorities´ entity. Choosing a case study research strategy enables investigation of interaction between the different factors. The multimethodological approach consists of four case study research strategies: theory building, experimentation, observation and systems development (Nunamaker, Minder Chen, & Purdin, 1991). Yin (2014) identifies five components of research design for case studies: (1) the questions of the study; (2) its propositions, if any; (3) its unit(s) of analysis; (4) the logic linking the data to the propositions; and (5) the criteria for interpreting the findings. This case study is carried out with the guidance of Yin (2014). This research concentrates in sources of scientific publications, collected articles and literary material.

3.1.2 Analyzing vulnerabilities

We can divide research-area in four sections; local, regional, national and European level. Local PPDR-area consists of one city or municipalities, regional area is wider area including organizations like regional administration with PPDR-authorities, cities and municipalities. The focus of the research is on the protection of

critical infrastructure at local and regional level and how the current EMS system could be developed to be able to respond to the future challenges of cross-border cooperation between PPDR authorities. This is an important question, because there is a common need to develop interoperability between information systems within European Union member countries. Firstly, next generation emergency response system should work in lowest local level before it can be connected to the next level.

We have used combination of different methodologies to find out those factors which affects to introduction of the next generation emergency response model. The Framework by National Institute of Standards and Technology focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework will help an organization to understand, align and prioritize its cybersecurity activities with its mission requirements, risk tolerances and resources. The Tiers or levels provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives (DHS & Office of Emergency Communications, 2016; National Institute of Standards and Technology, 2018).

A prescriptive metric known as Technology Readiness Level (TRL) has being used mainly by NASA, the DoD, the DoE and the Department of Homeland Security to address the readiness of systems under development. TRLs have been adapted for biomedical systems, modeling and simulation technologies, learning systems and software intensive systems, among others. Additional readiness levels (RLs) were developed to meet specific needs. Proliferation does emerge as a problem when the tendency is to add new undefined RLs that did not have the quality control in their construction as the original (Perseus, 2013).

To address integration, another metric called Integration Readiness Level (IRL) was introduced by the Systems Development & Maturity Laboratory (SysDML) at Stevens Institute of Technology. The introduction of an IRL to the assessment process not only provides a check as to where a technology is on an integration readiness scale but also presents a direction for improving integration with other technologies. Combining both TRL and IRL scales it is possible to form a knowledge base on the technological maturity level of the emergency response services infrastructure. Tier levels 1-3 are used instead of 1-9 in this research. Two emergency response systems were compared with each other; present system and the next generation hybrid emergency response model.

Three main categories have been chosen to classifications:

- Legislation concerning the smart hybrid model
- Technological maturity Level
- Readiness Level of organizational and political view

The approach of the research is at the local and regional level and it includes the intelligent city area with its authorities and operational functions of situation centers and emergency response information system.

4. Results

4.1 Emergency response model for critical infrastructure protection

The highest state decision-makers, such as members of the Finnish government or highest public safety officers must understand digital entity of the environment where citizens are living. As figure 2 illustrates, formation of cyber-physical threats is gathered from different sources and separate organizations handle those threats. There is no common preventive cyber functionalities or connection between emergency response administration and National Cyber Security Centre Finland which acts under the Finnish Communications Regulatory Authority.

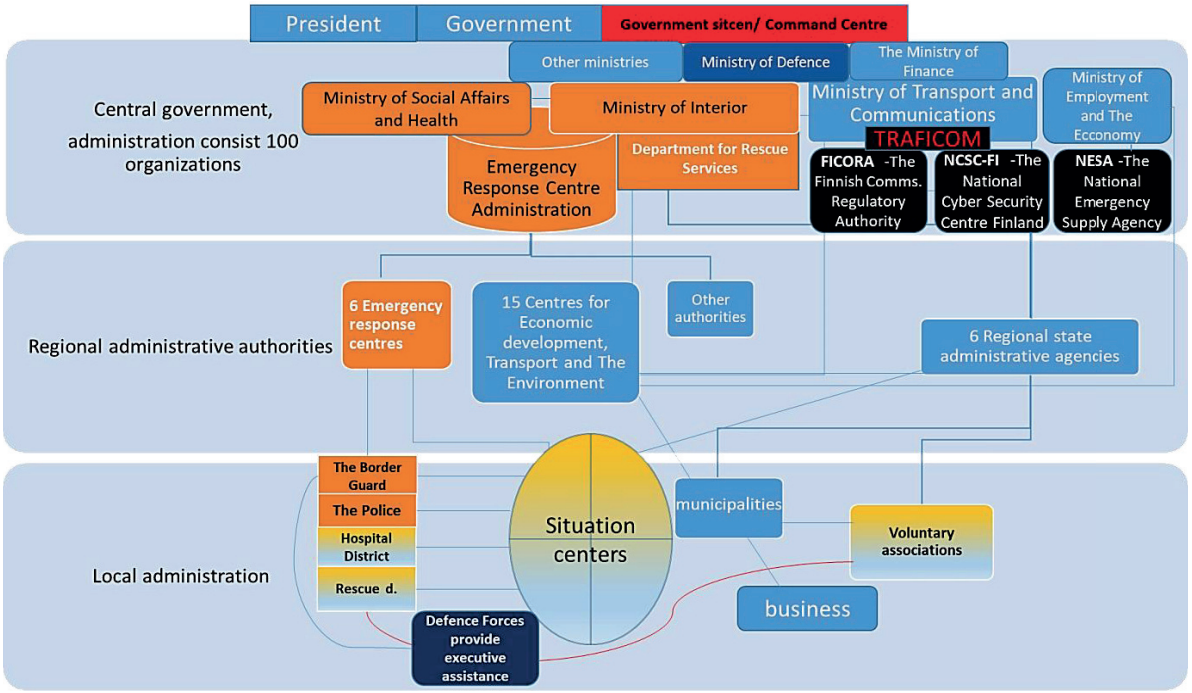


Figure 2: Organizations responsibilities of cyber security

Hybrid emergency response model as a part of smart society and smart city will create a secure framework with efficient procedure to identify and assess national and cross-boarding threats in critical infrastructure. It will provide efficient decision support solution for decision-makers and PPDR authorities how to protect critical infrastructure, but there are fundamental factors which prevent to start implementation of the system. When present national and European development concerning developing next generation emergency response model are taken into consideration the difference of new and the old model illustrated as fig.3.

Maturity level	**Low**	**Med**	**High**	
	1	2	3	
Low (red 1) presents that the maturity level of the system does not correspond the research area. Medium (green 2) presents that the maturity level is average. High (blue 3) presents that the maturity level of the system is ready for the implementation.				
Research areas	**Present system**		**Next gen. HERM syst**	
European legislation	1		2	
Legislation concerning technology	3		1	
Legislation concerning privacy issues	3		2	
Legislation concerning the smart hybrid model	sum	7		5
Technological maturity	2		3	
Smart city maturity	1		3	
Maturity of organizational Integration	1		2	
Opportunities to use smart devices	1		3	
Opportunities to integrate sensor tech.	2		3	
Maturity to integrate it-systems	1		3	
Operational reliability	2		2	
Technological maturity Level	sum	10		19
Organizations maturity level	3		1	
The political readiness at national level	3		1	
European policy	1		2	
Readiness Level of organizational and political view	sum	7		4
Total	24		28	

Figure 3: Maturity level of emergency response systems

Firstly, there are organizational factors which prevent to implement new system. Those factors are closely related to legislation, because there is PPDR administration like emergency services which act under the municipalities. Emergency Response Centre acts under Ministry of Interior. On the other Coast guard acts under the Ministry of Interior, but Defense forces act under The Ministry of Defence. There is a lot to do that the operating environment would be favorable to the next generation emergency response system. In Finland the legislation does not give permission for law enforcement to trace citizens digital behavior in real time. Tools like OSINT, Geo-targeting, Geo-fencing with Wi-Fi, Cell Towers and Beacons create a privacy-restricting advertisement and surveillance circuit that aims to trace consumer behavior. These tools are possible to use only with new Hybrid Emergency Response model. Therefore, maturity level for using mobile technologies is so low.

5. Discussion

In democratic society, it must be taken into consideration that privacy concerns and public safety functions both effect to our quality of life. No one wants to live in an environment where citizen´s rights and responsibilities are unclearly defined. Important things for us, such as the data privacy issues, can be more relieved on the grounds that the "common good" requires it. How can we then define the common good? This issue has been controversial in Europe. Determining the public interest or limiting the need to protect society has sometimes caused difficulties. The problem is related to situations where protected legal intresses are incompatible. Government agents, utility executives, policymakers and technology providers must agree about a common goal and take actions to accelerate the process towards final deployment, legal and organizational barriers have to be removed. Given the scale of the effort required and the enormity of the challenges ahead, collaboration among different sectors is essential and should be developed through various channels in order to ensure and accelerate the success of the future smart control centers. In a society where the limits of public and private commercial players have become obscured, the risks are also increasing. Citizens should be able to trust decision-makers, authorities, and society that they do not have to constantly think about what kind of digital footprints they are left behind in any department store control unit. As a single datum, separate information of human life is not significant, but if data is combined from the different sources, the position of a citizen as a manager of his or her own life may change significantly.

6. Conclusions

The new intelligence legislation package proposed by the Finnish government would include provisions on the principles of intelligence activities. If the legislation package will be approved, it is expected to enhance the ability of the PPDR authorities to respond on major national and international hybrid threats, because it also allows wider use of new decision support system technologies. It requires clarification of common rules. In other words, in a public place, e.g. in shopping centers privacy protection should be facilitated if citizen accept common rules which have been created in the form of legislation.

People have been irritated by the fact that people's behavior has been collected much more widely, what has been told and uses that are not known. Therefore, it might be important to look at the big picture of the protection of critical infrastructure. What kind of elements can be included in the framework which protect the vital functions of society? When all the things we do leave some data to tracking systems, people have the right to know what information is collected and for what purpose it has been collected. Perhaps even more important thing is to know who is the holder of the personal data and what is the storage time of the data.

The next generation hybrid model will integrate existing surveillance systems and networks with new ones and it based on active operations and automated functions. There is a need to strengthen the entire intelligence ecosystem in maritime and inland. There is also a need in command and control functions to design a combination of a new kind of hybrid sensor technology that uses location based solutions and OSINT tool in order to detect threats in advance because common cyber situational picture is needed. Location based intelligence is an applicable emergency response tool for public safety authorities in shopping malls and in city areas. The presented hybrid model will offer an updated emergency response management model to PPDR services. Effective cooperation between public safety authorities needs a common technology for all authorities and organizational cooperation requires a common infrastructure and clearer and faster connections.

A dynamic cyber-physical infrastructure is needed in order to respond to a rapidly evolving alert situation. The local and state level PPDR -atmosphere can no longer be separated in the traditional sense. Threats have

changed into combinations of threat types and, as a consequence, public safety organizations like the Police or Finnish Border Guard must be able to prevent new kinds of hybrid threats and respond to them. Improving the flow of information between the public sector and citizens, including volunteer associations, is also a relevant part of this framework. It must be possible to prevent and respond faster to the realization of threats. Municipal actors relying on municipal technical resources is not sustainable because cooperation between the Police, Finnish Border Guard and emergency services has developed. A modelling platform for a smart emergency response model can lead to important new results. The cyber domain can be used as a powerful dimension to enhance data fusion to more accurate overall situational awareness. By processing raw data on anomalous behavior in advance, PPDR services can use smart emergency response functions before any threats have occurred.

References

Ahokas, J., Guday, T., Lyytinen, T., & Rajamäki, J. (2010). Secure and reliable communications for SCADA systems. Paper presented at the *International Journal of Computers and Communications,6*(3)

Alberts, D. S., & Hayes, R. E. (2006). *UNDERSTANDING COMMAND AND CONTROL. DoD command and control research program.* Center for Advanced Concepts and Technology (ACT).

Ashish, N., Kalashnikov, D. V., Mehrotra, S., Venkatasubramanian, N., Eguchi, R., Hegde, R., & Smyth, P. (2007). Situational awareness technologies for disaster response. In H. Chen, E. Reid, J. Sinai, A. Silke & B. Ganoz (Eds.), *Terrorism informatics: Knowledge management and data mining for homeland security*. Springer.

Baldini, G. (2010). *Report of the workshop on "interoperable communications for safety and security" with recommendations for security research.* (No. JRC60381). Publications of Office of the European Union. doi:10.2788/19075

CHONG, C., & KUMAR, S. (2003). Sensor networks: Evolution, opportunities and challenges. Paper presented at the *IEEE, 91*(8) 1247-1256.

DHS, & Office of Emergency Communications. (2016). *Cyber risks to next generation 911.* Department of Homeland Security.

Electrical Technology. (2016). Internet of things (IOT) and its applications in electrical power industry. Retrieved from http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html

The emergency response act 692/2010, (2010).

Endsley, M. R. (1988). (1988). Design and evaluation for situation awareness enhancement. Paper presented at the *Proceedings of the Human Factors Society 32nd Annual Meeting,* 97-101.

Endsley, M. R. (1995). Toward a theory of situation awareness. human factors. (37), 32-64.

EU data protection directive 2016/680, Directive U.S.C. (2016a).

General data protection regulation (EU) 2016/679, Regulation U.S.C. (2016b).

Franke, U., & Brynielsson, J. (2014). *Cyber situational awareness: A systematic review of the literature*. *Computers & security* (pp. 18-31-46) doi: 10.1016/j.cose.2014.06.008

Glassman, M., & Kang, M.,Ju. (2012). Computers in human behavior; intelligence in the internet age: The emergence and evolution of open source intelligence (OSINT).*28*(2), 673-682.

IBP. (2014). *European union cyber security strategy and programs handbook. strategic information and regulations.* Washington DC, USA: International Business Publications.

Kini, R., B, & Suomi, R. (2018). Changing attitudes toward location-based advertising in the USA and Finland, journal of computer information systems.*58* doi:10.1080/08874417.2016.1192519

Lee, E., Ashford, & Seshia, S., Arunkumar. (2015). *Introduction to embedded systems, A cyber-physical systems approach* (2nd ed.) Lee & Seshia.

Ministry of Defence. (2010). *Security strategy for society, government resolution*. Helsinki: Ministry of Defence;

Ministry of the Interior. (2016). *National risk assessment 2015*. Helsinki: Ministry of the Interior.

Morrow, J., & Odierno, R. (2012). *Open-source intelligence, ATP 2-22.9, army techniques publication.* (). Washington: Headquarters, Department of the U.S. Army.

National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO). (2016). *NENA/APCO next generation 9-1-1 public safety answering point requirements.* (). USA: NENA and APCO. Retrieved from https://www.nena.org/resource/resmgr/Standards/NENA-APCO-REQ-001.1.1-2016_N.pdf.

National Institute of Standards and Technology. (2014). *Guidelines for smart grid cybersecurity national institute of standards and technology, volume 1 - smart grid cybersecurity strategy, architecture, and high-level requirements.* U.S. Department of Commerce. doi:10.6028/NIST.IR.7628r1

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity.* (No.1.1). NIST.

NIST. (2012). *Cyber-physical systems: Situation analysis of current trends, technologies and challenges.* (). Maryland, USA: National Institute of Standards and Technology.

Nunamaker, J., Minder Chen, J. R., & Purdin, T. (1991). Systems development in information system research. (3), 89-106.

Nurmi, P. (2015). *OSINT - avointen lähteiden internet-tiedustelu*. Helsinki: Aalto yliopisto.

Perseus. (2013). *Protection of European seas and borders through the intelligent use of surveillance D26.12 working document: Assessment report.*

Rachel, M. (2013). MIT Technology review. Retrieved from https://www.technologyreview.com/s/510491/every-step-you-take-tracked-automatically/

Rouse, M. (2017). Spear phishing. Retrieved from https://searchsecurity.techtarget.com/definition/spear-phishing

Simola, J., & Rajamäki, J. (2017). Hybrid Emergency Response Model: Improving Cyber Situational Awareness. Paper presented at the *16th European Conference on Cyber Warfare and Security,* University, College, Dublin, Ireland. 442-451.

Yin, R. K. (2014). *Case study research, design and methods* (5th ed.). Thousand Oaks: Sage Publications.

Yiu, M., L., Jensen, C. S., Møller, J., & Lu, H. (2011). Design and analysis of a ranking approach to private location-based services. *ACM Transactions on Database Systems, 36*(2), 10:1-10:42. doi:10.1145/1966385.1966388

IV

PRIVACY ISSUES AND CRITICAL INFRASTRUCTURE PROTECTION

by

Jussi Simola, 2019

Chapter in the book titled Emerging Cyber Threats and Cognitive Vulnerabilities

https://doi.org/10.1016/B978-0-12-816203-3.00010-1

CHAPTER

Privacy issues and critical infrastructure protection

Jussi Simola
Department of Information Technology, University of Jyväskylä, Finland

Emerging Cyber Threats and Cognitive Vulnerabilities
https://doi.org/10.1016/B978-0-12-816203-3.00010-1

Introduction

European Public Protection and Disaster Relief (PPDR) services such as law enforcement, firefighting, emergency medical and disaster recovery services have recognized that the lack of interoperability of technical systems limit the cooperation between the PPDR authorities. The military (MIL) and critical infrastructure protection (CIP) face similar challenges.

Cyberthreats have increased in spite of formal integration in Europe and the world. Therefore, authorities need to respond to growing challenges. As major terror attacks, hybrid warfare and major accidents, for example in Belgium, France, Ukraine and the United States have shown, preparation for different kind of threats is challenging. Recent major accidents have indicated that lack of human resources affects disaster recovery.

Due to the terrorist attacks that have occurred, public safety authorities are convinced that network traffic control is a good way to proactively prevent acts that threaten peace of society, but it is only one way to protect the citizens or control the situation.

There is an issue concerning privacy because most mobile user/end-users of web-based services or applications do not know where and to whom personal information is transmitted and how social media behaviour is analyzed for different purposes. It has been seen that data, which are collected from social media, are tradable goods that may violate an individual's privacy.

In the market economy, customer profiling or tracking is seen only from the point of view of data exploitation in Internet marketing. Marketing people and advertisers try to focus on services and products more efficiently for the right target audience. Location-based services rely on a combination of technologies to pinpoint the location of a user with contextual data to provide more value to a mobile user. For example,

Geo-targeting or Geo-fencing with Wi-Fi, cell towers and beacons create a privacy-restricting advertisement atmosphere that aims to influence consumer behaviour.

The main purpose of this chapter was to find local- and state-level factors concerning privacy issues, which affect the utilization of proposed smart hybrid emergency response model (Simola & Rajamäki, 2017). Privacy issues with ethical aspects are an important part of continuity management because the government cannot accept and produce services that are illegal.

The rest of this chapter is divided as follows. Section 2 handles the overview of legislation concerning privacy issues in the United States and Europe. Section 3 proposes central concepts and framework of this article. Sections 4 handles the organizational and management perspective of situational awareness. Section 5 presents location-based technologies. Section 6 handles the research process of this study. Section 7 presents findings. Section 8 presents discussion about usage of the proposed Hybrid Emergency Response Model. Section 9 handles expectations of implementation when the proposed model is applied on CI.

Legislation concerning privacy issues

European Data Protection Reform (EDPR) partly harmonizes data protection regulation in European Union (EU) countries. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. GDPR applies to all businesses offering goods and/or services to the EU. That means that the organizations do not have to reside in the EU area or even in Europe; if you are holding private information about an EU citizen whom you provide services, GDPR applies (European Commission, 2016a). The regulation introduces stronger citizens' rights as new transparency requirements. It strengthens the rights of information, access and the right to be forgotten. Regulation gives all data protection authorities the right to impose fines up to EUR 20 million or 4% of the worldwide annual turnover on companies (European Commission, 2016a).

The EU's new GDPR regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU. For this purpose, personal data are comprised of any information that

relates to an identified or identifiable living individual. Different pieces of information, which is collected together and can lead to the identification of a particular person, also constitute personal data. Personal data that have been encrypted or pseudonymized but can be used to re-identify a person remains personal data and fall within the scope of the law. Personal data that have been rendered anonymous in such a way that the individual is not or no longer identifiable are no longer considered personal data. For data to be truly anonymized the anonymization must be irreversible (European Commission, 2016a).

The GDPR protects personal data regardless of the technology used for processing that data. The law is technology neutral and applies to both automated and manual processing if the data are organized in accordance with pre-defined criteria (European Commission, 2016a). It also does not matter if the data are stored in an IT system through video surveillance or on paper. In all these cases personal data are subject to the protection requirements set out in the GDPR.

Personal data consist of, for example, name, address, email address, an Internet protocol address, location data on a mobile phone and a cookie ID, and the advertising identifier of your phone. In some cases, there is a specific sectoral legislation regulating, for instance, the use of location data or the use of cookies. Directive presents mostly a continuation of earlier Data Protection Directive efforts (European Commission, 2016a).

EU directive named the ePrivacy 2002/58 (European Commission, 2002) deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies. This directive has been amended by Directive 2009/136, which introduces several changes, especially in what concerns cookies, that are now subject to prior consent. The ePrivacy directive presents mostly a continuation to earlier Data Protection Directive (European Commission, 2002).

The directive does not apply to Titles V and VI (second and third pillars constituting the EU). Also, it does not apply to issues concerning criminal law and state security, public security and defence. The interception of data is covered by the new EU Data Retention Directive, the purpose of which is to amend ePrivacy Directive (IBP, 2014). In the future, Regulation on Privacy and Electronic Communications will repeal the ePrivacy Directive 2002/58/EC (European Commission, 2017).

The EU Data Protection Directive 2016/680 or Law Enforcement Directive regulate the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of

the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. This proposal applies cross-border and national processing of data by member states' competent authorities for the purpose of law enforcement. This comprises, for example the prevention, investigation, detection and prosecution of criminal offences and the safeguarding and prevention of threats to public security (European Commission, 2016b).

Information exchange

The exchange of information between the EU and the United States has been regulated, among other things, as follows: The European Commission and the US government reached a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes named the EU−US Privacy Shield. The European Commission adopted the EU−US Privacy Shield on July 2016 (European Commission, 2016c).

The framework protects the fundamental rights of anyone in the EU whose personal data are transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers.

The EU−US Privacy Shield is based on the principles like obligations on companies which handle data. (a) The US Department of Commerce will conduct regular updates and reviews of participating companies to ensure that companies follow the rules they submitted themselves to. (b) Clear safeguards and transparency obligations on US government access: The United States has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear oversight mechanisms. (c) Effective protection of individual rights: citizens who think that collected data have been misused under the Privacy Shield scheme will benefit from several accessible dispute resolution mechanisms. It is possible for a company to resolve the complaint by itself or give it to the alternative dispute resolution (ADR) to be resolved for free. Citizens can also go to their national data protection authorities, who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved. The Ombudsperson mechanism means that an independent senior official within the US Department of State will ensure that complaints are properly investigated and addressed in a timely manner (European Commission, 2016c).

All of this regulation reflects the need for privacy protection in the Western world.

Central concepts

Situational awareness

According to Endsley (1988), a general definition of situational awareness (SA) is 'the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future'. From a technical viewpoint, SA comes down to compiling, processing and fusing data, and such data processing includes the need to be able to assess data fragments as well as fused information and provide a rational estimate of its information quality (Franke & Brynielsson, 2014). The cognitive side of SA concerns the human capacity of being able to comprehend the technical implications and draw conclusions in order to come up with informed decisions (Franke & Brynielsson, 2014). According to Endsley (1988, 2015) humans are not as good at processing large volumes of data, quickly and consistently, nor of sustaining attention for long periods of time. The level of autonomy increases as the capability of the system increases for performing various components of any given function. Flexible autonomy should provide smooth, simple, seamless transition of functions between a human and the system (Endsley, 2015).

Cyber situational awareness

According to Franke and Brynielsson (2014), cyber SA is a subset of SA, that is cyber SA is the part of SA that concerns the 'cyber' environment. Such SA can be reached, for example, by the use of data from IT sensors (intrusion detection systems, etc.) that can be fed to a data fusion process or be interpreted directly by the decision-maker (Franke & Brynielsson, 2014). SA is a prerequisite for CPS to be resilient. According to Franke and Brynielsson (2014), cyber SA cannot be treated in isolation, but it is intertwined with and a part of the overall SA. Cyber SA concerns awareness regarding cyber issues but these need to be combined with other information to obtain full understanding regarding the current situation.

Public protection and disaster relief functions

The term PPDR or public safety organization implies that those groups are responsible for the prevention of and protection from events that could endanger the safety of the general public (Baldini, 2010). According to Baldini (2010), the main public safety functions include law enforcement, emergency medical services, border security, protection of the

environment, firefighting, search and rescue (SAR) and crisis management. PPDR is used to describe critical public services that have been created to provide primary law enforcement, firefighting, emergency medical services and disaster recovery services for the citizens of the political sub-division of each country. These individuals help to ensure the protection and preservation of life and property. Public safety organizations are responsible for the prevention of and protection from events that could endanger the safety of the general public. Such events could be natural or man-made.

One major challenge in defining a classification of public safety organizations at the European level is that, due to the non-homogenous historical development of public safety, similar organizations have different roles in different countries (Baldini, 2010).

Structural and organizational changes in Finnish PPDR

Structural changes within the public sector, such as the regional administration reform, the Emergency Response Centre (ERC) reform and so-called social welfare and health-care reform have influenced the public sector employee's work processes over the past 10 years. In addition, technological development has occurred rapidly (Hanni, 2013). Changes in PPDR organizations due to legislation have developed a need to create special operational working methods (Aine et al., 2011). The Finnish Security Intelligence Service (Supo) is an operational security authority engaged in close cooperation with international security and intelligence services. Supo moved directly under the Ministry of the Interior in 2016. Earlier the Finnish Secure Intelligence Service operated under the National Police Board (The Finnish Security Intelligence Service, 2015).

Command and control system

A command centre is any place that is used to provide centralized command for some purpose. An Incident Command Centre would be located at or near an incident to provide localized on-scene command and support of the Incident Commander. Mobile command centres may be used to enhance emergency preparedness and back up fixed command centres. Command centres may include emergency operations centres (EOCs) or transportation management centres (TMCs) as well.

Supervisory Control and Data Acquisition (SCADA) systems are basically process control systems (PCSs) that are used for monitoring, gathering and analyzing real-time environmental data from a simple office building or a complex nuclear power plant. PCSs are designed to automate electronic systems based on a predetermined set of conditions, such as traffic control or power grid management (Gervasi, 2010).

According to Gervasi (2010), SCADA systems can be described with the following components: operating equipment which can include but are not limited to valves, pumps and conveyors controlled by energizing actuators or relays. Local processors communicate with site's instruments and operating equipment including programmable logic controller (PLC), remote terminal unit (RTU), intelligent electronic device (IED) and process automation controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment. SCADA also consists of instruments in the field or in a facility with or which sense conditions such as power level, flow rate or pressure. Short-range communications mean wireless or short cable connections between local processors, instruments and operating equipment. Long-range communications between local processors and host computers cover a wide area using methods such as satellite, microwave, frame relay and cellular packet data. Host computers act as the central point of monitoring and control. The host computer is where a human operator can supervise the process, as well as receive alarms, review data and exercise control. The system may consist of automated or semi-automated processes. A networked control system (NCS) is a control system where the control loops are closed through a communication network. The defining feature of an NCS is that control and feedback signals are exchanged among the system's components in the form of information packages through a network (McLarty and Ridge, 2014; Rosslin & Tai-hoon, 2010).

Integration of safety functions

Decision support engine (DSE) is a facilitator intended to help authorities and other decision-makers that compiles key information from raw data using system rules and knowledge. It captures data from different sensors, for example surveillance cameras (Ahmed et al., 2012). Face detection camera (FDC) is also a decision support engine itself. Data processing for event detection follows next in order to identify events in current surveillance context (NEC Corporation, 2016). To understand the current surveillance state depends on the output of combined event detection units.

Distributed systems intercommunication protocol

Distributed systems intercommunication protocol (DSiP) forms multiple simultaneous communication channels between the remote end and the control room: if one communication channel is down, other channels will continue operating. DSiP makes communication reliable and unbreakable by using various physical communication methods in parallel. Applications, equipment and devices can communicate over a single unbreakable data channel. Satellite, TETRA, 2G/3G/4G, VHF-radios and

other technologies can be used simultaneously. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication (Ahokas, Guday, Lyytinen, & Rajamäki, 2010).

Critical infrastructure protection

Critical Information Infrastructure means any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice or video that is vital to the functioning of CI. CI includes energy production, transmission and distribution networks, ICT systems, networks and services (including mass communication), financial services, transport and logistics, water supply, construction and maintenance of infrastructure, and waste management in special circumstances. The smart network will integrate information and communication technologies with the power-delivery infrastructure (Ahokas et al., 2010; Ministry of the Interior, 2016).

Examples of cyberattacks

Cyber threats include denial of service (DoS), unauthorized vulnerability probes, botnet command and control, data exfiltration, data destruction and physical destruction via alternation of critical software/data. These attacks can be initiated and maintained by a mixture of malware, social engineering or highly sophisticated advanced persistent threats (APTs) that are targeted and continue for long periods of time. Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications (National Institute of Standards and Technology, 2014).

According to the National Institute of Standards and Technology (2014) cyber-physical attacks can be classified into three broad sections:

- Physical attacks informed by cyber
  The use of information gathered by cyber means that an attacker is allowed to plan and execute an improved or enhanced physical attack. For example, if an enemy has decided to destroy components within a substation though they are not sure which substation or components would have the greatest impact. They could access confidential information or aggregate unprotected information by cyber and they could then physically attack that specific substation and lines.
- Cyberattacks enhancing physical attacks
  An enemy uses cyber means to improve the impacts of a physical attack by either making the attack more successful (e.g. greater

consequences) or interfering with restoration efforts (thereby increasing the duration of the attack). Inadvertent actions could also cause such an attack. One example is an enemy tampering with the integrity of protective relay settings prior to a physical attack on power lines. Although the original settings were designed to contain the effects of a failure, the tampered settings allow the failure to cascade into impacts on a wider segment of the grid.

- Use of a cyber system to cause physical harm

  An enemy uses a cyber system that controls physical equipment in such a manner to cause physical damage. An example of this is the burner management system for a natural gas generator. In this case, an enemy or a careless operator could attempt to turn on the natural gas inflow without an ignition source present. As the burner unit fills with natural gas, the enemy could turn on the ignition source, potentially causing an explosion.

  Good cyber, physical and operational security planning and implementations can minimize the impacts of cyber-physical attacks. Defensive measures that can be used to minimize the likelihood of successful cyberattacks and physical attacks will also work to minimize the impacts of a cyber-physical attack. The attacker can also be the state. This type of cyberattacker is politically motivated and may try to use several tools to affect the state's vital functions.

Intelligence solutions for public safety organizations

OSINT is defined as the systematic collection, processing, analysis and production, classification and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security. It is any unclassified information, in any medium, that is generally available to the public, even if its distribution is limited or only available upon payment (Glassman and Kang, 2012; Morrow & Odierno, 2012; Nurmi, 2015).

Most information has geospatial dimensions. Examples of geospatial open source include maps, airborne imagery, atlases, gazetteers, port plans, gravity data, aeronautical data, navigation data, geodetic data, human terrain data (cultural and economic), environmental data, commercial imagery, LIDAR, hyper and multi-spectral data, geo-names and features, urban terrain, vertical obstruction data, boundary marker data, geospatial mashups, spatial databases and web services. Most of the geospatial data mentioned above are integrated, analyzed and syndicated using geospatial software such as a geographic information system (GIS) (Morrow & Odierno, 2012; Nurmi, 2015; Trottier, 2015; Vetter, 2015; Wood, 2016).

Social Media Intelligence (SOCMINT) identifies social media content in particular as a challenge and opportunity for open-source investigations (Trottier, 2015). Big data includes processes of analysis, capture, research,

sharing, storage, visualization and safety of information. Associated with OSINT, Big Data is the ability to map standards of behaviour and tendencies (Dos Passos, 2016). The availability of worldwide satellite photography, often of high resolution, on the web (e.g. Google Earth Pro) has expanded open-source capabilities into areas formerly available only to major intelligence services.

Emergency communications in Europe

The Emergency Response Centre Administration provides emergency response centre services throughout Finland. The duty of the Emergency Response Centre Administration is to receive emergency calls from all over the country for the rescue, police and social and health services; handle communications relating to the safety of people, property and the environment and relay the information they receive to the appropriate assisting authorities or partners.

European authorities communicate with each other in VIRVE network. There is a need to create a new trusted network with a wide bandwidth. The transmission capacity is often limited in an overload situation. The needs of data transmission must be classified. Classification can be used for the benefit of message traffic prioritizing the entire transmission chain. Therefore, it is important to reduce unnecessary data communications between the authorities (Simola & Rajamäki, 2016).

Emergency communications in the United States

Importance of enhancing common operational picture between public safety actors has been noticed also in the United States. The need to transmit live video but also different kinds of sensor data from the scene of an accident has become a main area for development of information systems. The National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) recognize the fundamental need to update the North American 9-1-1 system and are addressing the challenge with a system design called "Next Generation 9-1-1". i3 is the NENA architecture for a system of 9-1-1 services, functional elements and databases that run on an Emergency Service IP Network ESInet. The 9-1-1 centre of the future with First Responder Network Authority (FirstNet) systems will receive incoming data calls from the machines and sensor systems including automatic crash notification (ACN), break-in alarms and body health monitors. Use of both systems ensures multi-media capabilities throughout the entire call process (National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO), 2016; National Public Safety Telecommunications Council, 2015).

The US Congress established an independent government authority with a mandate to provide specialized communication services for public safety called FirstNet. It will be connected to the state-level ESinet. The service package consists of NG9-1-1 emergency services, Commercial Mobile Alert System. The dispatcher can utilize a combination of computer-assisted dispatch (CAD) and radio resources to relay information to the appropriate responder resources. FirstNet capable NG9-1-1−PSAP system would be used to relay the appropriate data. For example, processed video or picture material can be transmitted to the first responders via the FirstNet broadband network. In this way NG9-1-1 and FirstNet systems are highly complementary and both are required to ensure a seamless flow of information from the public, to the PSAP and to the responders. Use of both systems ensures multi-media capabilities throughout the entire call process (National Public Safety Telecommunications Council, 2015).

A smart grid system and internet of things

Internet of Things (IoT) connects systems, sensors and actuator instruments to the broader internet. IoT allows the things to communicate, exchange control data and other necessary information while executing applications towards the machine goal (Electrical Technology, 2016).

The idea of IoT was developed in parallel to Wireless Sensor Networks (WSN). Sensors are now everywhere. In our vehicles, in our smartphones, in factories controlling CO_2 emissions and even in the ground monitoring soil conditions in vineyards. A WSN can generally be described as a network of nodes that cooperatively sense and may control the environment, enabling interaction between persons or computers and the surrounding environment. The development of WSNs was inspired by MIL applications, notably surveillance in conflict zones (Bröring et al., 2011).

IoT is an emerging paradigm of Internet-connected things that allow the physical objects or things to connect, interact and communicate with one another similar to the way humans talk through the web in today's environment. It connects systems, sensors and actuator instruments to the broader Internet.

IoT allows things to communicate, exchange control data and other necessary information while executing applications towards machine goal. The IoT has also impacted the industrial sector, especially for industrial automation systems in which Internet infrastructure makes extensive access to sensors, controls and actuators, with a goal of increasing efficiency (Electrical Technology, 2016).

Cybersecurity risks should be addressed as organizations implement and maintain their smart grid systems. According to the National Institute

of Standards and Technology (2014), digital two-way communications between consumers and electric power companies, the smart grid system provides the most efficient electric network operations based on the received consumer's information.

A smart grid system may consist of IT which is a discrete system of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. A smart grid system may also consist of operational technologies (OTs) or industrial control systems (ICS) like SCADA systems, distributed control systems (DCSs) and other control system configurations such as programmable logic controllers (PLCs) (Chong & Kumar, 2003; National Institute of Standards and Technology, 2014).

Industrial Internet of Things (IIoT) collects data from connected devices (i.e. smart connected devices and machines) in the field or plant and then processes these data using sophisticated software and networking tools. The entire IIoT requires a collection of hardware, software, communications and networking technologies (Electrical Technology, 2016).

Management of situational awareness in Finland

The Ministry of Finance of Finland is responsible for the steering and development of the state's information security (Ministry of Defence, 2010). The Government Situation Centre ensures that the state leaders and central government authorities are kept informed continuously in Finland. The Government Situation Centre was set up in 2007, and it has the duty to alert the government, permanent secretaries and heads of preparedness and to call them to councils, meetings and negotiations at exceptional times required by a disruption or a crisis. The ministries have the duty to submit the situational picture for their entire administrative branch to the Government Situation Centre and notify the centre of any security incidents in their field of activity. In urgent situations, the Government Situation Centre also receives incident reports of security incidents directly from the authorities. In addition, the Government Situation Centre follows public sources and receives SA information in its role as the national focal point for certain institutions of the EU and other international organizations.

Organizational changes of intelligence services in the United States

It has been seen in the United States that it is important to combine the functions of cybersecurity organizations that work separately. The Department of Homeland Security (DHS) provides support to potentially impacted entities, analyzes the potential impact across CI, investigates

those responsible in conjunction with law enforcement partners and coordinates the national response to significant cyber incidents (Department of Homeland Security, 2018a). DHS's National Cybersecurity and Communications Integration Centre is a cyber SA, incident response and management centre that is a national connection of cyber and communications integration for the federal government, intelligence community and law enforcement. NCCIC co-locates National Communications System (NCS), National Coordinating Centre (NCC) for communications, United States Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) into NCCIC watch floor 2012. The Cybersecurity Act of 2015 designates NCCIC as the central hub for cyber threat indicator sharing between government and the privacy sector. In 2017 NCCIC completes internal realignment (Department of Homeland Security, 2018b).

Cyber situational awareness at national level in Finland

The Ministry of Transport and Communications is responsible for safeguarding the functioning of electronic ICT systems. The Ministry of Finance is responsible for safeguarding the state administration's IT functions, information security and the service systems common to the central government (Secretariat of the Security Committee, 2013). The Security Committee coordinates cybersecurity preparedness, monitors the implementation of the cybersecurity strategy and issues recommendations on its further development (Secretariat of the Security Committee, 2013). The Finnish Communications Regulatory Authority (FICORA) works under steering control of the Ministry of Transport and Communications (Functions of the Finnish Transport Agency and FICORA merged to form the new Finnish Transport and Communications Agency Traficom on January 2019). The National Cyber Security Centre Finland (NCSC-FI) operates within the Finnish Communications Regulatory Authority (FICORA) and offers an increasingly diverse array of information and cybersecurity services. In its role as a statutory supervisory and steering authority with a responsibility for information security tasks, NCSC-FI gathers information. FICORA's other operations yield more information governed by legislation on events relating to incidents, deviations and disturbance situations (Finnish Communications Regulatory Authority, 2014). The information gained from nationally or internationally detected information security incidents, deviations and threats (incident response function, CERT) is combined with the information gained from inspections of information systems and telecommunications arrangements (information assurance function, NCSA) and the information received in the role as a supervisory and steering authority. The organizational responsibilities of cybersecurity are unclearly divided as Fig. 10.1 illustrated.

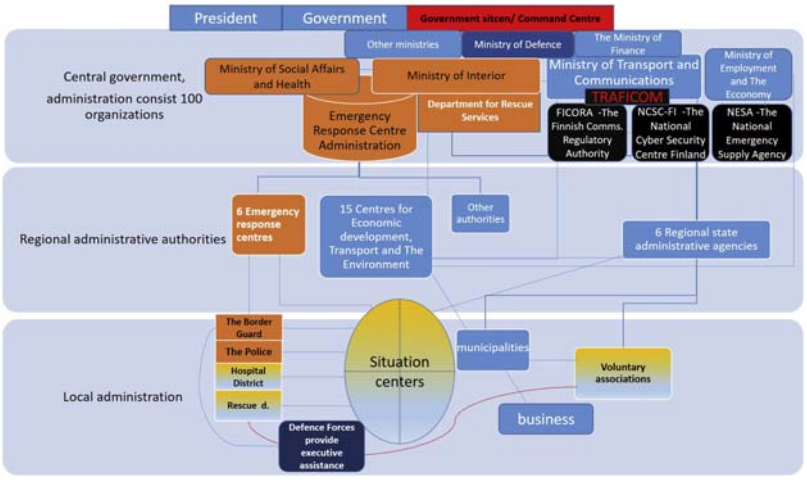


FIGURE 10.1 Organizations responsibilities of cybersecurity functions.

Cyber SA is combined; this information is used to produce NCSC-FI's combined cybersecurity situational picture, as illustrated in Fig. 10.2 (Finnish Communications Regulatory Authority, 2014).

Alert and detection system – HAVARO

HAVARO is an alert and detection system which FICORA has created in partnership with the National Emergency Supply Agency (NESA) in 2012. NESA is a public organization working under steering control of the Ministry of Employment and the Economy. NESA is responsible for planning and measures related to developing and maintaining security of supply.

For every Finnish organization, it is optional to join the HAVARO system, but joining brings many significant benefits. The information on situation awareness provided by the system increases understanding

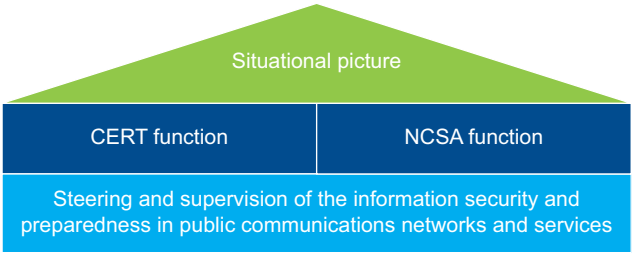


FIGURE 10.2 Producing of Finnish national cybersecurity situational picture (Finnish Communications Regulatory Authority, 2014).

about the organization's own and general state of information security. The system produces information which makes it also possible to alert other players about a detected threat and develop better means of detection. Clients can determine what sort of data the system processes and the ownership of the data remains with the company itself, in its own devices. HAVARO does not compete with commercial players or replace any other information security solutions. The participating organizations are responsible for the costs of equipment needed for their own network.

The system monitors information concerning security incidents only; it is incapable of monitoring the communication of individual users. Red observations indicate that the system has observed harmful traffic, which points to a likely information security breach in the organization.

The experiences from the system have been positive and have proved that the traditional controls are not always sufficient in the prevention and detection of malware. Between January and August 2015, the HAVARO system made a total of 1800 red observations. Red observations indicate that the system has observed harmful traffic, which points to a likely information security breach in the organization. Most observations concern utilization attempts made using mass distribution platforms, utilizing vulnerabilities in web browser add-ons (Adobe Flash in particular). A malware mass distribution platform is a program code which is run on a network server and utilized by criminals, the purpose of which is to install specific malware on the user's computer (Finnish Communications Regulatory Authority, 2014).

Cyber-physical systems

The term cyber-physical system (CPS) was coined by Helen Gill at the National Science Foundation in the United States to refer to the integration of computation with physical processes. In CPS, embedded computers and networks may monitor and control the physical processes with feedback loops where physical processes affect computations and vice versa. CPS are enabling the next generation of 'smart systems' like advanced robotics, computer-controlled processes and real-time integrated systems (Lee & Seshia, 2017).

Modern infrastructures include not only physical components but also hardware and software. These integrated systems are examples of CPS that integrate computing and communication capabilities with monitoring and control of entities in the physical world. Fig. 10.3 presents a CPS that consists of two physical layers (platform layer and human layer) and a cyber layer between them. The current trend is that the cyber layer is expanding.

Many CPS applications are safety-critical which means that their failure can cause irreparable harm to the physical system under control and to the people who depend on it. In particular, the protection of our CIs that

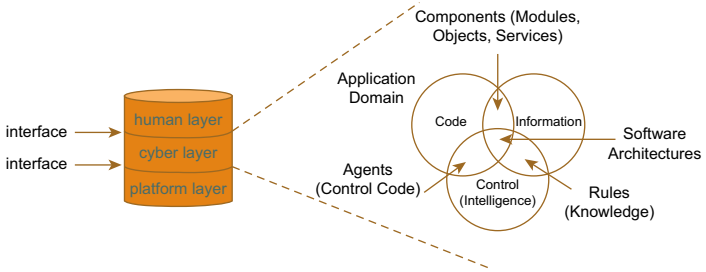


FIGURE 10.3 Layers of cyber-physical systems. *Modified from Hevner, A., Chatterjee, S., 2010. Design research in information systems: Theory and practice. Springer Science and Business. https://doi.org/10.1007/978-1-4419-5653-8.*

rely on CPS, such as the electric power transmission and distribution, ICSs, oil and natural gas systems, water and wastewater treatment plants, health-care devices and transportation networks play a fundamental and large-scale role in our society and their disruption can have a significant impact to individuals and nations at large. Increasingly many CPS are operated under automated controls and a sophisticated cyberattack can exploit weaknesses to its advantage (Hevner & Chatterjee, 2010).

Tracking in the everyday life of citizens

In the market economy, customer profiling or tracking is seen only from the point of view of data exploitation in Internet marketing. Advertisers try to focus on services and products more efficiently for the right target audience. Location-based services rely on a combination of technologies to pinpoint the location of a user with contextual data to provide more value to a mobile user. Geo-targeting or Geo-fencing with Wi-Fi, cell towers and beacons create a privacy-restricting advertisement circuit that aims to influence consumer behaviour. How can the need for CIP be understood in this context? The question is not simple because every person abandons some of their privacy by using smart devices. It does not always seem to matter whether or not a smartphone user is aware of the data 'leakage'. For example, when introducing a smartphone a user accepts many things that are required to make the smartphone work properly. If you do not give permission to provide privacy information to a third party, it is possible that the device may not work at all.

Most of the Western world carries a multifunction sensor called a smartphone. Intelligent devices are increasingly used to access the Internet rather than traditional calling. For proactive safety, data stored in a mobile phone combined with human behaviour can create new predictive ecosystems for the infrastructure. Different kinds of sensor

systems are already in use. The Berlin train station has created a detection system (Huggler, 2017) with face detection technology, and for example, in Stockholm, there is an ongoing traffic safety project (Scania, 2018) which utilizes motion detector-based artificial intelligence.

From location-based services to location-based intelligence

A citizen's smart device is quite easy to locate. International Mobile Equipment Identity (IMEI) number and SIM card with international mobile subscriber identity (IMSI) helps to track a mobile. Mobile phones transmit these numbers each time a call is made and when they 'check in' to the local base stations (Pettit, 2018).

Police may use an IMSI-catcher to encrypt a call. At that point the phone call is transmitted through an IMSI-catcher. It works like a fake base station. Law enforcement teams in the United States and Europe have used this technology to locate people etc., but nowadays criminals like hackers are deploying them (Langston, 2017). According to Shaik, Borgaonkar, Asokan, Niemi, and Seifert (2016), it has been shown that the vulnerabilities in LTE access network protocols lead to new privacy and availability threats to LTE subscribers.

Customers are concerned about their privacy because location-based technologies allow mobile advertising networks to accurately send advertisements to maximize the effect of advertisement (Kini & Suomi, 2018).

Retailers of malls may use indoor or/and outdoor navigation technologies to provide location-based services, using mobile 'push' notifications to provide advertisements. With this technology it is possible to provide appropriate, personalized marketing based on the consumer's location. If customers or mobile users give permission (opt-in) to their trusted companies whose brand, products and services they like, they send them personalized advertisements when they are shopping (Yiu, Jensen, Møller, & Lu, 2011).

Technologies are currently available to not only locate the customers; they are also able to establish a history of a path taken by a typical customer during the day. Consumer-oriented organizations are concerned about how advertisement networks are able to locate and custom-deliver an advertisement to a customer with or without the customer's permission (Kini & Suomi, 2018; Metz, 2013). According to Nakashima (2018), AP investigation found that Google stored location data even though 'location history' is turned off.

New smartphone technologies combine marketers and application providers to get their strategies to a new marketing area. As Kini and Suomi (2018) write, the big data analytical tools can do the data analysis and help marketing actors produce and deliver personalized advertisements to customers' or potential customers' smart devices everywhere. There is a

risk that collected data can be used for wrong purposes instead of proper use for protection of vital functions. Law enforcement may use the same tools as advertisers or marketers, but these tools are traditionally intended for marketing purposes rather than the needs of law enforcement agencies. It has been noted within PPDR authorities that the use of location-based services will become a more common tool in the field of crime prevention. As communication technology evolves, people's living environment also develops. Development of intelligent cities brings new kinds of opportunities to develop services from a safety environment perspective.

If a citizen walks to the geofenced area and receives a mobile advertisement message, the citizen might be motivated to look at and take action on the text message based on: if they permitted someone to send such a message (opted-in); if they trust such a company producing or selling a product or service (brand trust); if the product or service is relevant to the customer's current needs and wants; if the customer likes the price that is quoted on the message; if the customer is financially in a position to buy such a product or service and last, if the customer is in the right mood to buy such a product (Kini & Suomi, 2018).

If a citizen does not know the purpose of using privacy data, the situation is ethically untenable. Therefore, it is important for a citizen to be aware that he or she can be treated as a customer in marketing, but also as a potential threat to the functions of CI.

According to Sheng et al. (2006) customers' privacy concerns vary depending on their purpose or context for using the technology. Personalization has major implications in emergency situations, for example at the site of an accident where appropriate services need to be delivered to the right person and place. The effect of personalization on perceived benefits is greater in emergency than non-emergency contexts.

Research method and process

Case study of this research is carried out by the guidance of Yin (2014). Case study illustrates the attempt to produce profound and detailed information about the object under research.

The fundamental research data of this extended study are collected from earlier empirical research studies where the author has been the main researcher. Studies have been presented in international conferences and published. The research data included, for example, material of interviews and observations from four situation centres. A new type of emergency centre system was created as a result of previous research. The purpose of this study is to compare the results of the studies from a privacy perspective. Scientific literature materials and legislative publications have been used for comparison. The purpose of the comparison is to find the

factors concerning privacy issues that influence the introduction of the presented hybrid emergence model.

Four regional command/situation centres have been researched in an earlier (Simola & Rajamäki, 2017) empirical study: Southwestern Finland Police department, Southwest Finland Emergency Services, Hospital District of Southwest Finland and The Finnish Border Guards in Turku. The Finnish Border Guards have their own main situation/command centre in Turku called the Maritime Rescue Coordination Centre (MRCC). The situation centre of the Southwestern Finland Police department and the MRCC are managed by the state. Southwest Finland Emergency Services and Hospital District of Southwest Finland act under the municipality. The field commanders of the situation centres were interviewed in their own work environment.

The fundamental research data of earlier studies are based on observations, interviews, scientific publications, collected articles and literary material. Participant observation makes it possible to get close to the actors. It illustrates the identities of actors' diversity (Viinamäki & Saari, 2007). Observation is made on the field and the results are recorded and saved as notes. One prominent data collecting method used was focus interviews (Brannen, 2004).

Findings

Regional situational centres use different systems and therefore the same system can be used in two situation centres without cooperation with each other. None of the regional situation centres have direct contact with the Government Situation Centre, but the connections are handled through intermediaries. For rapidly evolving situations, access to the Government Situation Centres', data connection should be arranged to the essential situation centres.

As recent major accidents have indicated, lack of human resources affects disaster recovery. PPDR actors cannot start operations if there is a human factor preventing the flow of information. Preventing domino effect after the disaster may be delayed. Recent violent acts at local and state level (from local to national level) have shown this to be a reality. The communication activities of Intermediaries have been one of the major problems in recent major accidents. In Brussels, Belgium, federal police requested to close the metro, and the main railway stations did not reach the responsible chief of the railway police because phone networks were down. A request to close the railway station was sent to the responsible authority's personal email instead of work mail. The responsible authority did not see the message until after the attacks (McLaughlin, Haddad, & Hume, 2016). The November 2015 terror attacks also did not cause a total closure of the Paris

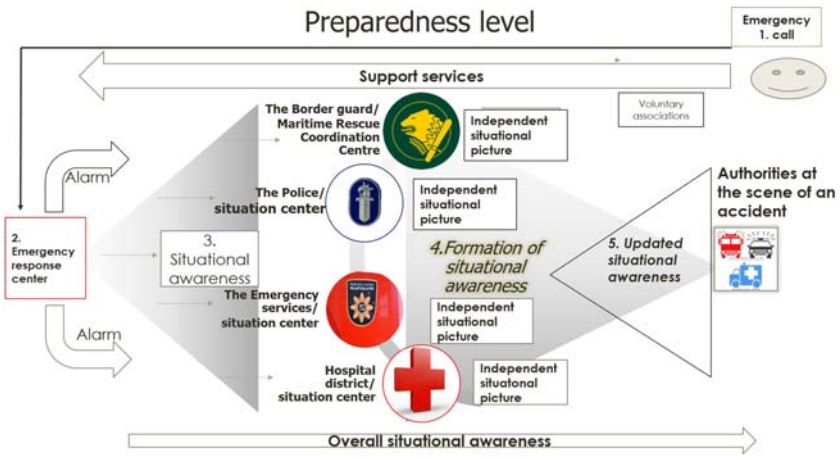
Metro or other public arenas (Steafel et al., 2015, The Guardian, 2016). Therefore, a workable cyber environment with automated functions must be seen as a common objective of organized societies. The main issue regarding reliable decision support analysis to decision-makers is at which point in the chain reaction the human action is more harmful than useful (Endsley, 1988, 1995, 2015). There is a lot to be done to transfer essential emergency procedures into automated emergency functions.

Hybrid emergency response model does not violate privacy of the citizens more than what is required to prevent a threat because the use of technology is linked to the current law, but underdeveloped local urban infrastructure prevent utilization of intelligence collection methods including local-based intelligence solutions. The ongoing privacy legislation reform in the EU and in United States creates some barriers for the artificial intelligence developers. Protecting vital functions of society and securing continuity management PPDR authorities receive major support among the citizens. Privacy issue problems related to personal data registers can be solved by automation. The automatized method allows almost 10,000 authorities to release resources from curiosity tasks.

Emergency situations

The lack of cooperation between situation centres prevents the ability to create a common SA and picture. Starting cooperation at the scene of an accident, as Fig. 10.4 illustrates, is not enough during a major accident in a modern CPS.

The officer in charge of the situation is responsible for maintaining the situational picture and for coordinating the operations. Unless otherwise agreed, the officer in charge of the rescue operations comes from the



rescue service region where the accident or dangerous situation occurred. The field commander and the officer in charge of rescue operations decide together if it is necessary to make a major accident alert. For example, the Turku University Hospital has its own command centre, which is set up in case of a major accident. The leading medical director, managing director and other managing personnel get together in their command centre depending on the type of major accident.

The differences of rescue operations illustrate the fact that it would be important to see all the resources available. However, a reliable and correct common situational picture should be created before arriving to the scene of the accident. If the scene is a modern CPS, a cyber situational picture is also needed.

As shown in picture 10.5. of the hybrid emergency response model, proactive accident/incident management begins before any physical harm has occurred. Sensor networks consist of cyber and physical elements with automated functions. The cyber environment of hybrid model works in many ways. It detects intrusions and threats in CI before any emergency call has been made. Data fusion analysis combine and produce important signals based on commands, which launch automatic processes like isolating an area under threat or robotic functions based on biometrics data such as thermal imaging or face recognition. Data fusion might also help with false alarms by fusing the information from multiple sources; also false alarms can be avoided by combining sensors. The processing device (controller) sends commands to a wireless sensor and actuator network (WSAN) which then converts them into input signals for the actuator, that acts with a physical process, thus forming a closed control loop. The field-tested DSiP solution with 4com routers (Simola & Rajamäki, 2014) enables parallel use of different network technologies in a consistent and transparent way, enabling communications services platforms to be created. In cyber-physical operations, this feature reduces network jamming. The hybrid model reduces the necessity of communication with VIRVE phones between authorities. It also eliminates errors of human activity when an accident situation is on. Automated safety measures can also bypass the problems related to the commandment of power relations. Hybrid emergency response system allows people to send pictures or video calls from the scene of an accident. Smart System allows crowdsourcing software to screen the images and videos automatically. Relevant data from the major accident will be directly shared to the field commanders and Government Situation Centres. To determinate discrepancies of limits is relevant to allocate additional reliable data. Combining pieces of information to ensure the correct and reliable information to be shared is of primary importance. The essential information is processed to the desired shape for the accident site command centre. The system is based on active operations and automated functions. Cyber defence operations are integrated and automated

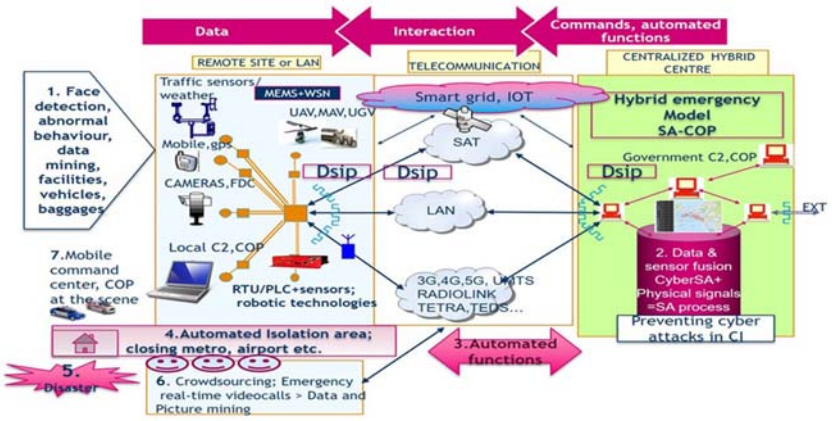


FIGURE 10.5 Hybrid emergency response model.

according to local capabilities, authorities and mission needs. In a local city area, sensor networks of a shopping mall may consist of LBS elements, for example geofencing area with automated functions like speed breakers, which automatically activate when the level of threat has risen high as Figs. 10.5 and 10.6 illustrates.

A lack of preparedness affects the cooperation within PPDR authorities in the field at a major accident. Reforms in public sector and changes in PPDR organizations with legislative amendment require changes in preparedness plans. At present, managerial personnel get together at each other's command centres depending on the type of accident.

Today, too many hierarchy levels in and between organizations exist. Therefore, deciding on new technology faces challenges. If there are too

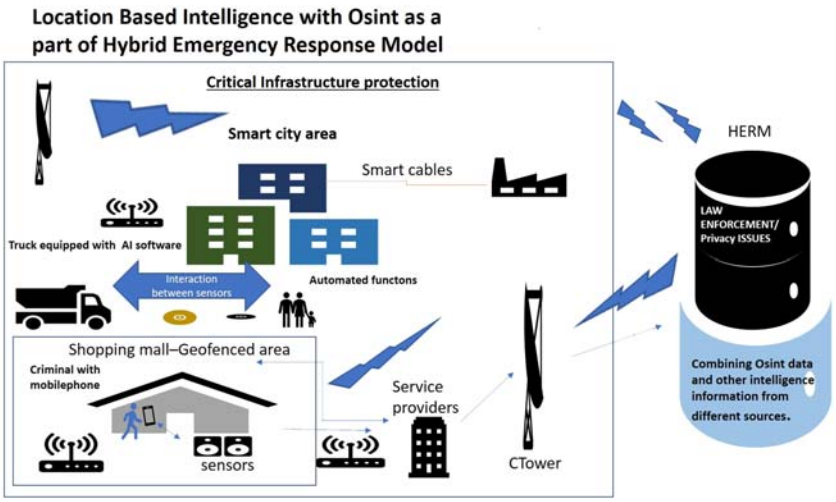


FIGURE 10.6 Location-based intelligence with OSINT as part of the HERM.

many hierarchy levels, information of a situation does not flow or, at least, it is slow (Rajamäki & Viitanen, 2014). Responsibilities for developing cybersecurity has been shared in too many factors (Finnish Communications Regulatory Authority, 2014; Kauppinen, 2015; Ministry of Defence, 2010; Ministry of the Interior, 2016; National Cooperation Network for Disaster Risk Reduction, 2012).

Discussion

Both the European and the American regulations aim at achieving cyber resilience, enhancing cooperation between public and private sectors in order to improve capacities, resources and processes to handle cyber-physical threats in CIs. But that is not enough; there is a need for common cyber ecosystem to control crossboarding threats.

In Europe there should be clearer common rules concerning which privacy issues need to be abandoned when getting around in public places and what kind of data should be considered private. Combining data from different sources can create opportunities, but also major threats at personal profiling level in the protection of CI. The collected data cannot be used if their use is unauthorized. Data must also be utilized for permitted purpose. There are also some problems in creating a monitoring system when considering political and technological aspects.

In Finland, the importance of privacy has risen to the surface of the social welfare and health care (SOTE) reform. The Finnish government's concept of human disease classification system based on patient records has raised protests. There is a clear trend for the creation of different classification systems in Europe, but the problem arises when people are classified on the basis of information and data management is given to a third party. In Finland, one of the focal points of the SOTE reform is related to the integration of patient registers and the creation of one information system.

Traditional thought within Finnish decision-makers has been that the commercial operators must be kept separate from regulatory activities. In the United Kingdom the Home Office-led Emergency Services Network (ESN) will replace the existing Airwave mobile radio system. ESN will be delivered using commercial network. The police communications network enables officers to access key databases, to take electronic fingerprints and witness statements and to stream live video while on the move (Nasir, 2016; Travis, 2015).

People have been irritated by the fact that their behaviour has been collected more widely than what has been told and for uses that are not known. Therefore, it might be important to look at the big picture of protecting the CI. What kind of elements can be included in the framework which protects the vital functions of society. When all the things we do leave some data to tracking systems, people have the right to know what information is collected and for what purpose it has been collected.

Perhaps even more important is to know who the holder (controller or processor) is of the privacy data and what is the storage time of the data.

According to Waterfield (2018), the navigator manufacturer TOMTOM reported in 2011 that it has sold data stored by the navigators from citizens' movements to the Danish police. The purpose of the collected data was to show where to set up speed traps. How can a citizen be assured that a publicly commented matter and a real case mean the same if the authorities supervise themselves? However, the fact is that technological hybrid models developed for CI also need hybrid models for data collection in order to identify threats in a predetermined and error-free manner.

In a society where the limits of public and private commercial players have become obscured, the risks are also increasing. Citizens should be able to trust decision-makers, authorities and society so that they do not have to constantly think about what kind of digital footprints they have left behind in any department store control unit. As a single datum, separate information of human life is not significant, but if data are combined from different sources, the position of a citizen as a person of his or her own life and knowledge may change significantly.

Conclusions

As discussed above, digitalization and location-based technologies create opportunities but also threats to citizen's privacy life. If political power relations change in a democratic society, public power may centralize, for example on the communist regime or for a dictator. How would the privacy-related information be used in different political environments? It is essential because the world order is in a turbulent state. Different types of extremism have increased their support.

The need for a new type of standardized hybrid emergency response model reflects the following factors. It is necessary for confidence that citizens accept automatized safety functions in public places. Legislation concerning privacy issues does not cause permanent obstacles to use sensing elements in hybrid emergency response model. It is necessary to rationalize organizational responsibilities for development of cybersecurity. A human is an individual with limited observation capability, and overlapping data transmission limits the effective cooperation between PPDR authorities. Limited data transmission capacity prevents communication between the authorities. Preventive functions against cyberthreats in the emergency response model are an essential part of the overall security in situation awareness management and CIP.

It is also important for the continuity management to create a confidential base between citizens and authorities. Confidential data cannot be leaked to outsiders, for example to the press. At present, the values of those Western worlds have been contrasted with the protection of overall

security and CI. Important things for us, such as the data privacy issues, can be more relieved on the grounds that the 'common good' requires it. How can we then define the common good? This issue has been controversial in Europe. Determining the public interest or limiting the need to protect society has sometimes caused difficulties. The fact that the intelligence services workers have come to the public with information acquired through the workplace has not made it any easier. The problem is related to situations where protected legal interests are incompatible.

Fighting against cyberthreats is an essential part of the overall security in continuity management. Often, urban built infrastructures represent a critical node within the intertwined networks of an urban area. A substantial part of our CPS today relies on complex systems of communication networks. There is just as much of a need to take into account the equally vulnerable built infrastructures of modern urban areas (Davis et al., 2006).

In the future a centralized hybrid emergency model with predictive emergency response functions is necessary. A shared common operational picture means that real-time communication links from local level to state level must exist. At the moment the flow of real-time data is not being transmitted to the Government Situation Centre. For example, if a cyberattack interrupted electricity transmission, telecommunication networks discontinue operating. A cyberattack becomes physical if intrusion has not been detected. Hybrid warfare needs hybrid responses. The government departments of Finland must take into consideration that cyber preparedness and privacy issues are not a separate part in the continuity management. In practice this means that there is need to integrate ERC and National Cyber Security Centre Finland emergency functions. Flow of information between intelligence authorities and data protection authorities must also be ensured. In an ideal model, privacy protection would be ensured automatically. When human weaknesses are left out of procedure, data leakage to third parties becomes more difficult. It could increase citizens' confidence in the system's activities.

The new intelligence legislation package proposed by the Finnish government would include provisions on the principles of intelligence activities. If the legislation package is approved, it is expected to enhance the ability of the PPDR authorities to respond to major national and international hybrid threats because it also allows wider use of new decision support system technologies. It requires clarification of common rules. In other words, in a public place, for example in shopping centres, privacy protection should be facilitated if citizens accept common rules which have been created in the form of legislation.

When we deal with an individual and the privacy of an individual, he or she would not immediately think it would also be connected to wider entities. What may be possible with micro-level tracking for an individual may occur at a macro level remotely by interfering with data cable connections.

The micro and macro levels will be encountered if a foreign state party intervenes to interfere with the functioning of data traffic in maritime areas. For example, there is a northeast cable project designed to connect networking activities between different continents. Nowadays the problem is that fibre optic and power supply are transmitted through the same cable. Vulnerabilities and risks have increased, though formally, the goal is to harmonize Eastern and Western data cable functionalities (Buchanan, 2018; Shackelford et al. 2017). The study shows that the most troublesome and most significant threats to national security and vital functions are related to politicians and political projects. It is difficult to anticipate the real direction of national policy in the macro level because good inter-state relations may indicate ignoring security issues. This state-level political dimension may prevent the utilization of the proposed smart hybrid emergency model.

References

Ahmed, D. T., Hossain, M. A., Shirmohammadi, S., Alghamdi, A., Pradeep, K. A., & El Saddik, A. (2012). *Utility based decision support engine for camera view selection in multimedia surveillance systems*. https://doi.org/10.1007/s11042-012-1294-7.

Ahokas, J., Guday, T., Lyytinen, T., & Rajamäki, J. (2010). Secure and reliable communications for SCADA systems. *International Journal of Computers and Communications, 6*(3), 167−174.

Aine, A., Nurmi, V., Ossa, J., Penttilä, T., Salmi, I., & Virtanen, V. (2011). *Moderni kriisilainsäädäntö*. Helsinki: WSOYpro.

Baldini, G. (2010). *Report of the workshop on "interoperable communications for safety and security" with recommendations for security research*. Publications Office of the European Union. https://doi.org/10.2788/19075.

Brannen, J. (2004). *Working qualitatively and quantitatively in qualitative research practice*. In C. Seale, G. Gobo, J. F. Gubrium, & D. Silverman (Eds.) (pp. 312−326). London: Sage Publications.

Bröring, A., Echterhoff, J., Jirka, S., Simonis, I., Everding, T., Stasch, C., et al. (2011). New generation sensor web enablement. *Sensors, 11*(3), 2652−2699.

Buchanan, E. (2018). *Sea cables in a thawing Arctic [homepage of lowy institute]*. Available from https://www.lowyinstitute.org/the-interpreter/sea-cables-thawing-arctic.

Chong, C., & Kumar, S. (2003). Sensor networks: Evolution, opportunities and challenges. *Proceedings of the IEEE, 91*(8), 1247−1256. https://doi.org/10.1109/JPROC.2003.814918.

Chrisafis, A. (2016). Paris attacks inquiry finds multiple failings by French intelligence agencies. *The Guardian*. Available from https://www.theguardian.com/world/2016/jul/05/paris-attacks-inquiry-multiple-failings-french-intelligence-agencies.

Corporation, N. E. C. (2016). *Face recognition: Technologies: Biometrics: Solutions and services | NEC, homepage of NEC*. Available from http://www.nec.com/en/global/solutions/biometrics/technologies/face_recognition.html.

Davis, R., Ortiz, C., Rowe, R., Broz, J., Rigakos, G., & Collins, P. (2006). *An assessment of the preparedness of large retail malls to prevent and respond to terrorist attack. (No. 216641*. Available from https://www.ncjrs.gov/pdffiles1/nij/grants/216641.pdf.

Department of Homeland Security. (2018a). *Cyber incident response [homepage of DHS]*. Available from https://www.dhs.gov/cyber-incident-response.

Department of Homeland Security. (2018b). *The national cybersecurity and communications integration center's (NCCIC)*. Available from https://www.us-cert.gov/about-us.

Dos Passos, D. (2016). Big data, data science and their contributions to the development of the use of open source intelligence. *11*(4). https://doi.org/10.20985/1980-5160.2016.v11n4.1026.

Electrical Technology. (2016). *Internet of things (IOT) and its applications in electrical power industry [homepage of ET]*. Available from http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In *Proceedings of the human factors society 32nd annual meeting human factors society, Santa Monica. CA* (pp. 97—101).

Endsley, M. R. (1995). Toward a theory of situation awareness. *Human Factors, 37*(1), 32—64.

Endsley, M. R. (2015). *Autonomous horizons, system autonomy in the air force - a path to the future, air force office of the chief scientist*. USA: Department of The Air Force. Available from https://www.hsdl.org/?view&did=768107.

European Commission. (2002). *Directive on privacy and electronic communications Directive 2002/58/EC, Directive* (Brussels).

European Commission. (2016a). *EU data protection directive 2016/680, directive* (Brussels).

European Commission. (2016b). *EU-U.S. privacy shield: Stronger protection for transatlantic data flows*. Brussels).

European Commission. (2016c). *General data protection regulation (EU) 2016/679, regulation* (Brussels).

European Commission. (2017). *Proposal for a regulation on privacy and electronic communications, regulation proposal* (Brussels).

Finnish Communications Regulatory Authority. (2014). *National cyber security centre: Action plan 2014-2016*. Available from https://www.viestintavirasto.fi/attachments/NCSC-FI_Action_plan_20142382112016.pdf.

Finnish Security Intelligence Service. (2015). *The year book 2015*. Helsinki: Ministry of the Interior. Available from:https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/67074_2015_Supo_ ENG.pdf?cb0cc853f98ed588.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*, 18-31-46 http://doi.org/10.1016/j.cose.2014.06.008.

Gervasi, O. (2010). Encryption scheme for secured communication of web based control systems. *Journal of Security Engineering, 7*(6), 12.

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of open source intelligence (OSINT). *Computers in Human Behavior, 28*(2), 673—682. http://10.1016/j.chb.2011.11.014.

Hanni, J. (2013). *The quality and amount of information for emergency situations management*. Oulu: Oulu University of Applied Sciences. http://www.theseus.fi/handle/10024/65618.

Hevner, A., & Chatterjee, S. (2010). *Design research in information systems: Theory and practice*. Springer Science and Business. https://doi.org/10.1007/978-1-4419-5653-8.

Huggler, J. (2017). *Facial recognition software to catch terrorists being tested at Berlin station*. Available from http://www.telegraph.co.uk/news/2017/08/02/facial-recognition-software-catch-terrorists-tested-berlin-station/.

IBP. (2014). *European Union cyber security strategy and programs handbook. Strategic information and regulations*. Washington DC, USA: International Business Publications.

Kauppinen, T. (2015). *Cyber security of supply, FIIF jam session*. National Emergency Supply Agency.

Kini, R.,B., & Suomi, R. (2018). Changing attitudes toward location-based advertising in the USA and Finland. *Journal of Computer Information Systems, 58*(1), 66—78. https://doi.org/10.1080/08874417.2016.1192519.

Langston, J. (2017). *Catching the IMSI-catchers: Sea glass brings transparency to cell phone surveillance [homepage of UW news]*. Available from https://www.washington.edu/news/2017/06/02/catching-the-imsi-catchers-seaglass-brings-transparency-to-cell-phone-surveillance/.

Lee, E., & Seshia, A. (2017). *Introduction to embedded systems, a cyber-physical systems approach* (2nd ed.). MIT Press, ISBN 978-0-262-53381-2. Available from https://ptolemy.berkeley.edu/books/leeseshia/releases/LeeSeshia_DigitalV2_2.pdf.

McLarty, T., III, & Ridge, F. T. (2014). *Securing the U.S. Electrical grid*. Washington D.C: The Center for the Study of the Presidency and Congress. https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf.

McLaughlin, E., Haddad, M., & Hume, T. (2016). *Brussels attacks: Order to close metro sent to wrong address -*. Available from CNN.com http://edition.cnn.com/2016/05/12/europe/belgium-brussels-attacks-metro-email/.

Metz, R., (2013). Every step you take tracked automatically. Technology Review, MIT. Available from: https://www.technologyreview.com/s/510491/every-step-you-take-tracked-automatically/. (Accessed: 28.8.2018).

Ministry of Defence. (2010). *Security strategy for society, government resolution*. Helsinki: Ministry of Defence. Avalable from https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf.

Ministry of the Interior. (2016). *National risk assessment 2015*. Helsinki: Ministry of the Interior. Available from http://urn.fi/URN:ISBN978-952-324-060-5.

Morrow, J., & Odierno, R. (2012). *Open-source intelligence, ATP 2-22.9*. Washington: Army Techniques Publication, Headquarters, Department of the U.S. Army. https://fas.org/irp/doddir/army/fmi2-22-9.pdf.

Nakashima, R. (2018). *AP exclusive: Google tracks your movements, like it or not [homepage of AP news]*. Available from: https://apnews.com/828aefab64d4411bac257a07c1af0ecb.

Nasir, R. (2016). *LTE to replace TETRA network for UK emergency services - [Homepage of Networkingplus]*. Available from https://www.networkingplus.co.uk/Media/Default/archive/Net1601.pdf.

National Cooperation Network for Disaster Risk Reduction. (2012). *National platform for disaster risk reduction*. Helsinki: Ministry of the Interior. Available from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79425/sm_142012.pdf.

National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO). (2016). *NENA/APCO next generation 9-1-1 public safety answering point requirements*. USA: NENA and APCO.

National Institute of Standards and Technology. (2014). Guidelines for smart grid cybersecurity national institute of standards and technology. In *Smart grid cybersecurity strategy, architecture, and high-level requirements* (Vol. 1). USA: U.S. Department of Commerce.

National Public Safety Telecommunications Council. (2015). *FirstNet and next generation 9-1-1 high-level overview of systems and functionality.* Available from http://www.npstc.org/download.jsp?tableId=37&column=217&id=3466&file=How_NG911_Will_Work_with_FirstNet_FINAL.pdf.

Nurmi, P. (2015). *OSINT - avointen lähteiden internet-tiedustelu*. Helsinki: Aalto yliopisto.

Pettit, H. (2018). *Are police tracking your movements using your mobile phone? Privacy watchdog to challenge five UK forces in court over their failure to deny they use 'fake cell towers' to spy on citizens [homepage of daily mail online]*. Available from http://www.dailymail.co.uk/sciencetech/article-6039023/Are-police-tracking-mobile-phone-Privacy-group-challenge-UK-forces-court-IMSI-catchers.html.

Rajamäki, J., & Viitanen, J. (2014). Near border information exchange procedures for law enforcement authorities. *International Journal of Systems Applications, Engineering & Development, 8*, 2015−2020.

Rosslin, J. R., & Tai-hoon, K. (2010). Communication security for SCADA in smart grid environment. no. In *Advances in data networks, communications, computers*. Available from http://www.wseas.us/e-library/conferences/2010/Faro/DNCOCO/DNCOCO-05.pdf.

Scania. (2018). *Scanias geofencing teknik visades upp i Stockholm*. Available from https://www.scania.com/scaniasodertalje/sv/home/nyheter-event/scanias-geofencing-teknik-visades-upp-i-stockholm.html.

Secretariat of the Security Committee. (2013). *Finland's cyber security strategy - government resolution*. Ministry of Defense. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

Shackelford, S. J., Sulmeyer, M., Deckard, A., Graig, N., Buchanan, B., & Micic, B. (2017). From Russia with love: Understanding the Russian cyber threat to U.S. critical infrastructure and what to do about it. *Nebraska Law Review, 96*(2), 321–337. https://digitalcommons.unl.edu/nlr/vol96/iss2/5.

Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J. (February, 2016). *Practical attacks against privacy and availability in 4G/LTE mobile communication systems*. USA: NDSS. https://doi.org/10.14722/ndss.2016.23236.

Sheng, H., Nah, F. F., & Siau, K. (2006). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems, AMCIS 2006 Proceedings, 9*(6), 80–84, 370 http://aisel.aisnet.org/amcis2006/370.

Simola, J., & Rajamäki, J. (2014). Using a real-time video to allocate public protection and disaster relief resources in rescue service process - natural diaster in Young voluntary firefigter's camp. In *5th European conference of computer science (ECCS '14)*. WSEAS Press. http://urn.fi/URN:NBN:fi:amk-201802132394.

Simola, J., & Rajamäki, J. (2016). Common cyber situational awareness: An important part of modern public protection and disaster relief. In *10th international conference on computer engineering and applications (CEA '16)* (p. 54). WSEAS press, ISBN 978-1-61804-365-8. http://urn.fi/URN.

Simola, J., & Rajamäki, J. (2017). Hybrid emergency response model: Improving cyber situational awareness. In M. Scanlon, & N. Le-Khac (Eds.), *16th European conference on cyber warfare and security* (pp. 442–451). UK: APCI, ISBN 978-1-911218-44-9. http://urn.fi/URN.

Steafel, E., Mulholland, R., Sabur, R., Malnick, E., Trotman, A., & Harley, N. (2015). *Paris terror attack: Everything we know on saturday afternoon – telegraph*. Available from http://www.telegraph.co.uk/news/worldnews/europe/france/11995246/Paris-shooting-What-we-know-so-far.html.

Travis, A. (2015). Questions over limited range of new £1bn emergency services network. *The Guardian*. https://www.theguardian.com/society/2015/dec/09/emergency-services-network-questions-limited-range-1bn.

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies, 18*(4–5), 530–547. https://doi.org/10.1177/1367549415577396.

Vetter, M. (2015). *Open source intelligence techniques and the Dark Web*. Available from www.itproportal.com/2015/10/30/open-source-intelligence-techniques-and-the-dark-web/.

Viinamäki, L., & Saari, E. (2007). *Polkuja soveltavaan yhteiskuntatieteelliseen tutkimukseen*. Helsinki: Tammi.

Waterfield, B. (2018). *Tom Tom sold driver's GPS details to be used by police for speed traps - Telegraph*. Available from https://www.telegraph.co.uk/technology/news/8480702/Tom-Tom-sold-drivers-GPS-details-to-be-used-by-police-for-speed-traps.html.

Wood, M., & Graham. (2016). Social media intelligence, the wayward child of open source intelligence. *Responsible Data Forum*. https://responsibledata.io/social-media-intelligence-the-wayward-child-of-open-source-intelligence/.

Yin, R. K. (2014). *Case study research, design and methods* (5th ed.). Thousand Oaks: Sage Publications.

Yiu, M.,L., Jensen, C. S., Møller, J., & Lu, H. (2011). Design and analysis of a ranking approach to private location-based services. *ACM Transactions on Database Systems, 36*(2), 10:1–10:42. https://doi.org/10.1145/1966385.1966388.

V

EMERGENCY RESPONSE MODEL AS A PART OF THE SMART SOCIETY

by

Jussi Simola, Martti Lehto & Jyri Rajamäki 2021

Proceedings of the 20th European Conference on Cyber Warfare and Security
ECCWS 2021. 24th - 25th June 2021, Chester, UK, 382-391

https://urn.fi/URN:NBN:fi-fe2021082343867

Emergency Response Model as a part of the Smart Society

Jussi Simola[1,2], Martti Lehto[1], Jyri Rajamäki[2]
[1]University of Jyväskylä, Finland
[2]Laurea Universtiy of Applied Sciences, Finland
jussi.hm.simola@jyu.fi
martti.j.lehto@jyu.fi
jyri.rajamaki@laurea.fi
DOI: 10.34190/EWS.21.079

Abstract: Centralized hybrid emergency model with predictive emergency response functions are necessary when the purpose is to protect the critical infrastructure (CI). A shared common operational picture among Public Protection and Disaster Relief (PPDR) authorities means that a real-time communication link from the local level to the state-level exists. If a cyberattack would interrupt electricity transmission, telecommunication networks will discontinue operating. Cyberattack becomes physical in the urban and maritime area if an intrusion has not been detected. Hybrid threats require hybrid responses. The purpose of this qualitative research was to find out technological-related fundamental risks and challenges which are outside the official risk classification. The primary outcomes can be summarized so that there are crucial human-based factors that affect the whole cyber-ecosystem. Cybersecurity maturity, operational preparedness, and decision-making reliability are not separate parts of continuity management. If fundamental risk factors are not recognized, technical early warning solutions become useless. Therefore, decision-makers need reliable information for decision-making that does not expose them to hazards. One of the primary aims of hybrid influence is to change political decision-making. Practically, this means a need to rationalize organizational, administrative, and operative functions in public safety organizations. Trusted information sharing among decision-makers, intelligence authorities, and data protection authorities must be ensured by using Artificial Intelligence (AI) systems. In advanced design, protection of critical infrastructure would be ensured automatically as part of the cyber platform's functionalities where human-made decisions are also analyzed. Confidential information sharing to third parties becomes complicated when the weaknesses of crucial decision-making procedures have recognized. Citizens' confidence in the intelligent system activities may strengthen because of the decision-making process's reliability. Existing emergency response services are dependent on human ability.

Keywords: Critical Infrastructure Protection, cyber ecosystem, emergency response, public protection and disaster relief, artificial Intelligence

1. Introduction

As earlier researches (Simola & Rajamäki, 2015; Simola &Rajamäki, 2017) has shown, technical solutions need a deeper understanding of user needs. That means the infrastructure of a smart city environment cannot be developed separately from user requirements. There is also a need to design a common emergency response ecosystem for European public safety actors. Therefore, communication solutions used within public safety authorities must suit well in urban and rural area**s.**

Public safety actors like European law enforcement agencies need a common shared situational picture for the cross-boarding tasks so that operational cooperation is based on a reliable platform. Formal integration in the European Union and between member countries has developed rapidly. That does not mean that collaboration between organizations has developed in the same proportion. Digitalization cannot evolve in isolation from society. There are fundamental needs within public European safety organizations that should be at the same level in every country.

Decision-makers in Finland need to consider that cybersecurity maturity, operational preparedness, and decision-making reliability are integral parts of continuity management. Technical early warning solutions become useless to develop if crucial risk factors are not detected. Therefore, decision-makers need reliable decision-support information for decision-making that does not expose them to hazards. Technological development, infrastructure development, and legislation changes are inner-country challenges and everyday European needs concerning safety development agendas. State-level factors should be added to the European safety framework. There are many strategic plans at the European level concerning

safety functions, but national implementation realizes in a different order. As the report of the SAI (2017) indicates, Finland has a lot to do to improve the information exchange in significant accident situations.

Citizens choose political decision-makers, but the highest authorities are selected on selection criteria. Hybrid influencing can destabilize society in many ways, especially if threats accumulate or arise from within the society (Simola, 2020). One of the primary key aims is to influence political decision-making. In practice, this means a need to rationalize organizational, administrative, and operative functions (SAI, 2017). The flow of reliable information between decision-makers, intelligence authorities, and data protection authorities must also be ensured by using artificial intelligence systems. In an ideal model, national protection of vital functions would be ensured automatically as part of the cyber platform's functionalities where human-based decisions are also analyzed. When human weaknesses are left out of decision-making procedures, e.g., data leakage to third parties becomes more difficult. It could increase citizens' confidence in the smart system's activities and increase trust in government institutions.

Security and intelligence agencies in Europe have acquired new rights under the law. In Finland acceptation of Intelligence legislation package concerning civilian and military intelligence legislation has been approved. It will be seen in the future how prepared our state-level decision-makers are to develop the legislative base for the new cyber-physical ecosystem. A substantial part of Finland's intelligence legislation has been updated to the same level as in other European countries. The rest of this paper is divided as follows. Section 2 handles the overview of the theoretical framework. Section 3 proposes the central concepts of critical infrastructure and the framework of this article. Section 4 presents the research background, objectives, and methods. Section 5 presents the findings. Section 6 includes a discussion about the research area. Section 7 handles conclusions.

2. Theoretical framework and literature review

Member countries of the European Union and smart cities need cooperation because, without smart cities, the European Union's intelligent ecosystem cannot be created. Financial competition between countries creates the need for the development of intelligent technology. Thus, intelligent information systems are being developed; there must be an already digital ecosystem to connect the system. Every smart city should be constructed from a long-term view. A smart city needs an urban built technology-oriented environment where different kinds of intelligent systems communicate with each other. This case study aims to find out those fundamental technological-related risks that expose society to hybrid threats. These threats affect the protection of critical infrastructure and prevent the detection of threats. Implementation of the presented Hybrid Emergency Response Model is the primary purpose because there are separate situation centers, emergency response centers, and organizations fighting against cyber threats. Still, there is no common emergency response model for all kinds of hybrid-threats. The main author of this research has innovated the next-generation emergency response model (Simola & Rajamäki, 2017).

2.1 Development of Emergency Response system solutions

Emergency Response Center uses an Emergency Response system. It is one kind of decision support system. Decision support systems are used to track key incidents and the progress of responding units, optimize response activities and act as a mechanism for queuing ongoing incidents (Ashish et al., 2007; Endsley, 1988; Endsley, 1995).

In Finland, traditional emergency response functions have been modeled from other countries. However, we still have significant challenges related to the possibilities of transferring emergency data correctly and in time to the Emergency response center. There was a separate emergency response unit in the Police organizations until 1999. E.g., regional Radio Police consisted of their dispatch personnel who answered citizens' emergency calls and managed the use of emergency units to the site of an accident. Also, municipal rescue services handled their emergency calls. In the 21st century, separate emergency call units and functions were combined with emergency response centers. Very soon after the organization's changes, PPDR authorities found the need to manage their emergency resources. PPDR organizations established their situation centers to allocate emergency resources concerning field workers' cooperation.

The culture of the organization needs to be understandable when the purpose is to develop new technological solutions. Public safety organizations have a common working culture but also separate inner-organizational subcultures. That same issue concerning the meaning of the working culture relation to organizational reform also occurs in a different atmosphere and a different field. In practice, smart city infrastructure is the fundamental framework that governs minor factors inside it. It is impossible to create technological solutions in their separate entity regardless of the organizations' culture.

2.2 Smart nations and smart cities

Political power relations affect the national future of digitalization. Urbanization changes our lifestyle, and the digitized environment creates the base for the new safety culture. Citizens meet friends in public places, and they might go to the shopping center for shopping goods. Time has changed more dangerous; global terrorism has impacted people's behavior. Historical similarities between countries in northern Europe helps to understand the safety needs of neighboring countries. While separate European societies are evolving, societies are developing their cooperation on digitalization. It is essential to see the digitalization development of the north from the same perspective. There are different political aspects between European Union countries concerning energy and security policy. EU as the commercial operator brings its own needs into the discussion. Collaboration with Russian and China challenges our culture and western way of thinking. We need cooperation, but possibilities for cybersecurity threats emerge too often (Robertson & Riley 2018). Nord Stream2 and different kinds of 5G and cable projects may expose national security under cross-boarding hybrid risks (Buchanan, 2017; Shackelford et al., 2017; Buchanan, 2018; Hutchens, 2018).

It is impossible to create the entirety of a smart society without understanding the continuity management of society. If departments of the central government design separate digitalization projects without a common understanding of the future needs, society's expenses and digitalization management become complex. The governance of digitalization needs common goals for all participants. It means that the regional and local administrative operators need exact central steering concerning all municipal constructions of infrastructure.

3. Critical Infrastructure

The united states define critical infrastructure as physical or virtual systems and assets that are so vital that destructions of the above would have a crucial influence on security, national economic security, national public health, and safety, or any combination of those matters (The White House, 2013). According to the Secretariat of the Security Committee (2013), critical infrastructure comprises vital physical facilities, infrastructures, and electronic functions and services.

Critical Information Infrastructure comprises any physical or virtual information system that controls, processes, transfers, receives, or stores electronic information in any form, including data, voice, or video that is vital to the functioning of critical infrastructure (DHS 2011).

3.1 Fundamental elements of critical infrastructure in smart society

U.S Department of Homeland Security (2013) classifies 16 different sectors for the Critical Infrastructure as follows: “Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare, and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation Systems and Water Wastewater System” (DHS 2013).

Department of Homeland Security categorizes, e.g., the communication sector closely linked to the Energy sector, the Information sector, the Financial services, the Emergency services, and the Transportation system sectors (DHS, 2013). Every government uses a different emphasis level between the importance of emphases. In this research communication sector, the energy sector, information technology, and emergency services sector have been chosen as selected sectors of critical infrastructure.

3.2 Risk management and preparedness

According to (NIST, 2018) the framework is used in U.S. suites well also in Finland. The risk management framework consists of three elements of critical infrastructure (physical, cyber, and human) that are explicitly identified and should be integrated throughout the steps of the framework. The critical infrastructure risk management framework supports a decision-making process that critical infrastructure actors or partners collaboratively undertake to inform the selection of risk management actions. It has been designed to provide flexibility for use in all sectors, across geographic regions, and by various partners. It can be tailored to dissimilar operating environments and applies to all threats (DHS, 2013).

Figure 1: Critical Infrastructure Risk Management Framework

The risk management concept enables the critical infrastructure actors to focus on those threats and hazards that are likely to cause harm and employ approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to secure continuity of essential functions and services and support enhanced response and restoration (DHS, 2013).

According to the Department of Homeland Security (2013), the first point recommends setting infrastructure goals and objectives that are supported by objectives and priorities developed at the sector level. To manage critical infrastructure risk effectively, actors and stakeholders must identify the assets, systems, and networks that are essential to their continued operation, considering associated dependencies and interdependencies. This dimension of the risk management process should also identify information and communications technologies that facilitate essential services (DHS, 2013).

The third point recommends assessing and analyzing risks. Those Risks may comprise threats, vulnerabilities, and Consequences. A threat can be a natural or human-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. The vulnerability-based risk may occur physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. A consequence can be the effect of an event, incident, or occurrence. Implementing risk management activities means that decision-makers prioritize activities to manage critical infrastructure risk based on the criticality of the affected infrastructure, the costs of such activities, and the potential for risk reduction. The last element measuring effectiveness means that the critical infrastructure actors evaluate the effectiveness of risk management efforts within sectors and at national, state, local, and regional levels by developing metrics for both direct and indirect indicator measurement (DHS, 2013).

In this research, we have used a modified combination of NIST and Octave Allegro Risk Assessment Frameworks. According to Caralli & al. (2007), Octave allegro is a strategy for prioritizing and sharing information about security risks, e.g., information technology. According to (Zio & Pedroni, 2012) NASA risk-informed risk is the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements. As Figure 2 illustrates, Risk Management by NASA integrates two complementary processes, Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM), into a single coherent framework. The RIDM process addresses the risk-informed selection of decision alternatives to assure effective approaches to achieving objectives, and the CRM process addresses the implementation of the selected alternative to ensure that requirements are met. These two processes work together to assure effective risk management as NASA programs (NASA, 2015).

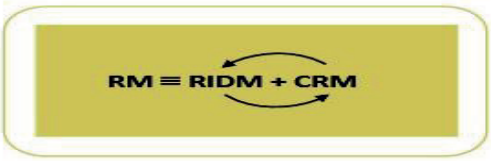


Figure 2. Combined risk management processes.

3.3 Protecting vital society

According to (The Security Committee, 2018; Ministry of defence, 2010), threats can occur on the individual, national, and global levels. Individual threats primarily affect the individual, national threats primarily affect the state, society and population, global threats affect the earth and the population's future security. Figure 3 illustrates those levels relations. According to the Ministry of the Interior (2018) three top-level threat scenarios are severe disturbances in the power supply and cyber threats like severe disturbances in the telecommunications and information systems. Vital functions to the Finnish society contain the management of Government affairs, international and EU activities, Finland's defence capability, internal security, the functioning of the economy, infrastructure and security of supply, functional capacity of the population and services and psychological resilience to a crisis (Ministry of the Interior, 2018).

Figure 3: Threats on the individual, national, and global level

3.4 Artificial Intelligence helps continuing management

Artificial Intelligence (AI) is a part of the system that displays intelligent behavior by analyzing their environment and taking multiple actions with autonomy to achieve given purposes. Software-based artificial intelligence systems can act in the virtual world consisting of image analysis software and search engines. Also, it may be embedded in hardware devices, e.g., advanced robots, unmanned vehicles, or Internet of Things applications (European Commission 2018).

An intelligent Agent (IA) is an entity that produces decisions. It allows performing, e.g., specific tasks for users or applications. It can learn during the process of performing tasks. Two main functions consist of perception and action. Intelligent Agents form a hierarchical structure that comprises different levels of agents. A so-called multi-agent system consists of several agents that interact with one another (Wooldridge 2009). That combination may solve challenging problems in society. The agent may behave in three ways: reactively, proactively, and socially (Wooldridge 2009).

4. Research background, objectives, and methods

There have been many state-level discussions concerning digitalization among decision-makers in media. At present public safety authorities and decision-makers do not use cyber-threat information in their operative daily routine almost at all. The challenge is that public safety authorities have separate cybersecurity organizations in their administrations. Organizations that have responsibilities for cybersecurity operations act as separated entities from PPDR services. As a part of TRAFICOM, the National Cyber Security Centre Finland (NSCS-FI) produces and shares cyberthreats information for stakeholders. Still, shared data does not achieve emergency response centers or situation centers. Separate organizational cybersecurity functions, methods, and procedures prevent an effective response to cyber-physical threats. In addition to this, developed innovations, e.g., emergency response systems, are all useless if our ministers and other decision-makers are not faithful or decisions are made to advantage a foreign power. It is essential to realize the source and degree of threat. The innovative urban areas and information systems may be constructed on an unstable ground level that may consist, e.g., energy supply solutions and dicey communication equipment. Overall situational awareness enhances by combining Open Source Intelligence data and traditional intelligence data (Morrow and Odierno 2012). The cyber situational picture is needed because Hybrid threats need hybrid responses.

4.1 Method and Process

The multimethodological approach consists of four case study research strategies: theory building, experimentation, observation, and systems development (Nunamaker & al., 1990). Yin (2014) identifies five components of research design for case studies: (1) the questions of the study; (2) its propositions if any; (3) its unit(s) of analysis; (4) the logic linking the data to the propositions; and (5) the criteria for interpreting the findings. This research is carried out with the guidance of Yin (2014). The research concentrates on sources of scientific publications, collected articles and literary material. The research subject comprises public safety organizations, procedures, and vital functions of Finland society.

The first purpose of this qualitative research was to collect and classify selected risks from different risk areas. In this research, we have used the Modified Risk Assessment Framework. The second purpose was to find out hidden technological-related state-level risks and challenges that are outside the official risk classification. A simple process model helps to identify those fundamental factors that are used in the creation of the scenarios. We have defined the research area concerning vital functions in four main sections; the Emergency services sector, the Communication sector closely linked to the Energy Sector, and the Information sector. Firstly, it is essential to find out technological-related risks and scenarios that expose society's vital functions to hybrid-threats and risks. It is easier to detect fundamental level risk factors when basic threats and risks are categorized and classified. These threats affect the protection of vital functions and prevent the detection of threats. We have used a combination of different methodologies to find out those factors that affect decision-making in society. As Table 1 illustrates, separate risks are divided into the main areas as follows: Administrative risks, conflict risks, emergency functions related risks, socioeconomic risks and infrastructure-related risks. The numbers A, B, C, D, and E indicate which main category the subcategories are also linked. Separate risks are categorized and ranked on a three risks level process. The first measure is valued "frequency of the phenomenon" (1 = phenomenon does not occur every year, 2 = phenomenon occurs yearly, and 3 = a phenomenon is permanent). The second value is titled "predictability and measurability of risks" (1= phenomenon is neither predictable nor measurable, 2= phenomenon is predictable. 3 = phenomenon is predictable and measurable.) The third value is named "impact of risk on overall security" (1= impact of the risk on one vital function, 2=impact of the risk on two to three vital functions, and 3 = impacts of risk to more than three selected vital functions.) Coefficients for variables are 1 to "frequency of the phenomenon," 2 to predictability and measurability of risks, and 3 to "Impact of risk on overall security.

Table1: Main risk classification

Main risk classification and subcategories								
A		B		C		D		E	
Aministrative risks		**Conflict risks**		**PPDR services and functions related risks**		**Sosioeconomic risks**		**Infrastructure related risks**	
Problems in local continuity management	C,D	**Cyberattacks**	A,C,E	**Overloaded Emergency management system**	B,E	**Unemployment**	A	**Structural problems in the built urban area**	A,B,C
Problems in cooperation between decisionmakers	B,C,D,E	**Human made disasters or pandemia**	E	**Lack of human resources in PPDR services**	A,D,E	**Refugees**	A,B	**Structural problems in the rural area**	A,B,C,D
Separate municipal activities	E	**Cross-border radiation**	C,D,E	**Lack of resources in PPDR services/**	A,D,E	**Cultural change**	A	**Recovery problems**	A,B,C,D
Organizational problems	B,C,	**Physical war**	A,C,D,E	**Emergency event**	D,E	**Use of substances**	B,C	**Secrets cyber influences**	A,B,C,D
Leadership problems in government	B,C,D,E	**Hybrid warfare**	A,C,D,E	**Resource awareness of volunteers**	A,D,E	**Citizens poverty**	A	**Communicatio n problems**	A,B,C
						Unidentified people	A,B,C,E		

The research aims to create a decision support subsystem solution for the proposed Hybrid Emergency Response system to assist politicians and public sector actors. That is an important issue because there is a need to detect sources of threats much earlier.

We have used the methodology model and framework by the National Aeronautics and Space Administration In designing the subsystem of Hybrid emergency response systems. The continuous Risk Management (CRM) process stresses the management of risk during implementation. The Risk-Informed Decision Making (RIDM) methodology is part of a systems engineering process that emphasizes the proper use of risk analysis in its broadest sense to make risk-informed decisions

that impact all mission execution domains, including safety, technical, cost, and schedule. RIDM helps ensure that decisions between alternatives are made with an awareness of the risks associated with each helping to prevent late design changes, which can be key drivers of risk and cancellation (NASA, 2016).

Figure 4 illustrated the risk analysis framework that helps to analyze the different alternatives and factors when decision-makers are making final decisions (Dezfuli et al.,2010; Zio and Pedroni, 2012).

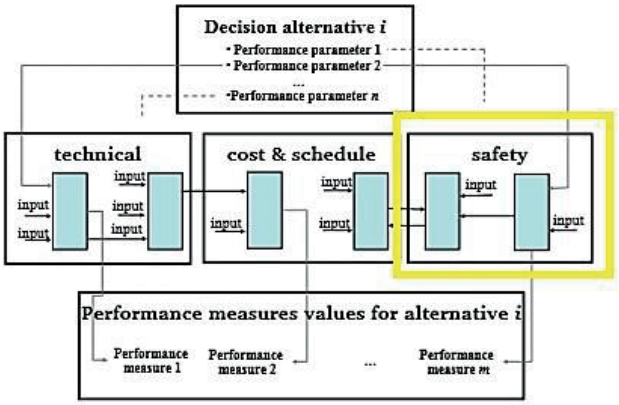


Figure 4: Risk analysis framework

The study's main goal is to find out fundamental societal factors that affect the effective protection of critical infrastructure. This research divides the types of risks into four sections. Ground Level indicates fundamental risks with scenarios that include factors, events, and actions of society. The scenarios' essential factors put all other societal factors, events, or actions into secondary threats level. Fundamental factors also make it possible to realize lower-level threats. This causes that the effective protection of critical infrastructure depends on external factors. The operator who controls external factors also dominates critical infrastructure. Therefore fundamental ground-level risk factors should be recognized and minimized.

5. Findings

Table 2 illustrates elements of society between risk levels. Higher risk levels are on the right, and these elements set the greatest threats to the vital functions. If ground-level threats are realized, the protection of critical infrastructure loses its meaning. E.g., the wide use of substances may indirectly harm society's overall security, but addiction cannot remain hidden for a long time. As a member of the EU, Finland gave away part of the national parliaments' sovereignty concerning national regulation. This kind of problem may happen when supranational legislation gives away the power of decision-making from the government to the commercial operators. E.g., change of ownership of the electricity transmission network.

Table 2: Classifications and impacts of risks

Classified by effetiveness of fundamental hidden risks and scenarios (red level) – Impacts and disruption on selected scenarios and consequences. Level of risks based on three values (frequency of the phenomenon, predictability and measurability of risks and impact of risk on overall security).
Impact level 1-3 (1 =low, 2=average level, 3=high impact) 1 = impact on 1-2 scenarios, 2 = impact on 3-4 scenarios, 3 =impact on 5-6 selected scenarios.
1 = X, 2 = XX, 3 = XXX

Classified basic risk levels. 1= low 4 =high	1		2		3		4	
	levels 6-10 –1		levels 11-13 –2		levels 14-16 –3		levels 17-18 – 4	
	Refugees	X	Overloaded Emergency management system	XX	Structural problems in the rural area	XX	Cyberattacks	XXX
	Cultural change	X	Lack of resources in PPDR services/	XX	Human made disasters or pandemia	XX	Separate municipal activities	XXX
	Use of substances	X	Resource awareness of volunteers	X	Structural problems in the built	XXX	Secrets cyber influences	XXX
	Unemployment	X	Emergency event	X	Leadership problems in government	XXX	Hybrid warfare	XXX
			Cross-border radiation	X	Lack of human resources in	XX	Unidentified people	XXX
			Organizational problems	XX	Communication problems	XXX		
			Problems in local continuity management	XX	Problems in cooperation between decision makers	XXX		
			Citizens poverty	X	Recovery problems	XXX		
					Physical war	XXX		

Findings indicate that lower-level risks of critical infrastructure do not cause problems to the ground-level risks. Higher-level risks also indicate structural governance problems in society. The effectiveness level indicates threats' impacts to the vital functions. Three x means that basic independent level risk becomes more dangerous due to connection ground level scenarios. As Table 3 illustrates, six scenarios were selected. At which impact level selected risks to affect to potential consequences of the scenarios? As illustrated in table 1 one X indicate impact on 1-2 scenarios, XX indicate impact on 3-4 scenarios, XXX = indicate impact on 5-6 selected scenarios. If higher (4) level risk support 4 or more scenarios and consequences, impact level is occasional for all vital functions. The domino effect causes this change of situation. E.g., a separate cyberattack is not so dangerous, but the event's danger will essentially change if it is due to a political decision.

Table 3*:* Scenarios and consequences (The table has been changed to match the original table of the research)

Ground-level – Scenario	Consequences
A) Legislation – Lack of possibilities to intervene in internal security	Lack of internal self-determination and internal sovereignty
B) Political decisions – Lack of continuity	Line changes in security policy - development of unstable decision-making culture
C) Energy solutions – Dependence on imported energy management, short-term political purposes	Exposure to extortion by an external actor
D) Equipment for Communication systems – E.g., 5g solutions devices, network equipment.	Foreign state spying and foreign country get a role in infrastructure
E) International public projects - Smart cable projects, gas pipeline projects	Vulnerability to sabotage - the foreign state may use cables and pipelines for hybrid influencing
F) Decision-makers credibility- corruption, discrimination, criminal contacts to foreign state	Ability to prevent disturbances will decrease. National overall security and resilience level decreases. As a result, management of overall security becomes uncontrollable**.**

Threats like severe disruptions to a power supply, severe disruptions to telecommunications and information systems risks are noticed in Finland's security strategy for society report. Still, the same fundamental risk types occur as the causes that have not been considered in decision-making.

6. Discussion

In Finland, existing solutions for public operators based on outdated technology and systems' life-cycles are short (DHS, 2018). Currently, the victim of an accident may have to wait long for the emergency response center's response because call center personnel have to exercise how the new Emergency Response Center system works (Saarenpää J. & Virtanen V. 2019). The handling of incoming and outgoing phone calls will lengthen.

Development towards the digital ecosystem starts with cultural understanding and process management. The subcultures of different PPDR authorities should be implemented through systems. Currently, all actors have their own separate operating model. E.g., if a complete emergency response system requires a significant additional workforce, designing has failed. Technological opportunities have not been exploited in Finland, such as in the U.S. The introduction of an immature system on holiday does not reflect the understanding of the situation in the operating environment (Rahko, 2018). A fully automated emergency response center can be a reality within a decade. An automated decision support system for the highest decision-makers can be a reality soon because vital functions require proof of political decisions.

7. Conclusions

As discussed above, we cannot hide our history and culture, but if we are developing a cyber-secure smart ecosystem, we need to make changes to the decision-making culture. The research has been shown that different kinds of structural fundamental-level threats may occur before any classified threat has been illustrated. Engineers, architects, and designers cannot develop anything new concerning smart solutions if the ground base is weak. An unsecured platform causes fundamental obstacles to designing solutions for an intelligent society. Legislation set challenges to the national politicians and authorities, but also power relations between union countries.

The micro and macro levels will be encountered if a foreign state party intervenes to interfere with data traffic functioning in maritime areas. E.g., there is a northeast cable project designed to connect networking activities between different continents. Nowadays, the problem is that fiber optic and power supply are transmitted through the same cable. So-called unexpected happenings influence all ecosystems. This kind of threat comes true and happens out of public safety control. In the future, it is an occasional issue to find the right balance between national security and warm bilateral relations.

Vulnerabilities and risks have increased, though formally, the goal is to harmonize Eastern and Western data cable functionalities (Buchanan, 2018; Shackelford et al., 2017). The study shows that the most troublesome and most significant threats to national security and vital functions are related to human factors, that are based on politicians' decisions and political projects. It is challenging to anticipate national policy's real direction at the macro level because good inter-state relations may indicate ignoring security issues. The study suggests that artificial intelligence-based solutions should be used enhancing to support decision-making. The subsystem could also operate as a part of the next-generation emergency response model. This model will work in two ways. Firstly, the framework consists of predictive and preventive elements that react when cyber-threat data fusion produces signals through the AI-agents and sensors that activate actuators, e.g., bollards or evacuation systems in smart cities infrastructure. Secondly, the system will output handled data for the decision-makers as politicians. This dimension uses the method that connects small pieces of data into a big view producing the situational picture. At present, state-level political decision-making culture may prevent the proposed smart hybrid emergency model's utilization and usefulness. Decision-makers of Finland need to consider if fundamental risk factors are not recognized, technical early warning solutions become useless.

References

Ashish, N., Kalashnikov, D. V., Mehrotra, S., Venkatasubramanian, N., Eguchi, R., Hegde, R., & Smyth, P. (2007). Situational awareness technologies for disaster response. In H. Chen, E. Reid, J. Sinai, A. Silke & B. Ganoz (Eds.), Terrorism informatics: Knowledge management and data mining for homeland security. Springer.

Buchanan, E. (2017). "From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and what to do about It." 96 (2).

Buchanan, E. (2018) Sea Cables in the Thawing Arctic. Lowy Institute, last modified 01.02.2018, accessed 20.08.2018, https://www.lowyinstitute.org/the-interpreter/sea-cables-thawing-arctic.

Caralli R. A., Stevens, J. F., Young, L. R., Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technical report. U.S. Software Engineer Institute. Carnegie Mellon University

DHS, (2011). Blueprint for a Secure Cyber Future – The Cybersecurity Strategy for the Homeland Security Enterprise

DHS, (2013). NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience.

DHS, (2018). Office of Emergency Communications: Cyber Risks to Next Generations 9-1-1.

Dezfuli, H., Stamatelatos M., Maggio G., Everett C., & Youngblood R. (2010). NASA Risk-Informed Decision Making Handbook: Office of Safety and Mission Assurance NASA Headquarters.

Endsley, M. R. (1988). "Design and Evaluation for Situation Awareness Enhancement. "Human Factors Society.

Endsley, M.R. (1995). "Toward a Theory of Situation Awareness. Human Factors." (37): 32-64.

European Commission (2018) Artificial Intelligence for Europe 237.

Hutchens, G. 2018 "Huawei Poses Security Threat to Australia's Infrastructure." The Guardian, last modified 30.10.2018, accessed 28.02.2019, https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says.

Ministry of Defence. (2010). Security strategy for society, government resolution. Helsinki: Ministry of Defence.

Ministry of the Interior. (2018). National Risk Assessment 2018. Helsinki: Ministry of the Interior.

Morrow, J., & Odierno, R. (2012). Open-source Intelligence, ATP 2-22.9, army techniques publication. Washington: Headquarters, Department of the U.S. Army.

NASA. (2015). Considering Risk and Resilience in Decision-Making. Hampton, Virginia: National Aeronautics and Space Administration.

NASA. (2016). Systems engineering handbook. Washington. National Aeronautics and Space Administration.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity: National Institute of Standards and Technology.

Nunamaker Jr. J., Chen M. & Purdin, T. (1990). Systems development in information system research. Vol 7 (3), 89–106.

Rahko, P. (2018) Uusi tietojärjestelmä otettiin käyttöön Oulun hätäkeskuslaitoksessa onnistuneesti, paikalla oli yöllä lähes kaksinkertainen henkilömäärä. Kaleva.

Robertson, J. and Riley, M. (2018) "The Big Hack: How China used a Tiny Chip to Infiltrate U.S. Companies?" Bloomberg, last modified 4.10.2018, accessed 2/28, 2019, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Saarenpää J. & Virtanen V. (2019) Erica-hätäkeskustietojärjestelmä Käyttöönoton vaikutukset poliisin päivittäiseen kenttätoimintaan.

SIA. (2017). Turku stabbings on 18 August 2017/ Puukotukset Turussa, Safety Investigation Authority, Helsinki 18.8.2017

Secretariat of the Security Committee. (2013). Finland's Cyber Security Strategy - Government Resolution: Ministry of Defense.

Shackelford, S. J., Sulmeyer M., Graig Deckard, A. N., Buchanan, B. & Micic, B. (2017). From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and what to do about It. 96 (2): 321-337.

Simola J. & Rajamäki J. (2015) "How a real-time video solution can affect to the level of preparedness in situation centers," 2015 Second International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM), Lodz, 2015, pp. 31-36, doi: 10.1109/CSCESM.2015.7331824

Simola, J. & Rajamäki, J. (2017). "Hybrid Emergency Response Model: Improving Cyber Situational Awareness." University, College, Dublin, Ireland, APCI, 29-30 June.

Simola, J. (2020). Privacy issues and critical infrastructure protection. In: V. Benson and J. McAlhaney, eds, Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, pp. 197-226.

The Security Committee. (2018). Security Strategy for Society. Helsinki: The Security Committee.

The White House. (2013). Federal register – Improving Critical Infrastructure Cybersecurity

Wooldridge, M. (2009) An Introduction to Multiagent System, 2 ed. John Wiley & Sons, United States.

Yin, R. K. (2014). Case Study Research, Design and Methods. 5th ed. Thousand Oaks: Sage Publications.

Zio, E. and Pedroni, N. (2012). Risk-Informed Decision-Making Process. Toulouse, France: Foundation for an Industrial Safety Culture.

VI

LITERATURE REVIEW OF THE SCIENTIFIC ARTICLES ABOUT CYBER INFORMATION SHARING

by

Jussi Simola, 2021

Journal of Information Warfare vol 20

https://www.jinfowar.com/sites/default/files/Literature%20Review%20of%20Scientific%20Articles%20about%20Cyber%20Information%20Sharing.pdf

Literature Review of Scientific Articles about Cyber Information Sharing

J Simola

Laurea Univerisity of Applied Sciences
RDI Espoo, Finland
University of Jyväskylä, Finland

Email: jussi.hm.simola@jyu.fi

Abstract: *This literature review presents a review of cyber information sharing based on systematic queries in four scientific databases. Hundreds of articles were handled and clustered. Relevant publications concerning cyber information sharing are succinctly described in the paper. The findings are discussed from the perspective of how to develop a cybersecurity information sharing system and what possible features might be included in the system. The literature review will comprise a new database for the Echo Early Warning System (E-EWS) concept. E-EWS aims at delivering a security operations support tool, enabling the members of the ECHO network to coordinate and share information in near real-time.*

Keywords: *CIP, Cyber-Ecosystem, Emergency Response, E-EWS, Cyber Information Sharing*

Introduction

This research belongs to the European network of Cybersecurity centres and competence Hub for innovation and Operations project (ECHO), which is part of the Horizon2020 program. The ECHO consortium consists of several partners from different fields and sectors including: health, transport, manufacturing, ICT, education, research, telecom, energy, space, healthcare, defence, and civil protection. The main objective of the ECHO is to strengthen the proactive cyber defence of the European Union. The literature review aims to gather essential scientific articles and official materials about cyber information sharing models. The literature review is based on systematic queries in different kinds of databases, such as IRIS. The findings will be discussed from the perspective of the added value that the review will offer to the stakeholders. The literature review will comprise a new database for the Echo Early Warning System (E-EWS) concept. E-EWS aims at delivering a security operation support tool, enabling the members of the ECHO network to coordinate and share information in near real-time. Within the E-EWS, partners of ECHO can retain their fully independent management of cyber-sensitive information and related data management. The early warning system will work as a parallel part of other mechanisms in the Public Protection and Disaster Relief environment. The development of the E-EWS will be rooted in a comprehensive review of information sharing and trust models from within the cyber domain. The literature review will present occasional scientific literature and official materials concerning information sharing between partners and stakeholders.

How to share sensitive data between stakeholders? What kind of information sharing-solutions already exist? The literature review is going to answer these questions as well.

Background

Modern infrastructures include not only physical components but also hardware and software. These integrated systems are examples of Cyber-Physical Systems (CPS) that integrate computing and communication capabilities with monitoring and control of entities in the physical world. In CPS, embedded computers and networks monitor and control the physical processes. Cyber-Physical Systems enable next-generation 'smart systems', such as advanced robotics, computer-controlled processes, and real-time integrated systems (Lee & Seshia 2015; Hevner & Chatterjee 2010).

There are separate cyber threat functions at the national and EU levels. Lack of synergy and separated functionalities concerning artificial intelligence solutions produce more potential vulnerabilities for vital functions. Therefore, it is important to develop functionalities in the ecosystem and to gather relevant data for the next generation's early warning solutions.

The content of the literature review is divided as follows. After the introduction, the next section handles shared situational awareness and cybersecurity information sharing. 'Base for the Research' covers methodologies used and the literature review process of the research. The next section discusses the overview of the findings. The last section presents conclusions.

Shared Situational Awareness and Cybersecurity Information Sharing

This section covers the notions of 'shared cyber situational awareness' and 'cybersecurity information sharing'. It aims to provide a theoretical framework and to limit the area of the literature study. It defines what to share, how to share, and with whom to share cybersecurity information. Shared (cyber) situational awareness is closely related to (cybersecurity) information exchange, because, without trusted information sharing, common situation or situational awareness is insufficient. The importance of this common situational awareness can be seen in a variety of areas. For example, public safety actors such as European law enforcement agencies need a common shared situational picture for the cross-boarding of tasks so that operational cooperation is based on a reliable platform.

According to Endsley and Robertson (2000a), good team situational awareness is dependent on team members understanding the meaning of the shared information. This means that teams need to share pertinent data and a higher level of situational awareness (Endsley & Robertson 2000a, 2000b). Bolstad and Endsley (2000) write that the development of shared situational awareness consists of four factors: 1) shared SA requirements (team members' ability to understand which information is needed by other team members); 2) shared SA devices (communications); 3) shared SA mechanisms (shared mental models); and 4) shared SA processes (effective team processes for sharing relevant information) (Bolstad & Endsley 2000). According to Munk (2018), cooperation between cybersecurity organisations is based on the effective and efficient exchange of information. Information interoperability is the joint capability of different actors—such as persons, organisations, and groups—necessary to ensure the exchange and common understanding of the information needed for their success (Munk 2018).

The Basis for the Research

In case of a hybrid incident, how can response and procedures be improved? Humans are not as good as automation at quickly and consistently processing large volumes of data. Flexible auton-

omy should provide a smooth, simple, seamless transition of functions between humans and the system (Endsley 1988). The target audience covers the ECHO partners, including several research organisations, large enterprises, industrial actors, and EU agencies across the countries. Clearly, a common platform for creating common cyber situational awareness is needed.

The fundamental needs concerning information sharing among ECHO partners are the basis for this research. The research question of the literature review is 'What are the main features of cyber exchange models?'. Collected materials are based on scientific literature, research articles, and official publications. The following scientific databases have been used: database of the JYKDOK library at the University of Jyväskylä (wide database concerning cybersecurity that provides access to resources such as the IEEE Xplore); the IEEE Xplore library (provides web access to more than 4.5 million documents from publications in computer science and to about 200 journals and about 1700 conference proceedings); Springer link (a database area of engineering that contains 17,000 books); and AI—a tool called IRIS, which is a search engine based on 100 entered keywords. The qualitative analysis was made by using traditional half-manual processing and Glue (Orange3) Python to explore the collected databases.

Search queries

In each case, the search queries such as 'cybersecurity information sharing' were entered, with no temporal limitation. A query without quotation marks returns some variations where the search engine allows for permutations and inflections. The so-called Artificial Intelligence tool IRIS returns wider variations, but the search engine works well. The author had to use quotations in some queries because some combinations made the searches too comprehensive.

As an initial screening, titles and abstracts have been read and the number of clusters has been identified. The selected list of groups can be regarded as a universal description of the research area. There were four main tasks of the research:

- Identify existing early warning systems and frameworks within public safety organisations;
- Identify information sharing models and governance models in private and public safety organisations;
- Identify features of cyber exchange model—for example, best practices and defensive measures;
- Classify phenomena, such as events, incidents, vulnerabilities, threats, and others.

Following the initial analysis method, a review form is an iteratively relevant aspect of the research. The aim is to cover the most relevant aspects of cyber information sharing models. Classification areas were used after the initial screening (an independent classification apart from the title, authors, or other text fields). Selected areas are solution area of results, threats and types of cybersecurity-related information, proposals, models, artefacts, and experiments/technology.

As noted above, findings create the fundamental database for the E-EWS, which is based on the framework of CPS (Cyber-Physical System). ECHO EWS will deliver a secure sharing support tool for personnel to coordinate and to share information in near real-time. It will support information sharing across organisational boundaries, will provide the sharing of general cyber information as

a reference library, will ensure secure connection management from clients accessing the E-EWS, and will combine different kinds of functions required in the management of information sharing functions—including sector-specific cyber-sensitive data. Thus, it concerns the whole ecosystem.

The systematic literature review sources

After defining the search queries, the initial search in Springerlink returned 1612 results for 'cyber-security information sharing' within content computer science, and it returned 31 researches with a quotation as **Table 1**, below, illustrates. Sharing technologies without the word 'cybersecurity' returned 517 results Features of cyber information sharing models without quotations returned 279 results.

Item Title	Authors	Publication Title	Year
Network Externalities in Cybersecurity Information Sharing Ecosystems	Z Rashid, U Noor, J Altmann	Economics of Grids, Clouds, Systems, and Services	2019
Risk Management Using Cyber-Threat Information Sharing and Cyber-Insurance	D Tosh, S Shetty, S Sengupta, JP Kesan, CA Kamhoua	Game Theory for Networks	2017
Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection	A Mermoud, M Keupp, S Ghernaouti, D David,	Critical Information Infrastructures Security	2017
Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance	DK Tosh, I Vakilinia, S Shetty, S Sengupta, CA Kamhoua, L Njilla, K Kwiat	Decision and Game Theory for Security	2017
Distributed, Collaborative, and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems	J Lane Thames	Cloud-Based Design and Manufacturing (CBDM)	2014
Toward a Safer Tomorrow: Cybersecurity and Critical Infrastructure	S Karchefsky, R Rao	The Palgrave Handbook of Managing Continuous Business Transformation	2017
IoT: Privacy, Security, and Your Civil Rights	CD Mares	Women Securing the Future with TIPPSS for IoT	2019
Part 2: Legal and Regulatory Framework	RH Weber, D Staiger	Transatlantic Data Protection in Practice	2017
Cybersecurity in the U.S.: Major Trends and Challenges	B Fonseca, JD. Rosen	The New US Security Agenda	2017
Cyber Attacks, Prevention, and Countermeasures	N Lee	Counterterrorism and Cybersecurity	2015
Regulation of Cyberspace and Human Rights	K Kittichaisaree	Public International Law of Cyberspace	2017
Toward a Holistic Approach of Cybersecurity Capacity Building through an Innovative Transversal Sandwich Training	J El Melhem, A Bouras,Y Ouzrout	Industry Integrated Engineering and Computing Education	2019
Frameworks and Best Practices	B Keys, S Shapiro	Cyber Resilience of Systems and Networks	2019
Economic Valuation for Information Security Investment: A Systematic Literature Review	D Schatz, R Bashroush	Information Systems Frontiers	2017
Main Initiatives to Safeguard Cyberspace Sovereignty	B Fang	Cyberspace Sovereignty	2018
Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?	G Christou	Cybersecurity in the European Union	2016
Learning Quasi-Identifiers for Privacy-Preserving Exchanges: A Rough Set Theory Approach	C Wafo SohL, L Njilla, KK. Kwiat, CA Kamhoua	Granular Computing	2018

Item Title	Authors	Publication Title	Year
IT-Security in Critical Infrastructures Experiences, Results, and Research Directions	U Lechner	Distributed Computing and Internet Technology	2019
Proposed Model for a Cybersecurity Centre of Innovation for South Africa	JJ van Vuuren, M Grobler, L Leenen, J Phahlamohlaka	ICT and Society	2014
Trends in Cyber Operations: An Introduction	F Lemieux	Current and Emerging Trends in Cyber Operations	2015
Cybersecurity in the U.S.	N Kshetri	The Quest to Cyber Superiority	2016
Sharing Cyber Threat Intelligence under the General Data Protection Regulation	A Albakri, E Boiten, R De Lemos	Privacy Technologies and Policy	2019
Vanishing Boundaries of Control: Implications for Security and Sovereignty of the Changing Nature and Global Expansion of Neoliberal Criminal Justice Provision	RP Weiss	The Private Sector and Criminal Justice	2018
International Cyberspace Governance	Chinese Academy of Cyberspace Studies	World Internet Development Report 2017	2019
The Role of Blockchain in Underpinning Mission Critical Infrastructure	H Jahankhani,S Kendzierskyj	Industry 4.0 and Engineering for a Sustainable Future	2019
Cyber Attacks, Prevention, and Countermeasures	N Lee	Counterterrorism and Cybersecurity	2013
Interpretation of the Concept of 'Cyberspace Sovereignty'	B Fang	Cyberspace Sovereignty	2018
Dark Web: Deterring Cybercrimes and Cyber-Attacks	FM De Sanctis	Technology-Enhanced Methods of Money Laundering	2019
Towards a Systematic View on Cybersecurity Ecology	W Mazurczyk, S Drobniak, S Moore	Combatting Cybercrime and Cyberterrorism	2016
More than Humans	S Iaconesi, O Persico	Digital Urban Acupuncture	2017
Digital Security – Wie Unternehmen den Sicherheitsrisiken des digitalen Wandels trotzen	A Weise	Digitalisierung in Industrie-, Handels- und Dienstleistungsunternehmen	2018

Table 1: Relevant Springerlink research publications

IEEE Xplore returned 147 results by using the following words: cybersecurity, information, and sharing altogether. Access was obtained to 129 files of data: Conferences (82), Journals (28), Magazines (16), Courses (15), Early Access Articles (3), and Books (2). Fifteen inessential IEEE Xplore courses were removed from the results, including results for Web Server & Web Application Security, Footprinting, and Network. Features of cyber exchange models returned 29 results. Information sharing returned 36 results and both 'cyber information sharing' and 'cyber information exchange' returned 5 results in which one was the same, as **Table 2** illustrates.

Document Title	Authors	Publication Title	Year
'Cybersecurity information sharing'			
A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)	F Sadique, K Bakhshaliyev, J Springer, S Sengupta	2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)	2019
Privacy-Preserving Cybersecurity Information Exchange Mechanism	I Vakilinia; DK Tosh, S Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017

Document Title	**Authors**	**Publication Title**	**Year**
A Coalitional Game Theory Approach for Cybersecurity Information Sharing	I Vakilinia, S Sengupta	MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)	2017
An Evolutionary Game-Theoretic Framework for Cyber-Threat Information Sharing	D Tosh, S Sengupta, C Kamhoua, K Kwiat, A Martin	2015 IEEE International Conference on Communications (ICC)	2015
Developing a Cyber Threat Intelligence Sharing Platform for South African Organisations	M Mutemwa, J Mtsweni, N Mkhonto	2017 Conference on Information Communication Technology and Society (ICTAS)	2017
'Cybersecurity information exchange'			
3-Way Game Model for Privacy-Preserving Cybersecurity Information Exchange Framework	I Vakilinia, DK Tosh, S Sengupta	MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)	2017
Attribute Based Sharing in Cybersecurity Information Exchange Framework	I Vakilinia, DK Tosh, S Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017
Privacy-Preserving Cybersecurity Information Exchange Mechanism	I Vakilinia, DK Tosh, S Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017
Structured Cybersecurity Information Exchange for Streamlining Incident Response Operations	T Takahashi, D Miyamoto	NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium	2016
A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)	F Sadique, K Bakhshaliyev, J Springer, S Sengupta	2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)	2019

Table 2: Specified IEEE returns

JYKDOC returned 9 results by using the following words: cybersecurity, information, and sharing together. Access was obtained to 9 files of data. Separate words cyber, exchange, and models returned 22 results. The term 'information sharing technologies' returned 268 results.

The AI tool IRIS requires the title of the research question and problem statement. The author has used the following words to describe the problem: "The research question of the literature review is 'What are the main features of cyber exchange models?' in order to capture a reasonably full range of the literature concerning the main features of cyber exchange models". Therefore, it was necessary to identify information sharing models and features of cyber exchange models. Early warning solution will deliver a secure sharing support tool for personnel to coordinate and to share information in near real-time, will support information sharing across organisational boundaries, will provide the sharing of general cyber information as a reference library, and will ensure secure connection management from clients accessing the early-warning system. The AI tool IRIS returned 270 results by using the following words in the title: cybersecurity, information, and sharing altogether, as **Figure 1** illustrates. The system calculates the relevance percentage for the results. All the results were between 78% and 95% relevant.

Figure 1: Identified papers by AI tool IRIS

Several studies were based on fundamental level public-related sources, which formed the main frame of the research. The most relevant public-related documents in this research are the following:

- Department of Homeland Security 2013, 'NIPP 2013: Partnering for critical infrastructure security and resilience', DHS, U.S.
- MITRE 2018, "Trusted Automated eXchange of Indicator Information — TAXII™ Enabling Cyber Threat Information Exchange".
- National Institute of Standards and Technology NIST 2016, *Guide to cyber threat information sharing*, *Special publication 800-150*, Tech. rep., Gaithersburg, MD, U.S.
- Johnson C, Badger M, Waltermire D, Snyder J, & Skorupka C, *Guide to cyber threat information sharing*, *Special publication 800-150*, Tech. rep. NIST, Gaithersburg, MD, US.
- OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017, *TAXII™ version 2.0. committee specification 01*, *OASIS Open*, Tech. rep. taxii-v2.0-cs01.
- OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017, *STIX™ version 2.0. part 2: STIX objects*, *OASIS open*, Tech. rep. stix-v2.0-wd03-part2-stix-objects.

As the results summarise, the information-sharing related models and frameworks are widely used among public safety organisations.

Findings

Cybersecurity information sharing architectures, frameworks, and models

There are few existing cybersecurity information sharing architectures and frameworks for the warning systems within public organisations divided into main groups. As the figure below illustrates, Mitre (2018) categorises information sharing models into three main models. The fourth model comprises a combination of the others.

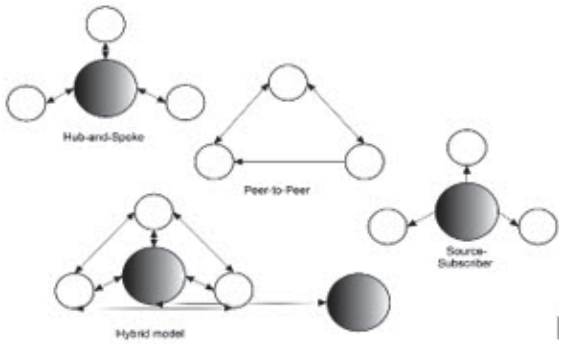


Figure 2 Traditional classification of information sharing models

- **Hub-and-Spoke**: Several data producers and consumers share information with each other; but instead of sending information directly, the information is sent to a central hub, which then handles dissemination to all the other spokes as appropriate. This model can be viewed as similar to email distribution lists, by which a sender provides a message to a mailing list service, which then forwards the message on to all list members.
- **Peer-to-Peer**: A group of data producers and data consumers organises direct relationships with each other. Members share directly with each other in a mesh pattern. The group may have a single governing policy, but all sharing exchanges are between individuals.
- **Source-Subscriber**: A single entity publishes information out to a group of consumers. This is a common model in commercial environments, where the data source is a vendor and the subscribers purchase access to the vendor's information. This is also a common model for free alerts from some authoritative source (Mitre 2018).

Despite the classification, many models are based on a hybrid structure. According to Sedenberg and Dempsey (2018), information sharing models can be divided into seven categories: government-centric; government-prompted—industry-centric; corporate—initiated-peer based (at the organisational level); small, highly vetted, individual-based groups; open-source sharing platforms; proprietary products; and commercialised services. Procedures and elements differ marginally from each other.

Government-centric is a centralised model, where one central organisation may share the information exchange or perform processing to enrich the data to others (NIST 2016; Meilin, Devine & Zhuang 2017). The Department of Homeland Security is one kind of hierarchical government-centric organisation. The central infrastructures use open, standard data formats and transport protocol (Meilin, Devine & Zhuang 2017).

Sector-Based Information Sharing and Analysis Centres (ISACs) are one kind of government-prompted, industry-centric sharing model. Centres are non-profit, member-driven organisations formed by critical infrastructure owners and operators to share information between government and industry. ISACs work through the National Infrastructure Protection Plan (NIPP) (Department of Homeland Security 2013). The National Cybersecurity and Communications Integration Centre (NCCIC) works in close coordination with all of the ISACs via the National Council of ISACs (NCI). They serve as collection and analysis points for private sector entities to share data on a peer-to-peer basis, to feed information into the federal government, and to provide a channel for federal information to flow out to the private sector. The purpose of Information Sharing and Analysis Organisations (ISAOs) is to gather, analyse, and disseminate cyber threat

information; but unlike ISACs, ISAOs are not sector-affiliated, and they are for any sector or community. ISAOs do not need to be part of the 16 critical infrastructures.

Corporate-initiated, peer-based groups are privately sponsored cybersecurity information sharing entities. These companies have undertaken their initiative without government intervention to coordinate information sharing. These information exchanges can be tailored to fit the specific needs of their members (Sedenberg & Dempsey 2018).

Individual-based groups are small online communities of peers that share sensitive information with the goal of immediate combat attacks. This kind of group requires a high degree of trust (Sedenberg & Dempsey 2018).

Open communities and platforms are open-source sharing platforms. For example, STIX indicators and open source intelligence feeds are examples of this kind of format. The Malware Information Sharing Platform (MISP) is a free, open-source platform developed by researchers from the Computer Incident Response Center of Luxemburg, the Belgian military, and NATO.

According to Sedenberg & Dempsey (2018), proprietary products and commercialised services consist of, for example, antivirus software and firewalls that disseminate cybersecurity information through software updates. Companies offering these products and services may participate in any of the other information exchanges to enhance the security of the small companies.

Features of Cyber-Threat Information Exchange Models

Automated Indicator Sharing (AIS) participants connect to a Department of Homeland Security-managed system in the Department's National Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of cyber threat indicators. A server housed at each stakeholder´s location allows each to exchange indicators with the NCCIC. Participants receive and can share DHS-developed indicators they have observed in their network defence efforts, which DHS will then share back out to all AIS participants (Department of Homeland Security 2015a).

Stakeholders who share indicators through AIS will not be identified as the source of those indicators to other participants unless they affirmatively consent to the disclosure of their identities. Senders are anonymous unless they want DHS to share them (Department of Homeland Security 2015a). Indicators are not validated by DHS, as the emphasis is on velocity and volume: their partners tell the DHS they will vet the indicators they receive through AIS. The Department's goal is to share as many indicators as possible as quickly as possible (Department of Homeland Security 2015a). The U.S. Government also needs useful information about indicators (Department of Homeland Security 2015b).

AIS utilises the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications for machine-to-machine communication (Department of Homeland Security 2015a). STIX is a language and serialisation format that enables organisations to exchange Cyber Threat Intelligence (CTI) in a consistent and machine-readable manner (Oasis 2017a). Trusted Automated eXchange of Intelligence Information (TAXII™) is an application layer protocol used to exchange Cyber Threat Intelligence (CTI) over the HTTPS (Oasis 2017b).

OASIS defines several STIX Domain Objects. 1. Attack Pattern is a type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets. 2. The campaign is a grouping of adversarial behaviours that describes a set of malicious activities or attacks that occur over time against a specific set of targets. 3. A course of action is an action taken to either prevent an attack or to respond to an attack. 4. Identities mean individuals, organisations, or groups, as well as classes of individuals, organisations, or groups. 5. The indicator means a pattern that can be used to detect suspicious or malicious cyber activity. 6. Intrusion Set is a grouped set of adversarial behaviours and resources with common properties believed to have been organised by a single entity. 7. Malware is a type of TTP (also malicious code and malicious software) used to compromise the confidentiality, integrity, or availability of a victim's data or system. 8. Observed Data means conveyed information observed on a system or network (for example, an IP address). 9. The report consists of collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details. 10. Threat actors are individuals, groups, or organisations believed to be operating with malicious purpose. 11. The tools are software that threat actors can use to perform attacks. 12. A vulnerability is a software-based error that a hacker can directly use to gain access to a system or network (Oasis 2017a).

Cybersecurity information sharing governance and mechanisms

As **Figure 3**, below, represents, collection-based communications describe the situation when a single TAXII client requests a TAXII server and the TAXII server carries out that request with information from a database. A TAXII channel in TAXII server enables TAXII clients to exchange information with other TAXII clients in a publish-subscribe model. TAXII clients can push messages to channels and can subscribe to channels to receive published messages. A TAXII server may host multiple channels per API root (Oasis 2017b). TAXII is the main transport mechanism for cyber threat information represented in STIX. Stakeholders may share indicators with DHS through an ISAC or an ISAO without TAXII client.

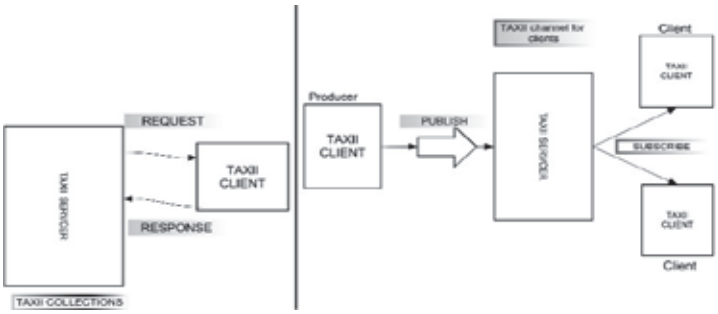


Figure 3: Flow of cyber threat information in TAXII

According to NIST (2016), cyber threat information is any information that may help an organisation identify, assess, monitor, and respond to cyber threats. Threat information is any information related to a threat that might help an organisation protect itself against a threat or detect the activities of an actor. Major types of threat information include the following:

- Indicators are technical artifacts or observables. Indicators can be used to detect and defend against threats. Indicators may consist of the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS)

domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message (NIST 2016).

- Tactics, Techniques, and Procedures (TTPs) describe the behaviour of an actor. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, a delivery mechanism (for example, phishing or watering hole attack), or exploit (NIST 2016).
- Security alerts, also known as advisories, bulletins, and vulnerability notes, are brief and usually readable technical notifications regarding, for example, current vulnerabilities. Security alerts originate from sources such as the United States Computer Emergency Readiness Team (US-CERT), Information Sharing and Analysis Centres (ISACs), the National Vulnerability Database (NVD), Product Security Incident Response Teams (PSIRTs), commercial security service providers, and security researchers (NIST 2016).
- Threat intelligence reports are generally prose documents that describe TTPs, actors, types of systems and targeted information, and other threat-related information that provide greater situational awareness to an organisation. Threat intelligence is threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes (NIST 2016).

Information sharing methodologies between Certs and Law Enforcement

Enhancing cooperation between EU member states and related Network and Information Security communities (NIS) as Certs is also a crucial part of the cyber-ecosystem. It is not enough that small, closed groups share information without synergy with public safety organisations.

The main goal of the Europol Information System (EIS) is to be the reference system for offenses, individuals involved, and other related data to support EU Member States, Europol, and its partners in their fight against organised cybercrime, terrorism, and other forms of serious crime. For example, the European Cybercrime Centre (EC3), as a part of Europol, uses an open-source MISP platform (DG Home Affairs 2014). A Malware Information Sharing Platform (MISP) is a tool for information sharing about malware samples and malicious campaigns related to specific malware variants. It offers architectural flexibility, allowing the utilisation as a centralised platform (for example, CIRCL and FIRST instances), but also as a decentralised (peer-to-peer) platform (ENISA 2015). According to Europol (2019), there is a need to develop new information management architecture and to continue improving operational capabilities and tools by focusing on automation and modernisation, for example, to continue automating the direct follow-up processes through SIENA for successful (self-) searches on Europol's and EU member states' data. There is also a need to harmonise further the Technical Infrastructure Capability including Identity and Access Management (IAM) landscape of Europol by integrating more IT-systems with IAM and taking further steps towards establishing a single enterprise identity, taking into account various networks and security standards, including IAM for Basic Protection Level (BPL) business solutions (Europol 2019).

SIENA is a VPN (Virtual Private Network) designed to enable a swift, secure, and user-friendly exchange of operational and strategic crime-related information and intelligence between member states, Europol, law enforcement cooperation partners, and public safety organisations (DG Home

Affairs 2014). SIENA has been used to allow the EU member states to communicate and to share intelligence information.

In the U.S., National Information Exchange Model (NIEM) is an XML-based partnership mechanism between the U.S. Departments of Justice (DOJ) and Homeland Security (DHS) and enables information sharing focusing on information exchanged among organisations as part of their current or intended business practices (Criminal Intelligence Coordinating Council 2013).

The Federal Bureau of Investigation (FBI) hosted InfraGard's Secure Web Portal, which allows secure messaging that promotes communication among members. Members give access to iGuardian, the FBI's cyber incident reporting tool designed specifically for the private sector. InfraGard membership also allows peer-to-peer collaboration across InfraGard's broad membership and information-sharing and relationship-building with FBI and law enforcement. InfraGard engages subject matter experts and addresses threat issues across each of the 16 critical infrastructure sectors recognised by Presidential Policy Directive-21 (PPD), the Department of Homeland Security (DHS), and the National Infrastructure Protection Plan (NIPP) (Department of Homeland Security 2013).

Digital Forensics XML (DFXML) is an XML language (Garfinkel 2012) intended to represent the following kinds of forensic data: metadata describing the source disk image, file, or other input information; detailed information about the forensic tool that did the processing (for example, the program name and where the program was compiled and linked libraries); the state of the computer on which the processing was performed (for example, the name of the computer; the time that the program was run; the dynamic libraries that were used) (Garfinkel 2012); the evidence or information that was extracted (how it was extracted, and where it was physically located); cryptographic hash values of specific byte sequences; and operating-system-specific information which is useful for forensic analysis (Garfinkel 2012).

The Cybersecurity Information Exchange Framework (CYBEX) will advance the development of automating cybersecurity information exchange. The CYBEX Forensics domain is an operation domain that supports law enforcement operations by collecting evidence. The necessary information for this operation is stored in the evidence database. CYBEX provides a framework for exchange information between a network mediation point and a law enforcement facility to provide an array of different real-time network forensics associated with a designated incident or event (Rutkowski *et al.* 2010).

CYBEX-P and the Privacy-Preserving Cybersecurity Information Exchange mechanism are modified from CYBEX and both are based on an information-sharing platform with a robust operational and administration structure. The Privacy-Preserving Cybersecurity Information Exchange mechanism enables the organisations to share their cybersecurity information without revealing their identities (Vakilinia, Tosh & Sengupta 2017). CYBEX-P platform addresses the inefficiency in dealing with cybersecurity problems by an individual entity. Real-time exchange of threat data helps organisations analyse threats to predict and to prevent future cyberattacks. There are three parties involved throughout the complete lifecycle of the threat data: 1) Client organisation; 2) CYBEX-P; 3) analysts and researchers. The client organisation acts as a source of threat data. It can be

any external or internal threat data source willing to share threat data with others. CYBEX-P works as the intermediary between all organisations and data analysts. Threat data may be machine-generated or curated by a security specialist (Sadique *et al.* 2019). The processing server in CYBEX-P has a TPM Trusted Platform Module (TPM). The TPM verifies the integrity of the software and hardware running in the processing server (Sadique *et al.* 2019).

Making Security Measurable (MSM), led by MITRE categorises heterogeneous information and standardises data formats and exchange protocols (MITRE 2013). MSM presents a comprehensive architecture for cybersecurity measurement and management, where current standards are grouped into processes and mapped to the different knowledge fields. MSM standards can be grouped into six major knowledge areas, each of which refers to a process (put in parentheses): asset definition (inventory); configuration guidance (analysis); vulnerability alerts (analysis); threat alerts (analysis); risk/attack indicators (intrusion detection); and incident report (management) (MITRE 2013).

In many cases, a fundamental structure of the information-sharing mechanisms does not differ significantly. It is, therefore, suitable to continue on this issue in the conclusions.

Conclusion

This literature review indicates that 'cybersecurity information sharing' is not precisely defined in the area of cybersecurity. As mentioned above, the structures of information sharing models are generally very sector-specific and are created in different environments. There is a need at the EU level to determine the development of a common Early Warning Solution. Usually, the word 'warning' also refers to preventive functions, as U.S. intelligence services operate. The fight against hybrid threats means not only preventing cyberattacks but also identifying, tracing, and prosecuting a criminal/criminal group. This means an even deeper integration of government systems in the future.

Relevant information from the site of a major hybrid incident must be directly shared with the national participants—for example, cybersecurity centres. It is relevant to allocate additional reliable data for determining discrepancies of limits. Combining pieces of information to ensure the correct and reliable information to be shared is of primary importance. The essential information should be processed to the desired shape for the participants. In the future, cyber defence operations will be more integrated and automated according to local capabilities, authorities, and mission needs. The shared common operational picture means that real-time communication links from the local level to the national and EU level exist. A common cyber situational awareness is needed for operating CPS and emergency and crisis management. There should be a connection between cyber situational awareness functions and emergency management.

When developing an early warning system at the EU level, it is important to account for three requirements: 1) the possibility that some EU member states may leave an early warning system (Edgington 2020); 2) the need to engage participants in the values of the western world (Tidey, Gill & Parrock 2020); and 3) the possibility of combining some elements of the Cyber Threat Warning System to NATO Cyber Situational Awareness Solutions. These factors have a direct link to sharing confidential information (Simola 2019, Ilves *et al.* 2016).

It is important to consider how national Cyber Security Centres cooperate with other organisations within critical infrastructure at the national level. The state departments of the United States work closely together in the fight against threats in the field of cybersecurity. The organisations of public administration in the European Union work together more formally. This is important to notice when cybersecurity expertise is being strengthened. The fundamental problems of the European community must be solved before permanent solutions can be built. While this does not prevent the development of operating models, this factor must be taken into account when developing new systems. Confidence between member states must be on a stable basis.

As Ilves *et al.* (2016) mention, there are no crucial barriers to increase collaboration concerning, for example, early warning solutions between the U.S., NATO, and the EU. According to Dandurand & Serrano (2013), for example, Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) provide a knowledge management tool for the NATO partners. The U.S. Cybersecurity Sharing Act and Europe´s directive on Network and Information Security (NIS) have similar goals. In addition to this, the EU and NATO signed a technical arrangement in 2016 to increase information sharing between the NATO Computer Incident Response Capability (NCIRC) and the EU Computer Emergency Response Team (CERT-EU) (Ilves *et al.* 2016). Common E-EWS solutions would create an effective way to respond to cross-boarding hybrid threat situations. All major companies whose businesses are related to critical infrastructure should be linked to an early warning system.

Before closer cooperation on information sharing can be achieved, legislation, bilateral agreements, data management standards, and certifications need to be brought to an acceptable level of privacy. The holder of the information is the winner in the smart society. Protecting privacy is also part of the Western tradition, as is crime prevention.

References

Bolstad, C & Endsley, M 2000, 'The effect of task load and shared displays on team situation awareness', *14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society*, Santa Monica, CA, US.

Criminal Intelligence Coordinating Council (CICC) 2013, *National criminal intelligence sharing plan; Building a national capability for effective criminal intelligence development and the nationwide sharing of intelligence and information*, Tech. rep. 2, CICC, US.

Dandurand, L & Serrano O 2013, *Towards improved cyber security information sharing requirements for a cyber security data exchange and collaboration infrastructure (CDXI)*, NATO CCD COE Publications, Tallinn, EE.

Department of Homeland Security (DHS) 2013, 'NIPP 2013: Partnering for critical infrastructure security and resilience', DHS, US.

——2015a, 'Automated Indicator Sharing (AIS)', viewed 1 July 2019 <https://www.us-cert.gov/ais>.

——2015b, *Automated Indicator Sharing (AIS) FAQ*, viewed April 2019, <https://www.uscert.gov/sites/default/files/ais_files/AIS_FAQ.pdf>.

DG Home Affairs 2014, *UINFC2 Project, Deliverable D.1.3: Law Enforcement Agents Requirements*, European Union.

Edgington, T 2020, *Brexit: All you need to know about the UK leaving the EU*, BBC News, viewed 20 September 2020, <https://www.bbc.com/news/uk-politics-32810887>.

Endsley, MR 1988, 'Design and evaluation for situation awareness enhancement', *Proceedings of the Human Factors Society 32nd Annual Meeting Human Factors Society*, Santa Monica, CA, US, pp. 97-101.

—& Robertson, M 2000a, 'Situation awareness in aircraft maintenance teams', *International Journal of Industrial Ergonomics*, no. 26, pp. 301-25.

—2000b, 'Training for situation awareness in individuals and teams', *Situation awareness analysis and measurement*, eds. M Endsley & D Garland, Lawrence Erlbaum Associates, Mahwah, NJ, US.

European Network and Information Security Agency (ENISA) 2015, 'Information sharing and common taxonomies between CSIRTs and law enforcement', ENISA, Heraklion, GR.

Europol 2019, 'Europol programming document 2019-2020', The Hague, NL.

Garfinkel, S 2012, 'Digital forensics XML and the DFXML toolset', *Digital Investigation*, vol. 8, pp. 161-74.

Hevner, A & Chatterjee, S 2010, *Design research in information systems theory and practice*, Springer, New York, NY, US.

Ilves, L, Evans, T, Cilluffo, F & Nadeau, A 2016, 'EU and Nato Global Cybersecurity Challenges', PRISM, NDU, vol. 6, no. 2.

Lee, E & Seshia, S 2015, *Introduction to embedded systems, A Cyber-Physical Systems approach*, 2nd edn., MIT Press, Cambridge MA, US.

Meilin, H, Devine, L & Zhuang, J 2017, *Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach: Cybersecurity information sharing. risk analysis*, John Wiley & Sons, Ltd, Hoboken, NJ, US.

MITRE Corporation 2018,'Trusted Automated eXchange of Indicator Information—TAXII™: Enabling cyber threat information exchange', Department of Homeland Security, viewed 5 July 2019, <https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf>.

—2013, 'A collection of information security community standardization activities and initiatives', viewed 1 July 2019, <https://makingsecuritymeasurable.mitre.org/about/index.html>.

Munk, S 2018, 'Interoperability services supporting information exchange between cybersecurity organisations', *Academic and Applied Research in Military and Public Management Science*, vol. 17, no. 3, pp. 131-48.

National Institute of Standards and Technology (NIST) 2016, *Guide to cyber threat information sharing, NIST Special Publication (NIST SP) 800–150*, NIST, Gaithersburg, MD, US.

OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017a, *STIX™ Version 2.0. Part 2: STIX objects, OASIS open*, viewed 20 January 2020, <https://oasis-open.github.io/cti-documentation/stix/intro>.

——2017b, *TAXII™ Version 2.0. Committee specification 01, OASIS open*', viewed 20 January 2020, <https://oasis-open.github.io/cti-documentation/taxii/intro>.

Rutkowski, A, Kadobayashi, Y, Furey, I, Rajnovic, D, Martin, R, Takahashi, T, Schultz, C, Reid, G, Schudel, G, Hird, M & Adegbite, S 2010, 'CYBEX - The Cybersecurity Information Exchange Framework (X. 1500)', *Computer Communication*, vol. 40, pp. 59-64.

Sadique, F, Bakhshaliyev, K, Springer, J & Sengupta, S 2019, 'A system architecture of cybersecurity information exchange with privacy (CYBEX-P)', *Proceedings of the 9th Annual IEEE Computing and Communication Workshop and Conference (CCWC)*, pp. 493-8.

Sedenberg, E & Dempsey, J 2018, *Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs*, viewed 20 September 2019, <https://arxiv.org/ftp/arxiv/papers/1805/1805.12266.pdf>.

Simola, J 2020, 'Comparative Research of Cybersecurity Information Sharing Models', *Information & Security: An International Journal*, vol. 43, no. 2 , pp. 175-95, viewed 20 September 2020, <https://doi.org/10.11610/isij.4315>.

Tidey, A, Gill, J & Parrock, J 2020, 'EU warns Turkey of quick sanctions if dialogue over Eastern Mediterranean drilling fails', *EURONEWS*, viewed 20 September 2020, <https://www.euronews.com/2020/10/02/eu-leaders-break-deadlock-over-belarus-sanctions>.

Vakilinia, I, Tosh D & Sengupta S 2017, 'Privacy-preserving cybersecurity information exchange mechanism', *Proceedings of the 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, pp. 1-7.

VII

COMPARING CYBERSECURITY INFORMATION EXCHANGE MODELS AND STANDARDS FOR THE COMMON SECURE INFORMATION MANAGEMENT FRAMEWORK

by

Jussi Simola, 2020

Chapter in the book titled Digital Transformation, Cyber Security and Resilience of Modern Societies

https://doi.org/10.1007/978-3-030-65722-2_9

Comparing Cybersecurity Information Exchange Models and Standards for the Common Secure Information Management Framework

Jussi Simola

University of Jyväskylä, Mattilanniemi 2, Jyväskylä, Finland
e-mail: jussi.hm.simola@jyu.fi

Abstract Cyber threats have increased inspite of formal economic integration int he world. Decision-makers and authorities need to respond to the growing challenge of cyber threats by increasing cooperation. Information is one of the main facilities when the objective is to prevent hybrid threats at EU level and between the western countries. The main purpose of the study is to find out separating and combining factors concerning existing cyber information sharing models and information management frameworks in western countries. The aim is also to find out crucial factors, which affect the utilization of a common Early Warning System for the ECHO stakeholders. The main findings are that unclear allocation of responsibilities in national government departments prevents authorities from fighting together against cyber and physical threats. Responsibilities for developing cybersecurity have been shared among too many developers. Operational work concerning cyber threat prevention between European public safety authorities should be more standardized, with more centralized information management system. When the purpose is to protect the critical infrastructure of society, public safety organizations in European Union member states need proactive features and continuous risk management in their information systems. The sharing of responsibilities for standardization concerning information management systems and cyber emergency procedures between authorities and international organizations is unclear.

Keywords Information sharing · Early warning · Standards · ECHO project

1 Introduction

The purpose of this paper is to support European ECHO Early Warning Solution developers, European politicians and end users but also provide features of existing information sharing models to identify and to take into consideration territorial, organizational, managerial, legal and societal dimensions of the existing information sharing solutions, models and frameworks. The research will comprise new database for the Echo Early Warning System concept. E-EWS aims at delivering a security operations support tool enabling the members of the ECHO network to coordinate and share information in near real-time. Echo Early Warning

System will provide a mechanism for EU partners to share incident and other cybersecurity relevant data to partners within the ECHO network.

The sub-research's question focused on how it is possible to integrate US-related cyber information sharing models to Europe. Within E-ECHO consortium, there is a need to protect information sharing, information management and practices. The purpose is to propose initial risk management framework for the common early warning system. There are territorial and cultural differences between The United States of America and European Union, but technological solutions create new kind of opportunities within EU member countries to reach the same situation as USA have concerning proactive intrusion detection systems. The research needs equivalences of the concepts and other variable factors in other territory—in the area of European Union.

USA is the main actor in the field of information exchange in the western world. Therefore it is important to notice information sharing frameworks and models that are already in use in global level. There are many similarities concerning legislation and technical solutions between the unions and organizations, but also differences. It is important to separate predictive and preventive purposes, because legislation differ between the countries. Despite of the formal legislative dimension, agencies of The United States of America has enough resources to act proactively and use predictive functions in cyber space. According to they have capability already and legislative implementation for the new cybersecurity features is under the progress. This research belongs to European network of Cybersecurity centres and competence Hub for innovation and Operations project, which is part of the Horizon2020 program. The rest of this paper is divided as follows. Section 2 proposes central concepts. Section 3 handles background of the cyber information sharing. Sections 4 handles legislation and regulation. Section 5 handles relevant standards. Section 6 presents Method and Process. Section 7 handles information sharing models and frameworks. Section 8 presents findings. Section 9 presents conclusion about the research.

2 Central Concepts

CERT (Computer Emergency Response Team)

An organization that provides incident response services to victims of attacks, including preventive services (i.e. alerting or advisory services on security management). The term includes governmental organizations, academic institutions or other private body with incident response capabilities.(European Union Agency for Cybersecurity (ENISA) [12]. The EU Computer Emergency Response Team (CERT-EU) was set up in 2012 with the aim to provide effective and efficient response to information security incidents and cyber threats for the EU institutions, agencies and bodies.

Critical Infrastructure protection (CIP) Critical Information Infrastructure Protection (CIIP)

Critical infrastructure refers to the structures and functions which are necessary for the vital functions of society. They comprise fundamental physical facilities and structures as well as electronic functions and services. Critical infrastructure (CI) includes Energy production, transmission and distribution networks, ICT systems, networks and services (including mass communication), financial services, transport and logistics, water supply, construction and maintenance of infrastructure, waste management in special circumstances. Transforming the nation's aging electric power system into an interoperable smart grid enabling two-way flows of energy and communications. That smart network will integrate information and communication technologies with the power-delivery infrastructure [4, 28] According to Secretariat of the Security Committee [39].

Critical Information Infrastructure means any physical or virtual information system that controls, process, transmits, receives or stores electronic information in any form including data, voice or video that is vital to the functioning of critical infrastructure. Those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy [32].

Cyber-Physical Systems (CPS)

Cyber-physical systems integrate computing and communication capabilities with monitoring and control of entities into the physical world. In CPS, embedded computers and networks monitor and control the physical processes. CPS are enabling next generation "smart systems" like advanced robotics, computer-controlled processes and real-time integrated systems [25].

Cyber Threats in Critical Infrastructure

These threats can be initiated and maintained by a mixture of malware, social engineering, or highly sophisticated advanced persistent threats (APTs) that are targeted and continues for a long period of time. Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications. According to National Institute of Standards and Technology [32], National Institute of Standards and Technology [34].

ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security [6].

Information Security Management System (ISMS)

An Information Security Management System (ISMS) describes and demonstrates an organization's approach to Information Security (and privacy management). It

includes how people, policies, controls and systems identify, then address the opportunities and threats revolving around valuable information and related assets.

The European Cyber Security Organisation (ECSO)

It represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public–Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

Information Exchange

According to ISO/IEC 27002 Information exchange should base on policies, procedures and agreements (e.g. non-disclosure agreements) concerning information transfer to/from third parties, including electronic information sharing (e.g., messaging).

Information Sharing and Analysis Centers (ISACs)

ISAC is collaboration community created for sector-specific national or international information sharing. Information Sharing and Analysis Centers are trusted entities to foster information sharing and good practices about physical and cyber threats and mitigation. The ISAC could support the implementation of new European legislation (e.g. NIS Directive) or support economic interests [7].

Information Sharing and Analysis Organization (ISAO)

An ISAO is any entity or collaboration created or employed by public- or private sector organizations, for purposes of gathering and analysing critical cyber related information in order to better understand security problems and interdependencies related to cyber systems to ensure their availability, integrity, and reliability [43].

North Atlantic Treaty Organization (NATO)

NATO is a 70 years old security alliance of 28 full member countries from North America and Europe. NATO's primary goal is to protect the Allies' security by political and military means. NATO is the principal security instrument of the transatlantic community.The security of North America and Europe are permanently tied together with allies. NATO enlargement has furthered the U.S. goal of a Europe whole, free, and at peace [42].

Risk Assessment Framework (RAF)

According to National Institute of Standards and Technology [35], the purpose of risk assessments is to inform decision makers and support risk responses by

(a) Identifying relevant threats to organizations or threats directed through organizations against other organizations;
(b) Identifying internal and external vulnerabilities;

(c) Impact to organizations that may occur given the potential for threats exploiting vulnerabilities and
(d) Likelihood that harm will occur. The result is a determination of risk.

Risk Management Framework (RMF)

Comprehensive risk management process by NIST, which Integrate the risk Management Framework into the system development lifecycle.

Standards ISO 27000 family

This family of 27000 standards provide fundamental bases for the definition and implementation of an Information Security Management System (ISMS) [31] (JRC TAXONOMY). The Security Measurement Index is based on ISO 27000 international standards and input from an advisory board of security professionals. It consists benchmarking tools for assessing organizations' security practices, a global assessment of IT and a basis for developing security measurement best practices to help make cybersecurity more effective and efficient [22].

Among ISO 27000 family, target audience comprise e.g. personnel of risk management. Personnel as skilled lead auditors are needed to grant certification [13].

Standard ISO/IEC 27010:2015 (ISO/IEC 2700 family)

Is a key component of trusted information sharing is a "supporting entity", defined as "A trusted independent entity appointed by the information sharing community to organise and support their activities, for example, by providing a source anonymization service" [18].

Tactics, Techniques, and Procedures (TTPs)

The behaviour of an actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower level, highly detailed description in the context of a technique (National Institute of Standards and Technology [33].

Threat Information

Any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations [33].

3 Cooperation Within the USA, NATO and EU

The Department of Homeland Security (DHS) is the U.S. Federal Government focal point of the U.S. cyber information-sharing ecosystem. It is responsible for the government's operational responses to major cybersecurity incidents, analyzing threats and exchanging critical cybersecurity information with the owners and operators of critical infrastructures and trusted worldwide partners. DHS as part of

U.S Government and NATO (North Atlantic Treaty Union) have developed advanced situational awareness systems within cyber ecosystem. NATO is developing a Cyber Rapid Reaction Team (RRT) that protect its critical infrastructure. U.S. Cyber Command's Cyber Protection Teams (CPT's) creates security for all states in USA. NATO does not have an inherent cyber offensive capability, as the U.S Cyber CPT.

NATO CCD COE's mission is to enhance cooperation and information sharing between NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organizing conferences, workshops and cyber defence exercises,and offering consultations upon request [37]. NATO does not have own cyber weapons against cyberattacks [41]. The U.S.-led alliance established an operations centre on Aug. 31.2018 at its military hub in Belgium and the U.S.A, Britain, Estonia and other allies have since offered their cyber capabilities [3]. NATO's CYOC (CYOC Cyber Operations Center) is under development, and it will provide coordination and integration fuctions for allies.

The MITRE Corporation is a private, not-for-profit organization that manages and operates federally funded research and development centers (FFRDCs) that support United States (U.S.) government sponsors. FFRDCs serve as long-term strategic partners to the government, providing objective guidance in an environment free of conflicts of interest. MITRE has substantial experience as a trusted, independent third party providing secure stewardship, sharing, and transformational analyses of sensitive information in the USA [2].

3.1 Background of Information Sharing in EU

In2009 ENISA (European Network and Information Security Agency) defined information exchange as follows: An information exchange is a form of strategic partnership among key public and private stakeholders. The common goal of information exchange is mostly to address malicious cyber-attacks, natural disasters, and physical attacks. The drivers for this information exchange are the benefits of member countries working together on common problems and gaining access to information, which is not available from any other sources [12].

The European Commission presented the cybersecurity strategy of the European Unionin2013. It sets out the EU approach on how to best prevent and respond to cyber disruptions and attacks as well as emphasizes that fundamental rights, democracy and the rule of law need to be protected in the cyber atmosphere. Cyber resilience as one of the strategic priorities. That means effective cooperation between public authorities and the private sector is crucial factor [7].

The European Public-Private Partnership for Resilience (EP3R) was established in 2009 and was the very first attempt at the Pan-European level to use a Public-Private Partnership (PPP) to address cross-border Security and Resilience concerns

in the Telecom Sector. After the EP3R, the main principles for setting up a PPP ecosystem in Europe are to provide legal basis of cooperation. It is also important to ensure open communication between public and private sector. Involvement of Small and Medium Enterprises (SMEs) in the process of PPP building is also crucial, since they are the backbone of the European economy [11, 14].

3.2 Information Exchange in Law Enforcement

How to prevent criminal activities has been one of the main question when public safety authorities have tried to solve a common problem within EU countries. Hague Programme and Stockholm Programme introduced the principle of availability as the guiding concept for information exchange of law enforcement. Information that is available to law enforcement authorities in one Member State should be made accessible to law enforcement authorities or public safety authorities in other Member States [27].

Regulations and Policy Documents; European Regulation and policy documents were considered as sources for legal definitions and to cover the gaps left by the vocabularies extracted from standards when dealing with non-technical definitions [27].

Law enforcement authorities can use Schengen Information Systems (SIS) to consult alerts on wanted persons etc. both inside the EU and at the EU external border. The SIS improves information exchange on terrorist suspects and efforts Member States of EU invalidate e.g. the travel documents [27].

The European Commission has adopted a Communication on the European Information Exchange Model (EIXM). The instruments covered by EIXM allows other to exchange automatically fingerprints, DNA and vehicle registration data (Prum decision). Swedish decision sets out how information should be exchange between EU Member States [27].

Europol supports Member States of the European Union as the information hub for EU law enforcement. Its Secure Information Exchange Network Application (SIENA) enables authorities to exchange information with each other, with Europol, and with a number of third parties. Europol's databases help law enforcement from different countries to work together by identifying common investigations, as well as providing the basis for strategic and thematic analysis [27].

4 Legislation and Regulation Concerning Information Exchange in USA and Europe

4.1 Regulation in the USA

The White House designated the National Coordinating Center for Communications (NCC) as Information Sharing and Analysis Center (ISAC) for telecommunications in accordance with presidential Decision Directive 63 in 2000 (President's National Security Telecommunications Advisory Committee (NSTAC) [38].

The communications Information Sharing and Analysis Center (Comm-ISAC) incorporates dozens of organisations. It has facilitated the exchange of information

among industry and government participants regarding vulnerabilities, threats, intrusions and anomalies affecting the telecommunications infrastructure.

The exchange of information between the EU and the US has been regulated among other things, as follows; The European Commission and the U.S. Government reached a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes named the EU-U.S. Privacy Shield. The European Commission adopted the EU-U.S. Privacy Shield on July of 2016 [8].

The framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers.

The EU-U.S. Privacy Shield based on the principles: Obligations on companies that handle data. (a) The U.S. Department of Commerce will conduct regular updates and reviews of participating companies to ensure that companies follow the rules they submitted themselves to. (b) Clear safeguards and transparency obligations on U.S. government access: The US has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear oversight mechanisms. (c) Effective protection of individual rights: citizen who thinks that collected data has been misused under the Privacy Shield scheme will benefit from several accessible dispute resolution mechanisms. It is possible for a company to resolve the complaint by itself or give it to The Alternative Dispute resolution (ADR) to be resolved for free. Citizens can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved [8]. The Court of Justice of the European Union issued a judgement declaring as invalid the European Commission's Decision (EU) 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when sharing personal data from the European Union to the United States [45]. Participated organizations of the Privacy Shield program are required to re-certify to the Department of Commerce annually. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to achieve its annual re-certification to the Department. An organizations's removal from the list means it may no longer claim that it benefits from the Privacy Shield.

4.1.1 Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. The FOIA requires agencies to proactively post online certain categories of information, including frequently requested records. It is often described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under the FOIA unless it comprises under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement. Any person can make a FOIA request (Office of Information Policy (OIP) [36].

4.1.2 Cybersecurity Information Sharing Act (CISA)

CISA authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats. CISA provides certain protections to encourage companies voluntarily to share information about "cyber threat indicators" and "defensive measures" with the federal government, state and local governments, and other enterprises and private entities. These protections comprise protections from liability, non-waiver of privilege, and protections from FOIA disclosure, although, importantly, some of these protections apply only when sharing with certain entities. Qualifying these protections requires that, the information sharing must comply with CISA's requirements, including regarding the removal of personal information [16].

4.2 Regulation in the European Union

The list of the most relevant regulation taken into consideration in EU level.

4.2.1 NIS Directive

ENISA, Europol/EC3 and the EDA are three agencies active from the perspective of NIS, law enforcement and defines respectively. These agencies have Management Boards where the Member States are represented and offer platforms for coordination at EU level [10].

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 (NIS directive). The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. The NIS directive was adopted in 2016 and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or "transposes' the directive. EU directives give EU countries some level of flexibility to take into account national circumstances, for example to re-use existing organizational structures or to align with existing national legislation [5]. The European Parliament resolution on the European Union's cyber Security Strategy states e.g. that the detection and reporting of cyber-security incidents are central to the promotion of information networks Sustainability in the Union [26]. The NIS Directive consists three parts:

1. National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.
2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.
3. National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, and finance sector), expost

supervision for critical digital service providers (internet exchange points, domain name systems, etc.).

4.2.2 General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) harmonizes data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. GDPR applies to all businesses offering goods and/or services to the EU. That means that the organizations do not have to reside in the EU area or even in Europe, if you are holding private information about an EU citizen whom you provide services, GDPR applies [9]. The Regulation introduces stronger citizens' rights as new transparency requirements. It strengthens the rights of information, access and the right to be forgotten. The law is technology neutral and applies to both automated and manual processing if the data is organized in accordance with pre-defined criteria [9]. It also does not matter if the data is stored in an IT system through video surveillance, or on paper. In all these cases personal data is subject to the protection requirements set out in the GDPR.

5 Relevant Standards Concerning Cyber Secure Information Sharing

What is Data protection and relationship between 27000 and 29000 family standards?

Data protection is the basic legal right of all individuals to protect their own personal information. Personal information is any information relating to an identified or identifiable person. The purpose of data protection is to indicate when and under what conditions personal data may be processed. Organizations processing personal da ta are required to take reasonable steps to protect it [15].

How should personal data be processed?

The processing of personal data or privacy issues is subject to requirements in several different laws. The processing of personal data must be confidential and secure. The processing of personal data according to the principles is only for a specific and legitimate purpose. Privacy Policy—Consent and Freedom of Choice. Legality and definition of purpose. Limitation of data collection. Restriction of data processing. Restriction on Use, Storage and Disposal SFS-ISO / IEC 2910 [15].

Important standards of data protection

The 29000 series contains standards that fundamentally govern privacy, although the 29000 series contains a very wide variety, most of which have nothing to do with privacy issues. The 27000 series describes the standards related to the security management method, some of which also directly concern data protection. The 27000 Series management template can be used to implement a data-driven environment, which is a prerequisite for data protection [15]. As Fig. 1 illustrates, information security consist of CIA (Confidentially, Integrity and Availability)

features. Confidentiality means that information is only accessible to those entitled to it.

Integrity or correctness of information means that the information must be true and correct. Availability means that in formation is available when you want to use the data of the data subject. The right to privacy or the rights of the data subject required by data protection cannot be fulfilled without the implementation of the data security attributes as mentioned above. For example, the data subject has the right to know who has accessed the data stored in the register. This requires confidentiality and integrity.

Figure 1 presents relationships between the elements of data protection.

Figure 2 presents relationships between the elements of data protection and standards (modified from SFS 2018 publication).

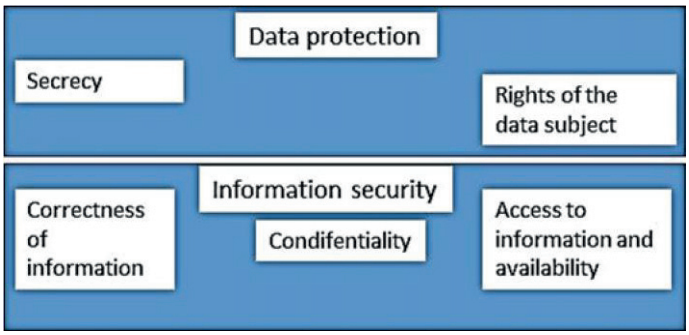


Fig. 1 Privacy elements (CIA)

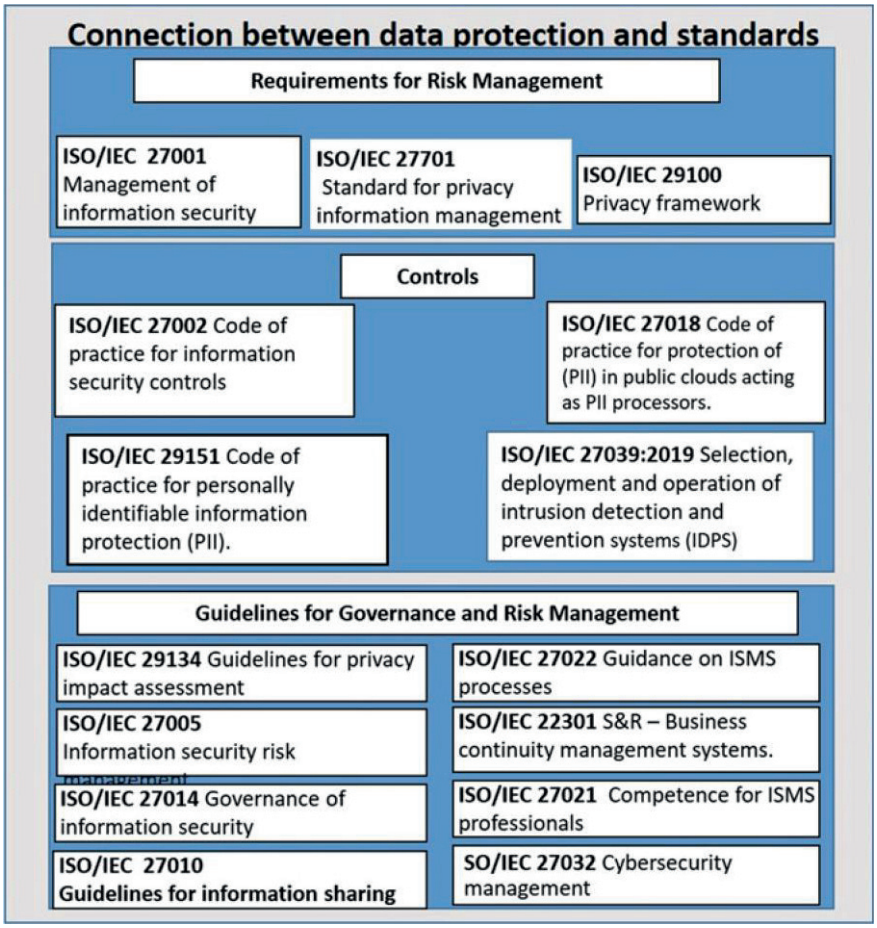


Fig. 2 Elements of the data protection

According to ISECT [23] risk management, ISO/IEC 27005 is a remarkable standard which propose ongoing process consisting of a structured sequence of activities, some of which are iterative:

- Establish the risk management context (e.g. the scope, approaches or methods to be used and relevant policies and criteria such as the organization's risk tolerance) • Quantitatively or qualitatively assess means identify, analyze and evaluate relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a "level of risk".
- Manage and modify by using information security controls, retain or "accept", avoid and/or share with third parties the risks appropriately, using those "levels of risk" to prioritize them;

- Keep partners informed throughout the process; and Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes [23].

ISO/IEC 29134:2017 [19] gives guidelines for a process on privacy impact assessments and a structure and content of a PIA report. It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations. ISO/IEC 29134:2017 is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII [19].

According to requirements for system management ISO/IEC 29100:2011 provides a privacy framework that specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology. It is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII [17].

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS). It is a suite of activities concerning the management of information risks (called "information security risks" in the standard). The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts—an important aspect in such a dynamic field, and a key advantage of ISO27 family's flexible risk-driven approach. "Statement of Applicability" (SoA) is not explicitly defined, it is a mandatory requirement. SoA refers to the output from the information risk assessments and in particular the decisions around treating those risks. The SoA may, i.e. take the form of a matrix identifying various types of information risks on one axis and risk treatment options on the other and show how the risks are to be treated in the body, and perhaps who is accountable for them. It usually references the relevant controls from ISO/IEC 27002 but the organization may use a completely different framework such as NIST SP800-53, the ISF standard, BMIS and other [24].

Management methods and controls

Management consists ISO/IEC 29151:2017 and ISO/IEC 27002:2013. ISO/IEC 29151:2017 establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII). ISO/IEC 29151:2017 is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII [21].

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; implement commonly accepted information security controls; develop their own information security management guidelines [20].

Continuity management and relationship to the Cyber-Physical System

ISO/IEC 22301:2019 set frames to the Security and resilience. It consists requirements for business continuity management systems. It represents how to manage business continuity in an organization [1]. This standard based on leading business continuity specialists opinions and supplies the framework for managing business continuity in an organization [1]. Other relevant standards are listed on the Fig. 3.

6 Method and Process of the Research

Case study illustrates the attempt to produce a profound and detailed information about the object under research. The materials collected for this case study based on scientific publications, official documents, collected articles and literary material. The research is focused on how it's possible integrate USA- related information sharing models in European level. Yin [44] identifies five components of research design for case studies: (1) the questions of the study, (2) its propositions, if any; (3) its unit(s) of analysis; (4) the logic linking the data to the propositions; and (5) the criteria for interpreting the findings. This case study is carried out with the guidance of Yin [44].

There are country-specific differences, institutional differences, legislative differences in legislation, etc. The purpose is to categorize things into their own groups. Some information sharing models and information management frameworks are simple diagrams, some are ready-made templates, and some information sharing models have concrete instruments and tools. The purpose of the analysis is to find out about the functionalities, useful standards and features of information sharing systems in the EU, USA and NATO. Outcome of the research is combined proposal of information sharing model and initial risk management framework.

7 Definition of Information Sharing Goals

According to National Institute of Standards and Technology [33] the organization should establish goals and objectives that describe the desired outcomes of threat information. These objectives will help guide the organization through the process of scoping its information-sharing efforts, joining sharing communities and providing ongoing support for information sharing activities.

According to Skopik et al. [40] primary dimensions of security information sharing can be divided as follows: (a) Cooperation and coordination economic need

for coordinated cyber defense. There exists variety of classification of information that are viable for a wide range of stakeholders: indicators of compromise, technical vulnerabilities, zero-day exploits, social engineering attacks or critical service outages. (b) Legal and Regulatory Atmosphere: information sharing requires a legal basis. Therefore, the European Union and its Member States and the US, have already done a set of directives and regulations. (c) Standardization Efforts means enabling information sharing, standards and specifications need to standardize that are compliant with legal requirements (e.g. NIST, ENISA, ETSI and ISO). (d) Regional and International Implementations means taking these standards and specifications, organizational measures and sharing structures need to be realized, integrated and implemented. CERTs and national cyber security centers work on this issue. (e) Technology Integration into Organizations means sharing protocols and management tools on the technical layer need to be selected and set into operation.

7.1 Identify Internal Sources of Cyber Threat Information

CORA (Cyber Operations Rapid Assessment) methodology was developed to study issues and best practices in cyber information sharing. In addition, it consists as an engagement tool for assessing and improving threat-based security defenses. CORA identifies five major areas of cyber security where the proper introduction of threat information can have tremendous impact on the efficacy of defenses: External Engagement—Tools and Data Collection—Tracking and Analysis—Internal Processes—Threat Awareness and Training.

The TICSO gather cyber threat intelligence and information from a variety of sources including open source reporting by researchers and consultants, government and law enforcement sources [USCERT, INFRG], fee-for-service threat Intel feeds from vendors and industry sector and regional threat sharing communities such as ISACs and ISAOs. The TICSO focuses collection efforts on the most relevant information by defining prioritized intelligence requirements (PIR), and continuously evaluating the quality of intelligence from different sources in terms of relevance, timeliness, and accuracy (MITRE Corporation).

A first step in any information sharing effort is to identify sources of threat information within an organization. According to National Institute of Standards and Technology [33]. The process of identifying threat information sources includes the following sections:

(a) Identify sensors, tools, data feeds, and repositories that produce threat information and confirm that the information is produced at a frequency, precision, and accuracy to support cybersecurity decision-making.
(b) Identify threat information that is collected and analyzed as part of an organization's continuous monitoring strategy.
(c) Locate threat information that is collected and stored, but not necessarily analyzed or reviewed on an ongoing basis.

(d) Identify threat information that is suitable for sharing with outside parties and that could help them more effectively respond to threats. Examples of selected Internal Information Sources [33].

7.2 Comparing Features of the Information Sharing Models

There are several different information sharing models in the world. The most important thing was to choose such cyber information sharing models that are widely used in the European Union countries, USA and NATO. It is not necessary to compare all models or frameworks because availability of information varies a lot. Usually the information-sharing model is incomplete frame that is believed to solve all the problems concerning cyber security. As Table 1 illustrates five different type of models has chosen to more detailed review.

8 Findings

Mechanism type of the ISAC concerns the overall structure that is used to exchange information. This type of mechanism often has a central hub that receives data from the participants. The hub can redistribute the incoming data directly to other members, or it can provide value-added services and send the updated information or data to the members. The hub may act as a "separator" that can facilitate information sharing while protecting the identities of the members. One of the main tasks of ISACs is sharing information on intrusions and vulnerabilities. These types of information are usually troublesome; therefore, companies often decide to keep silent. ISAC hub system relies on the functionality of the hub, which makes the system vulnerable to delays and systemic failures [29]. Important information is often unnecessary to achieve, delays in information sharing can reduce the benefits of the information-sharing hub mechanism. In post to all model information is shared among stakeholders. MITREs model is one kind of hybrid information sharing model. It is a partner for helping private or public organizations stand-up and run information sharing exchanges. Mechanism of MITRE use automated processing of information. This work has enabled security automation in vulnerability management, asset

Table 1 Examples of information sharing models

Organization //Name //System/model or framework type	Main tasks/ features	Special tasks or info	Major areas of cyber impacts	Instruments
MITRE// CORA // Assessment of cyber operations (not-for-profit organization)	Developed for to study issues and best practices in cyber information sharing. It serves as an engagement tool for assessing and improving threat-based security defences	Based on NIST Special Publication 800–150: Guide to Cyber Threat Information Sharing	External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	indicators scan networks and systems—Reporting new indicators about attacks on its own networks
MITRE// TISCO// Threat-Informed Model	It collects cyber threat intelligence and information from a variety of sources including open source reporting by researchers and consultants		External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	Sensors monitoring attack activity such as phishing email addresses and URLs of malicious sites, host-based indicators
ENISA// ISAC// Member driven organization model Country-focused ISAC - International ISAC -	Sharing knowledge about incidents with the member organizations and prevent/ respond to the incidents which occur (ISAC is a fast way to get all the knowledge and way of networking and meeting people from different organizations	ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It provides information about threats and incidents. (close cooperation with the industry, public entities get better understanding of the private sector)	(a) Some information can be shared widely with all members. (b) The shared information is more detailed in internal circle. c) use of the (TLP) to share information	web portal/platform (following a specific template) and encrypted emails

(continued)

Table 1 (continued)

Organization //Name //System/model or framework type	Main tasks/ features	Special tasks or info	Major areas of cyber impacts	Instruments
ENISA// PPP// Cooperative model	Access to public funds. Opportunity to influence national legislation and obligatory standards. Access to public sector knowledge and confidential information (EU legislation, fighting against cybercrime)	Helps to achieve resilience in the cyber ecosystem. PPP Increase the trust between public-public–private. it allows to have better information and proactive attitude in case of crisis	Incident handling and crisis management, Information exchange, Early warnings, Technical evaluation, Defining standards etc.	Help desk helps PPP's members. PPP does not consist real-time instruments against cyberattacks
NIST// Framework//	NIST FW targeting on risk management, procedures and privacy preservation aspects	The guidelines included in the ISO/IEC27010 standard, it is oriented toward the protection of the data exchanged in the information sharing process	Techniques standards and protocols for systems monitoring, threat detection, vulnerability inventory and incident exchange	Framework adds consist different kind of tools, but only framework does not offer protection for shared information or information for incident handling process

management, and configuration management though the Security Content Automation Protocol program. Members of MITRE do not share information. Each participant sends its sensitive data to MITRE, and MITRE works diligently to ensure that member data is kept confidential [29].

There is a need to develop Public–Private information-sharing models in EU level because public safety organizations of the Department of the Homeland Security in USA are capable to handle external threats more effectively. There are international organizations which have formulated co-operational working environment such a way that western world could operate for the common purpose. International organizations like UN (United Nations) and NATO are the connecting factors concerning harmonization of information sharing procedures in the EU and USA and between them, not forgetting NATO. In this author's view, the so-called "triangle" should be called a "square."

The requirements of the system integrity means that it's impossible to separate information system -related standards from the information sharing methods when the purpose is to design common cyber ecosystem for the western world. Interoperability should be coordinated through standards as Fig. 3 illustrated.

Cyber-physical system allows to protect critical infrastructure because of the automated functionalities. E.g., in a finance sector it is not possible to protect it without interfering with the activities of the attacker. Automated physical actions mean Physical functionalities e.g., in finance sector and/or cyber-defence functionalities against the attacks but everything must be reverted to existing standards. Privacy impact (PI) is crucial element in all situations when the purpose is to develops ystem which handle

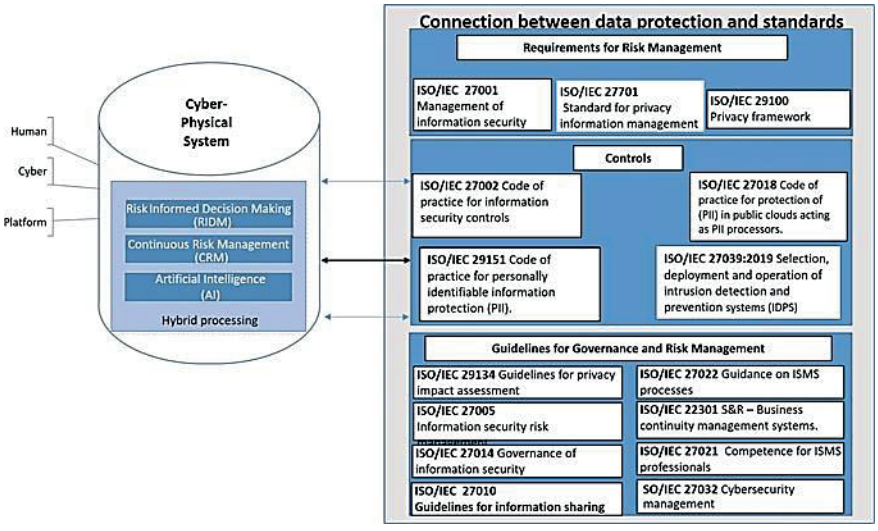


Fig. 3 Relationship between CPS and continuous risk management system

privacy identifiable information. PI could result from the processing of Privacy Identifiable information (PII). According to ISO/IEC 29134:2017 (International Organization for Standardization (ISO) [19] a Privacy Impact Assessment (PIA) is a tool for addressing the potential impacts on privacy of a process information system, programme, or device. It will inform to all participants which have to take actions in order to treat privacy risk. PIA is ongoing process and report may include documentation about measures taken for risk treatment, measures may arise from the use of the ISMS.

At a general level, collaboration between cyber-physical system and continuous risk management requires collaboration between these elements. In the traditional sense, three levels can be found; human; platform layer and cyber layer as figure illustrates, but that's not enough. Proposed framework require to take into account standards and information management when purpose is to develop common early warning solution for the western allies.

At the technical level, the challenge of semantic interoperability is that information systems should automatically understand the concepts arising from the actions of people and organizations. Therefore, it is important to create a common risk management framework for both. It is possible to connect different kind of decision-making strategies to the cyber physical framework as proposal illustrates above. Legislation and regulation must be the fundamental basis for all functions and operations.

This means that fundamental frame of the cyber-physical system based on legislation, rules and standards. E.g., higher-level EWS should be structured from the view of "regulation". The operations of the system must be based on rules and standards. Semantic interoperability means that an information system is able to combine the information it receives from different sources and process it in a way that preserves the meaning of the information. E.g., there are business-related differences concerning sector-specific stakeholders of the ECHO consortium.

9 Conclusions

Separate functionalities between the EU member states are not only problem. When the common goal is to improve Cyber Situational Awareness, it is important to deepen the cooperation between western stakeholders. Major problem of information sharing models is related lack of real-time cyber information management between participants. There is essential problem with features of information sharing models. When the purpose is to protect vital functions of society, public safety organizations in European Union member states needs proactive features in their information systems. A shared common cyber situational awareness means that real time communication links between the states must exist.

Legislation is not only factor, which affects to completely secure cyber-ecosystem. Developed systems need coherent standardization, common management system and governance model. The USA and its public safety cyber defense organizations has ability to combat cyberattacks, which have made against vital functions, but also make counter-attacks [41]. It is one of the most important features in protecting the western world. Cooperation and collaboration in triangle

EU-NATO-USA is therefore particularly important. In addition The United Nations acts as the fourth element. Utilizing the best features of the information sharing models will ensure procedures of continuity management. It is therefore important to place EU countries in the right context. Legislation has been harmonized, but occasional is to trust organization's functionalities. Common continuous risk management system helps to handle the data bases concerning privacy issues. Lack of standardization may cause obstacles when the aim is to catch cyber criminals or find out state level actor that has caused a cyber or hybrid attacks.

It is a fundamental problem that, as the geographical area of the European Union expands, it does not have the capability to prevent hybrid-threats. Controlled governance model for the EWS and common standardization concerning information management systems and cyber emergency procedures between authorities, and international organizations helps to achieve common situational awareness inside the western world. It is not enough that every country tries to tackle cyber threats separately. There is a need for a jointly controlled information exhange framework for the EU countries and credible counter operation tools for counter-attack operations that must be connectable to another defense mechanism. Nato is setting up a joint coordination center against cyberattacks by 2023, but NATO will also need centralized mechanism to defend allies against cyber-threats.

References

1. Advisera Expert Solutions: What is ISO 22301? [Homepage of Advisera Expert Solutions] (2019). [Online]. Available: https://advisera.com/27001academy/what-is-iso-22301/. 28 Aug 10
2. Bakis, B., Wang, E.D.: Building a National Cyber Information-Sharing Ecosystem. MITRECorporation (2017)
3. Bigelow, B.: The Topography of cyberspace and its consequences for operations. In: 10thInternational Conference on Cyber Conflict 2018, NATO CCD COE Publications (2018)
4. Department of Homeland Security (DHS): Blueprint for a Secure Cyber Future—TheCybersecurity Strategy for the Homeland Security Enterprise. DHS (2011)
5. ENISA: NIS Directive [Homepage of European Union Agency for Network and InformationSecurity] (2019-last update), [Online]. Available: https://www.enisa.europa.eu/topics/nis-dir ective [6/2019]
6. ENISA: Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS). European Union Agency for Network and Information Security, Greece (2013)
7. ENISA & ITE: Information Sharing and Analysis Centres (ISACs) Cooperative models.European Union Agency for Network and Information Security, Greece (2017)
8. European Commission: EU-U.S. Privacy Shield: Stronger Protection for Transatlantic DataFlows. Brussels (2016)
9. European Commission: General Data Protection Regulation (EU) 2016/679. Regulation edn. Brussels (2016)
10. European Commission: Joint Communication To The European Parliament, The Council, the European Economic And Social Committee And The Committee Of The Regions. European Commission, Brussels (2013)
11. European Union Agency for Cybersecurity (ENISA): Public Private Partnerships (PPP) Cooperative models. European Union Agency for Network and Information Security, Greece (2017)
12. European Union Agency for Cybersecurity (ENISA): Good Practice Guide—Network SecurityInformation exchanges. ENISA, Greece (2009)

13. European Union Agency for Network and Information Security (ENISA): Smart grid security certification in EUROPE. ENISA, Greece (2014)
14. European Union Agency for Network and Information Security (ENISA): EP3R 2013—Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS). European Union Agency for Network and Information Security, Greece (2013)
15. Finnish Association for Standardization SFS RY: Information technology. Safety. Information security management systems. Privacy Standards. SFS (2018)
16. Harvard Law School Forum on Corporate Governance and Financial Regulation: Federal Guidance on the Cybersecurity Information Sharing Act of 2015 [Homepage of The President and Fellows of Harvard College] (2016). [Online]. Available: https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/. 11 Oct 2019
17. International Organization for Standardization (ISO): ISO/IEC 29151:2017 Information technology—Security techniques—Code of practice for personally identifiable information protection [Homepage of ISO] (2018), [Online]. Available: https://www.iso.org/obp/ui/#iso:std:isoiec:29151:ed-1:v1:en
18. International Organization for Standardization (ISO): International Standard ISO/IEC 27010:2015. Standard edn. Switzerland (2015)
19. International Organization for Standardization (ISO): ISO/IEC 29134:2017 Guidelines for privacy impact assessment (2017). Available: https://www.iso.org/standard/62289.html
20. International Organization for Standardization (ISO): ISO/IEC 27002:2013 Security techniques—Code of practice for information security controls [Homepage of ISO] (2013), [Online]. Available: https://www.iso.org/standard/54533.html
21. International Organization for Standardization ISO: ISO/IEC 29100:2011 information technology—Security techniques—Privacy framework [Homepage of ISO] (2018), [Online]. Available: https://www.iso.org/standard/45123.html2019
22. International Telecommunication Union: Global Cybersecurity Index (GCI) 2018. ITU, Switzerland (2018)
23. ISECT: ISO/IEC 27005:2018 Information technology—Security techniques—Information security risk management (third edition [Homepage of IsecT Limited] (2018), [Online]. Available: https://www.iso27001security.com/html/27005.html
24. ISECT: ISO/IEC 27001 Information security management systems—Requirements [Homepage of IsecT Limited] (2017), [Online]. Available: https://www.iso27001security.com/html/ about_us.html
25. Lee, E.A., Seshia, S.A.: Introduction to Embedded Systems, A Cyber-Physical SystemsApproach, 2 edn. (2015)
26. Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J., Salminen, M.: Kyberturvallisuudenstrateginen johtaminen Suomessa. 28. Valtioneuvoston kanslia, Helsinki (2018)
27. Migration and Home Affairs: Information exchange [Homepage of European Commission] (2019), [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange_en. [06/2019, 17/06/2019].
28. Ministry of the Interior: National Risk Assessment. Ministry of the Interior, Helsinki (2018)
29. MITRE: Cyber Information-Sharing Models: An Overview. MITRE Corporation (2012)
30. MITRE Corporation: Cyber Operations Rapid Assessment (CORA): A Guide to BestPractices for Threat-Informed Cyber Security Operations | The MITRE Corporation. Available: https://www.mitre.org/sites/default/files/publications/pr_15-2971-cyber-operations-rapid-assessment-best-practices_0.pdf [3/20/2016, 2016]
31. Nai-Fovino, I., Neisse, R., Lazari, A., Ruzzante, G., Polemi, N., Figwer, M.: European Cybersecurity Centres of Expertise Map—Definitions and Taxonomy. Publications Office of the European Union, Luxemburg (2018)
32. National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity. 1.1. NIST (2018)

33. National Institute of Standards and Technology: Guide to Cyber Threat Information Sharing.NIST Special Publication 800–150. National Institute of Standards and Technology, Gaithersburg (2016)
34. National Institute of Standards and Technology: Guidelines for Smart Grid Cybersecurity—Volume 2 privacy and the Smart Grid. U. S. Department of Commerce (2014)
35. National Institute of Standards and Technology: Guide for Conducting Risk Assessments.800–30. U.S. Department of Commerce, Gaithersburg (2013)
36. Office of Information Policy (OIP): What is FOIA? [Homepage of U.S. Department of Justice] (2019), [Online]. Available: https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-onthe-cybersecurity-information-sharing-act-of-2015/ [10/11, 2019].
37. Pernik, P., Wojtkowiak, J., Verschoor-Kirss, A.: National Cyber Security Organisation: UnitedStates. CCDCOE, Tallinn (2016)
38. President's National Security Telecommunications Advisory Committee (NSTAC): Report tothe President on the National Coordinating Center. Department of the Homeland Security (2006)
39. Secretariat of the Security Committee: Finland's cyber security strategy—government resolution. Ministry of Defense (2013)
40. Skopik, F., Settanni, G., Fiedler, R.: A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput. Secur., 154–176 (2016)
41. Smeets, M.: NATO Allies Need to Come to Terms with Offensive Cyber Operations [Homepageof Lawfare] (2019), [Online]. Available: https://www.lawfareblog.com/nato-allies-need-cometerms-offensive-cyber-operations [11/19, 2019].
42. U.S. Mission to NATO: About NATO (2019). Available: https://nato.usmission.gov/our-relationship/about-nato/
43. White, G., Lipsey, R.: ISAO SO Product Outline. ISAO Standards Organization (2016)
44. Yin, R.K.: Case Study Research, Design and Methods, 5th edn. Sage, Thousand Oaks, CA(2014)
45. Court of Justice of the European Union: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield (2020)

VIII

ENHANCING THE EUROPEAN CYBER THREAT PREVENTION MECHANISM

by

Jussi Simola, 2021

Journal of Information Warfare, vol.20

https://www.jinfowar.com/sites/default/files/Enhancing_the_European_Cyber_Threat_Prevention_Mechanism.pdf

Enhancing the European Cyber Threat Prevention Mechanism

J Simola

Laurea University of Applied Sciences
RDI Espoo, Finland
University of Jyväskylä, Finland

Email: simolajussi@gmail.com

Abstract: *This research will determine how it is possible to implement the national cyber threat prevention system into the EU level Early Warning System. Decision makers have recognized that lack of cooperation between EU member countries affects public safety at the international level. Separate operational functions and procedures between national cyber situation centres create challenges. One main problem is that the European Union does not have a common cyber ecosystem concerning intrusion detection systems for cyber threats. Also, privacy and citizens' security as topics are set against each other. The research will comprise a new database for the ECHO Early Warning System concept.*

Keywords: *Information Sharing, Cybersecurity, HAVARO, Privacy, Early Warning*

Introduction

This paper will comprise a new database for the ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) Early Warning System concept. E-EWS aims at delivering a security operations support tool which enables the members of the ECHO network to coordinate and share information in near real time. Within the E-EWS, partners of ECHO can retain their fully independent management of cyber-sensitive information and related data management. The Early Warning System will work as a parallel part of other mechanisms in the public safety environment. Crucial scientific literature, interviews, and official publications concerning cybersecurity information sharing generate fundamental knowledge to understand the main factors, which separate and combine EU member countries in this environment. The purpose is to support the technical designers of the E-EWS consortium to develop the Early Warning System. Also, interviews of the cybersecurity specialists form crucial sources for the paper.

The HAVARO, organized by TRAFICOM (the Finnish Transport and Communications Agency) and NESA (National Emergency Supply Agency), is one kind of national early warning system, which gathers threat-informed data and produces crucial information concerning the situation of cybersecurity information sharing within critical infrastructure (Ladid, Armin & Kivekäs 2019).

This paper will explore those factors (requirements) which affect the conversion of a national EWS to a common early warning ecosystem at the EU level. Every EU member country has its own system for monitoring and protecting the cyber domain among vital functions. It must be understood

that national systems must find common procedural and governance models in the name of the common good. In addition, privacy-issue-related problems concern the whole cyber ecosystem. The public safety sector will not operate in an isolated dimension without connection to private sector companies. The crucial question is how to combine and share relevant data between stakeholders at the national level and at the international level.

The paper starts with a section introducing the background of challenges concerning critical infrastructure protection and discusses cybersecurity information sharing at the EU level and with the U.S. The next section handles the national HAVARO system and system requirements. The paper concludes with suggestions for a bases of the solution and conclusions about the research area.

Challenges Concerning Critical Infrastructure Protection

According to the Horizon 2020 work program, disruption in the operation of EU member countries within critical infrastructure may result from hazards and physical or cyber-physical events (European Commission 2019).

Public safety authorities have noticed in Finland that protecting modern infrastructures and vital functions needs not only to protect physical operative functionalities and equipment; they also need the cyber-dimension in their daily routine. It is possible to integrate cyber-threat-informed functionalities of the computer emergency response teams and operative functions of the public safety organizations. These integrated systems are examples of Cyber Physical Systems (CPS) that integrate computing and communication capabilities with monitoring and control of entities in the physical world (Secretariat of the Security Committee 2019).

In the European Union, there has been a common will to enhance cooperation between public authorities. According to the European Council (2010), Europol collects and exchanges information and facilitates cooperation between law-enforcement authorities in their fight against cross-boarding organized crime and terrorism. Eurojust drives coordination and increases the effectiveness of judicial authorities. Frontex manages operational cooperation at the external borders. The EU operates as the Counterterrorism Coordinator. Several networks have also been established in the fields of training, drugs, crime prevention, corruption, and judicial cooperation in criminal matters (European Council 2010). Solutions are based on common recognition for information sharing and are designed to ease joint investigations and operations. Instruments based on mutual recognition include the European Arrest Warrant and provision for the freezing of assets (European Council 2010). The report is only 10 years old, and only two lines of text have been used to analyse cyber threats.

There are separate local situation centres for emerging situations and emergency response systems, and there are separate cyber-threat functions at the national and EU level. All work mainly without synergy. ICT development projects—for example MARISA, EUCISE, and RAPID—are European-Commission-funded projects that are producing better common situational awareness among EU member countries. The main limitation to implement the RAPID system is related to a lack of cooperation between the EU countries and real-time features of the mechanism. In addition, a lack of leadership causes problems in collaboration (Apuzzo 2019).

One crucial thing is still missing: combined cyber-physical functionalities (Simola & Rajamäki 2017). It is not enough that there are national computer emergency response teams, which only

monitor Internet traffic. In the future, there is a growing need to use proactive or preventive functionalities among public safety organizations.

Information Sharing at the EU Level and a National Intrusion-Detection System

Shared (cyber) situational awareness is closely related to (cybersecurity) information exchange (Bolstad & Endsley 2000). Bolstad and Endsley (2000) define the development of shared Situational Awareness as consisting of these four factors:

- Shared SA requirements (degree to which team members realize which information is needed by other team members);
- Shared SA devices (communications);
- Shared SA mechanism (shared mental models); and
- Shared SA processes (effective team processes for sharing relevant information).

According to Munk (2018) information interoperability is the joint capability of different actors—such as persons, organizations, and groups—necessary to ensure the exchange and common understanding of the information needed for their success.

The central government of Finland is one of the most important administrative actors that needs correct environment-related cyber situational awareness. When something abnormal occurs, different ministries try to gather and to share the same data from the site of an accident. The common cybersecurity information-sharing procedure enables the government to react to new kinds of threats. There is a need to create a common early warning system with preventive functions. Service producers may be based on public organizations and private companies. One of the most important things is that governance responsibilities of the operational functions should be designated in the future.

In partnership with the National Emergency Supply Agency (NESA), TRAFICOM created the system called HAVARO 1.0 in 2011 (National Cybersecurity Center-FI [NCSC-FI] 2019). It is optional for every Finnish organization to join the system. The information on situation awareness provided by the system increases understanding of the organization´s own and the general state of information security. The system produces information, which makes it possible to alert other players about a detected threat and to develop better tools of detection. The participating organizations are responsible for the costs of equipment needed for their network.

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 traffic can be detected from the organization's network traffic. The NCSC-FI receives the information about the anomalies and analyses them. In case of an information security threat, the organization is warned. Based on the information from the HAVARO, the other operators can also be warned about the detected threat. That way, the system helps not only individual organizations, but also helps form a general view of information-security threats against Finnish information networks. 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 main problem with HAVARO 1.0 concerns the monitoring ability (Lehto *et al.* 2018). It mainly monitors informa-

tion-security incidents in Internet traffic (KPMG 2013). It is incapable of monitoring the communication of individual user behaviour.

In the future, it is not enough to monitor only the Internet traffic of companies. There should be a wider right to access the organizations' information systems and communication because the Internet of Things (IoT) is changing the way the Artificial Intelligence atmosphere is understood. When electrical and telecommunication cables are placed in the same pipeline, possibilities for vulnerabilities increase.

The HAVARO service is now under development. Instead of being a government service, HAVARO 2.0 will be jointly provided by commercial operators and the NCSC-FI. Some of the events will be processed and reported by information Security Operations Centres (SOC). The objective of the HAVARO 2.0 project is to create the trust network in which the members can exchange information among themselves better than they have before. The HAVARO 2.0 Early Warning System will consist of features of the existing 1.0 system with developed early-warning dimensions. Existing cyber-threat sensor systems need more specialized detection features. Increasing the cyber-threat atmosphere will force stakeholders to develop a better and more efficient system. Separate forensics methods, gathering logs, gathering information, reverse engineering, and analysing risks are not enough in the future. It is crucial to produce added value by combining different data sources and weak threat signals. HAVARO 2.0 will only be complementary to other cybersecurity services.

HAVARO 2.0 will include the GovHavaro feature (Lehto *et al.* 2018). That means that there will be a connection between public organizations and the HAVARO Early Warning System. This information is classified as more confidential, but sector-based sharing requires the sharing of this information to all public safety organizations and to the central government. At the EU level, this information is important to be shared in real time to the stakeholders if threat-information regarding cybersecurity related information to other countries or threat information generates a common risk to vital functions. New stakeholders of the HAVARO 2.0 have contractual relationships with SOCs, not with the NCSC.

Cybersecurity Information Sharing with the U.S.

There are no fundamental differences in administrative functions between the European Union and the United States. Mainly there are more similarities than differences. Legislation and regulation between the U.S. and the EU are coming closer to each other. The NIS directive in the EU will help to develop next-generation early warning systems.

According to the European Parliament and the Council of the European Union (2016), General Data Protection Regulation (GDPR) was designed to harmonize data-privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy. GDPR applies to all businesses offering goods and/or services to the EU. That means, if a company is holding private information about an EU citizen to whom it provides services, GDPR applies. It strengthens the rights of private information, access, and the right to be forgotten. The GDPR protects personal data regardless of the technology (automated and manual processing) used. GDPR concerns both unions. The U.S. and the EU have made fundamental agreements to generate a common base for fluent information sharing (European Parliament and the Council of The European Union 2016). Public safety actors, like European law enforcement agencies, need a common situational picture for the cross-boarding tasks so that operational cooperation will be based on a reliable platform.

The European Commission presented the cybersecurity strategy of the European Union in 2013. It set out the EU approach on how to best prevent and to respond to cyber disruptions and attacks as well as emphasized that fundamental rights, democracy, and the rule of law need to be protected in the cyber domain. Cyber resilience is one of the strategic priorities. That means that effective cooperation between public authorities and the private sector is a crucial factor, that the national Network and Information Sharing competent authorities should exchange relevant information with other regulatory bodies.

The information sharing between the EU and the U.S. has been regulated among other things, as follows; the European Commission and the U.S. Government reached a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes named the EU-US Privacy Shield (European Commission 2016). The framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as brings legal clarity for businesses relying on transatlantic data transfers. The EU-US Privacy Shield is based on several principles that govern companies that handle data. They are as follows: a) the U.S. Department of Commerce will conduct regular updates and reviews of participating companies to ensure that companies follow the rules they submitted themselves to; b) the U.S. has given the EU assurance that the access of public authorities for law enforcement and national security are subject to clear oversight mechanisms; c) citizens who think that collected data has been misused under the Privacy Shield scheme will benefit from several accessible dispute resolution mechanisms. It is possible for a company to resolve the complaint by itself or give it to the Alternative Dispute Resolution (ADR) to be resolved for free. Citizens can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved. The Ombudsperson mechanism means that an independent senior official within the Department of State will ensure that complaints are properly investigated and addressed in a timely manner (European Commission 2016).

According to the U.S. Department of Commerce (2020), the United States has taken a different approach to improving the protection of privacy from that taken by the European Union. The United States uses a sectoral approach that is based on a combination of legislation, regulation, and self-regulation. The approach provides organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union. This mechanism ensures that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when it has been shared to outside of the EU area. The Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles under its statutory authority to foster, promote, and develop international commerce (U.S. Department of Commerce 2020).

Challenges with the Privacy Shield Agreement

Privacy activists have challenged the Privacy Shield Agreement by arguing that U.S. national security laws did not protect EU citizens from government snooping. On 16 July 2020, the EU Court of Justice made the decision about the adequacy of the protection provided by the EU-US Data Protection Shield by invalidating the agreement (Court of Justice 2020). Despite this decision, the EU Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries is valid. Affected companies will now have to sign 'standard contractual clauses'—non-negotiable legal contracts drawn up by Europe, which are used in other countries besides the U.S. As regards the requirement of judicial protection, the Ombudsperson

mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the U.S. intelligence services. For the above, the Court of Justice declared the European Commission Decision 2016/1250 invalid (Court of Justice 2020).

The purpose of standards is to simplify the work of authorities, to facilitate trade, and to make consumers' everyday lives easier. Standardization helps companies and enterprises to create common rules for information sharing and data handling. The family of 270XX standards provides the bases for the definition and implementation of an Information Security Management System (ISMS). For example, standard ISO/IEC 27010:2015 belongs to an ISO 27000 family and is a key component of trusted information sharing. This International Standard is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors (International Organisation for Standardisation 27010:2015).

A trusted independent entity would be appointed by the information-sharing community to organise and to support their activities, for example, by providing a source anonymization service (International Organisation for Standardisation 27010:2015).

ISO standard 11179 (2019) provides guidelines for the naming and definition of data elements, as well as information about the metadata captured about data elements (International Organisation for Standardisation 11179-7:2019). Standard 24745 (2011) ensures that any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains; from which identification or contact information of an individual person can be derived; or that is or might be directly or indirectly linked to a natural person be kept private. These are only examples of a wide range of standards that companies must follow. Standardization strengthens product compatibility and safety, protects the citizens, and protects the environment (International Organisation for Standardisation 24745:2011).

System Requirements

Humans are not as good at processing large volumes of data—quickly and consistently. Flexible autonomy should provide a smooth, simple, seamless transition of functions between the human and the system (Endsley 1988).

National early warning system and information sharing among ECHO EWS partners sets requirements for the basis of the research. Collected materials comes from the scientific literature, interviews of IT specialists, research articles, and official publications.

ECHO EWS will deliver a secure sharing support tool for public-safety personnel to coordinate and to share information in near real-time. It will support information sharing across organizational boundaries and will provide the sharing of general cyber information as a reference library. It will also ensure secure connection management from clients accessing the E-EWS. It will combine different kinds of functions required in the management of information-sharing functions, including sector-specific cyber-sensitive data. All participants (administrative actors, EU countries, companies, cyber situational centres, and public safety authorities) set requirements for developing

ECHO system governance and the Early Warning System. The big challenge is the diversity of stakeholders included in the ECHO. Therefore, system requirements cannot place too many challenging barriers to the development of the E-EWS.

When the aim is to share essential information between stakeholders as soon as possible, information sharing must be automatized. AIS (Automatic Identification System) utilizes the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications for machine-to-machine communication. STIX is a language and serialization format that enables organizations to exchange Cyber Threat Intelligence (CTI) in a consistent and machine-readable manner. Trusted Automated eXchange of Intelligence Information (TAXII™) is an application layer protocol used to exchange cyber threat intelligence (CTI) over the HTTPS (Department of Homeland Security [DHS] 2019). Echo EWS system requirements are based on requirements concerning governance model and Echo Federated Cyber Range.

Bromander, Muller and Jøsang (2020) have criticized the use of STIX because of various ways of representing the same information, the possibility of automatic consumption, and the fact that computer-based analysis becomes limited. If a computer cannot identify information because the information type is not normalized, 'Big Data'-style analysis is not possible; therefore, manual work is needed to correct and to analyse the data Also lack of standardization concerning all relevant information poses a problem for automation. Bromander, Muller and Jøsang (2020) argue that while many claim to use STIX, in most cases it is not used as a standardized way of sharing CTI suitable for automation. The criticism is justified and seems to concern large companies. However, there are currently no well-developed alternative good solutions.

Suggestion for a Basis of the Solution

This section describes the findings and suggested basis of a solution for national information sharing. First, the information-sharing architecture in the U.S. will be addressed. After that, methodologies for the indicator sharing and possible features for the early warning system will be introduced.

Information-sharing architecture in the U.S.

NCSC-FI (National Cybersecurity Center) and NESA (The National Emergency Supply Agency) have made an industry-specific classification for sharing cyber-threat information. The classification is demonstrated as follows: VIRT, public organizations, defense industry, energy sector, finance, industry automation, chemical and process industry, logistics sector, food industry, health sector, industrial companies, equipment and product manufacturers, ICT, media industry, security consultants, security researches, CERT-actors. Despite the classification, there is a need to expand collaboration within public and private actors. NESA, as a partner of TRAFICOM, is responsible for vital functions of society in Finland (NCSC-FI 2017). This classification mainly follows the European model, but also follows the sector-based classification in the U.S.

As mentioned above, the information-sharing model used in the U.S. is possible to replicate in the European Union. There are more similarities than differences. The simple picture in **Figure 1**, below, shows how information is shared. Automated information (indicator) sharing is mainly based on centralized ISACs, which consist of all actors of the specific sector. As illustrated in **Figure 1**, below, sector-based Information Sharing and Analysis Centers (ISACs) are one kind of government-prompted, industry-centric sharing model. Centers are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between

government and industry (ENISA & ITE 2017). Finland uses a similar national level structure of information sharing. It is based on the classification of different sectors of critical infrastructure. There are 16 levels of critical infrastructure used in the U.S. The same sector-specific frame is almost in use everywhere in western countries (White House 2013a; 2013b).

Open Communities and Platforms are open-source sharing platforms. For example, STIX indicators and open-source intelligence feeds are this kind of format. The Malware Information Sharing Platform (MISP) is a free, open-source platform developed by researchers from the Computer Incident Response Center of Luxemburg, the Belgian military, and NATO. For example, Interpol uses the Malware Information Sharing Platform (GitHub 2019; OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017a).

HAVARO as a part of the European Early Warning System

There are several factors that are important to notice if the purpose is to integrate the national Early Warning System to the common European Union level Early Warning System. First, the use of cloud services is not a secure way to store and gather threat-informed data. When customers of the early warning solution are connected to the system from all around Europe, using cloud-only service solutions is not secure because cyberattacks against virtual machines may jam the whole system. Therefore, the authors recommend using a centralized main server that produces services to EWS stakeholders. This sharing model requires using local (national) E-EWS servers where ECHO-EWS is connected This is one kind of hybrid model, but the model is a secure part of the architecture, which allows sharing trust-level information. It is important that, for example, the National Bureau of Investigation have the ability to gather and to share trust-level information concerning vital functions of society and have the ability to be connected in the Early Warning System. It is relevant that the early warning data is shared from the central server to the affected sectors. International researchers recommend using a controlled information-sharing model, where national public safety actors share relevant data to stakeholders via a centralized center (EWS Center [Department of Homeland Security]) as **Figure 1** illustrates.

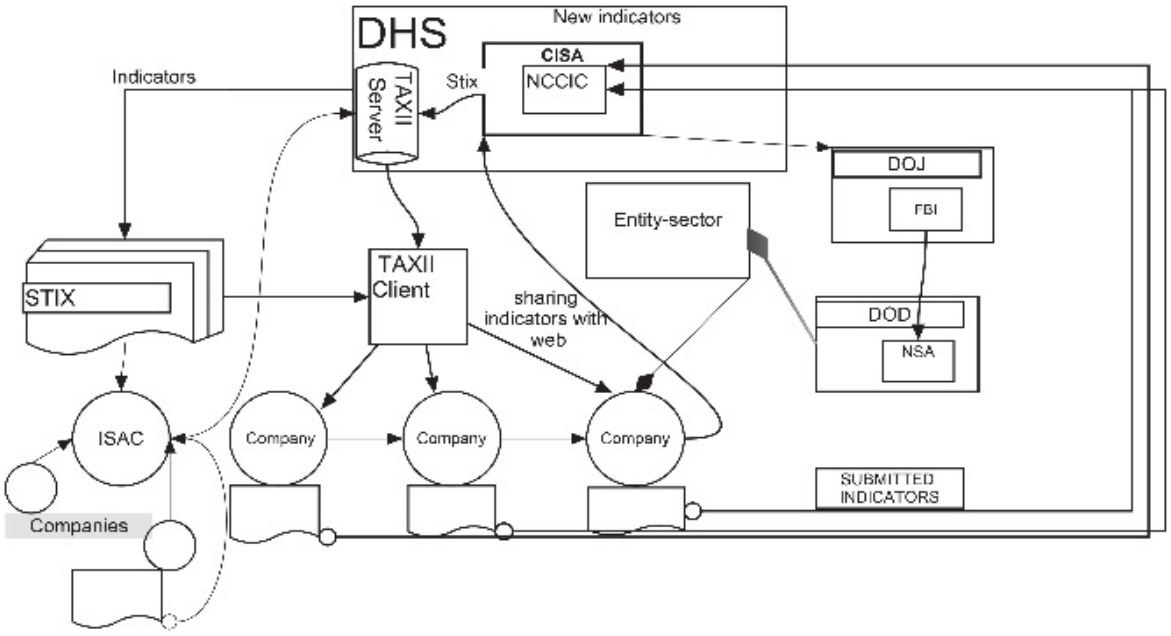


Figure 1: Cyber-information sharing model in the U.S.

Two-way models also allow public safety organizations to use gathered information for the prevention of hybrid threats before the domino effect is caused by two or more separate phenomena. It is important that cross-boarding cooperation work directly and instantly. Echo EWS will not work as a separate system but plays a crucial and parallel part in wider mechanisms, including the European-level situational awareness system of NATO. All Echo partners must understand that common language means in a wider manner—for example, taxonomies, techniques, procedures, and common ways to respond and act.

The U.S. Department of Homeland Security uses a system called Automated Indicator Sharing (AIS). AIS participants may connect to a national early warning system in the National Cybersecurity Center (NCSC) that allows also bidirectional sharing of cyber threat indicators. A server housed at each stakeholder´s (community) location allows the stakeholder to exchange indicators with the National Cybersecurity Center (NCCC) as **Figure 1** illustrates. Participants receive and can share DHS-developed indicators that they have observed in their own network defence efforts, which the national cyber situation centre will then share back out to all AIS participants. Stakeholders who share indicators through AIS will not be identified as the source of those indicators to other participants unless they consent to the disclosure of their identity. Senders are anonymous unless they want NCSC to share their identity (Hernandez-Ardieta, Tapiador & Suarez-Tangil 2013). Official cyber-security partners will vet the indicators they receive through AIS.

The government also needs useful information about indicators and other threat-informed data. Therefore, local NCSC should share at least weekly reports to the government situation centre. AIS utilizes the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications for machine-to-machine communication. STIX is a language and serialization format that enables organizations to exchange Cyber Threat Intelligence (CTI) in a consistent and machine-readable manner. Trusted Automated eXchange of Intelligence Information (TAXII™) is an application layer protocol used to exchange cyber threat intelligence (CTI) over the HTTPS (Department of Homeland Security 2019).

Collection-based communications indicate that a single TAXII client is making a request to a TAXII server and the TAXII Server carries out that request with information from a database. A TAXII channel in TAXII Server enables TAXII clients to exchange information with other TAXII clients in a publish-subscribe model. TAXII clients can push messages to Channels and Subscribe to Channels to receive published messages. A TAXII Server may host multiple channels per API root (MITRE 2018; OASIS Cyber Threat Intelligence [CTI] TC, DHS [CS&C] 2017b). TAXII is the main transport mechanism for Cyber Threat Information (CTI) represented in STIX. Stakeholders may share indicators with NCSC through an ISAC or an ISAO without being a TAXII client.

According to the Department of Homeland Security (2019) Cyber Threat Information is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor.

There are a wide range of the information-sharing methodologies and systems in law enforcement. For example, the main approach of the Europol Information System (EIS) is to be the reference system for offenses, individuals involved, and other related data to support EU member states, Europol, and its cooperation partners in their fight against organized cybercrime, terrorism, and

other forms of serious crime. For example, the European Cybercrime Centre (EC3), as a part of Europol, uses an open source based MISP platform (ENISA 2017). Malware Information Sharing Platform (MISP) is a tool for information sharing about malware samples and related malicious campaigns related to specific malware variants. It offers architectural flexibility and allows the use of a centralized platform (for example, CIRCL and FIRST instances), but also as a decentralized (peer-to-peer) platform.

Europol´s SIENA is a VPN (Virtual Private Network) designed to enable a swift, secure, and user-friendly exchange of operational and strategic crime-related information and intelligence between member states, Europol, law enforcement cooperation partners, and public safety organizations (EUROPOL 2019).

Databases of the Schengen Information System (SIS) and networks have also been established for the exchange of information on criminal records, on combating hooliganism, on missing persons or stolen vehicles, and on visas which have been issued or refused. DNA and fingerprint data help put a name to anonymous criminals who left crime scenes. EU legal instruments facilitate operational cooperation between member states, such as the setting up of collaborative investigation teams and the organizing of joint operations (European Council 2010).

Sharing digital information between stakeholders may include Common Vulnerabilities and Exposures (CVE) or CVE-ID and CVEs that include a list of common identifiers for publicly known cybersecurity vulnerabilities. For example, the HAVARO EWS solution exploits identifiers to detect threats. CVE Numbering Authorities (CNAs) are authorized organizations which assign CVE IDs to vulnerabilities affecting products within their distinct agreed-upon scope for inclusion in first-time public announcements of new vulnerabilities (MITRE Corporation 2019a). MITRE Corporation (2019b) CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities (MITRE Corporation 2019b).

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management. The NVD consists of databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics (NIST 2019).

In the CVE list feeds, NVD and CVE entries provide enhanced data for each entry—such as fix information, severity scores, and impact ratings. NVD also supplies advanced searching features (MITRE Corporation 2019a; 2019b).

Digital Forensics XML (DFXML) is an XML language. DFXML improves composability by providing a language for describing forensic processes (for example, cryptographic hashing), forensic work products (for example, the location of files on a hard drive), and metadata (for example, file names and timestamps) (Garfinkel 2012).

According to Garfinkel (2012), the Digital Forensics XML toolset is intended to represent the following types of forensic data:

- Metadata describing the source disk image, file, or other input information.

- Detailed information about the forensic tool that did the processing (for example, the program name, where the program was compiled, and linked libraries).
- The state of the computer on which the processing was performed (for example, the name of the computer, the time that the program was run, the dynamic libraries that were used).
- The evidence or information that was extracted (how it was extracted and where it was physically located); cryptographic hash values of specific byte sequences; operating-system-specific information useful for forensic analysis (Garfinkel 2012).

Conclusion

The fight against hybrid threats means not only preventing functions against cyberattacks, but also identifying, tracing, and prosecuting a criminal/criminal group. This means even multifunctional integration where existing intrusion detection/prevention systems complement new solutions in the future.

There are no essential barriers to increase collaboration in organizational, tactical, strategical, and technical levels between national CERTs, NATO Computer Incident Response Capability (NCIRC), and EU Computer Emergency Response Team (CERT-EU). Common E-EWS solution would create an effective way to respond to cross-boarding hybrid thread situations. All major companies whose businesses are involved with the vital functions of society should be connected to an early warning system.

The future HAVARO 2.0 that is under development reflects a tendency to develop early warning functions at the national level. However, this is not enough. Critical information must be able to share between EU member countries because several enterprises operate at the international level. Cross-border cyber threats force countries to exchange critical information within EU member countries and between EU and other western states. That means cyber risks have become common challenges.

Operative public safety functions require quicker response or even prediction. HAVARO 2.0 should utilize the Artificial Intelligence (AI) dimension to detect threats. It is not possible to design next-generation early warning information systems without machine learning as part of the Artificial Intelligence (AI) functionalities because the early warning system requires predictive features. Artificial Intelligence functionalities enable entities to exploit difference databases and produce characterized data more effectively than a human can; it may also come to a conclusion by learning from input information. In addition, AI can make a decision without human interaction. This means also that not every ECHO participant has the same potentiality or opportunity to develop national system architecture. International cyber-physical dimension of threats sets requirements, what should be the minimum cybersecurity level or requirements of cyber situational centers at the national level. Framework for the local, national, and international information sharing should follow the same principles in each EU member country. **Figure 2**, below, illustrates the simple formation of cybersecurity information sharing between countries in which HAVARO 2.0 may join. This example consists of separate national sub-hubs and one centralized hub. Information-Sharing participants do not exchange information with each other. All threat-informed data is shared via a hub.

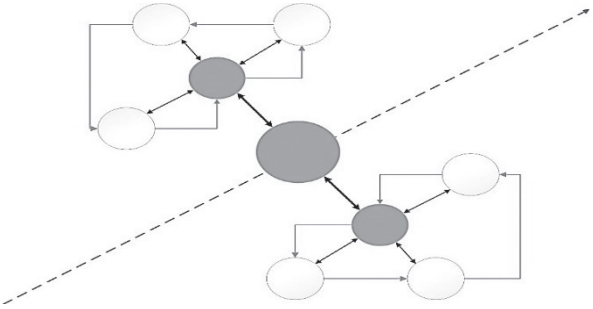


Figure 2: Connection between sub-hubs

Therefore, ISAC based national sectorial classification is the optimal way to share classified information as **Figure 3** illustrates.

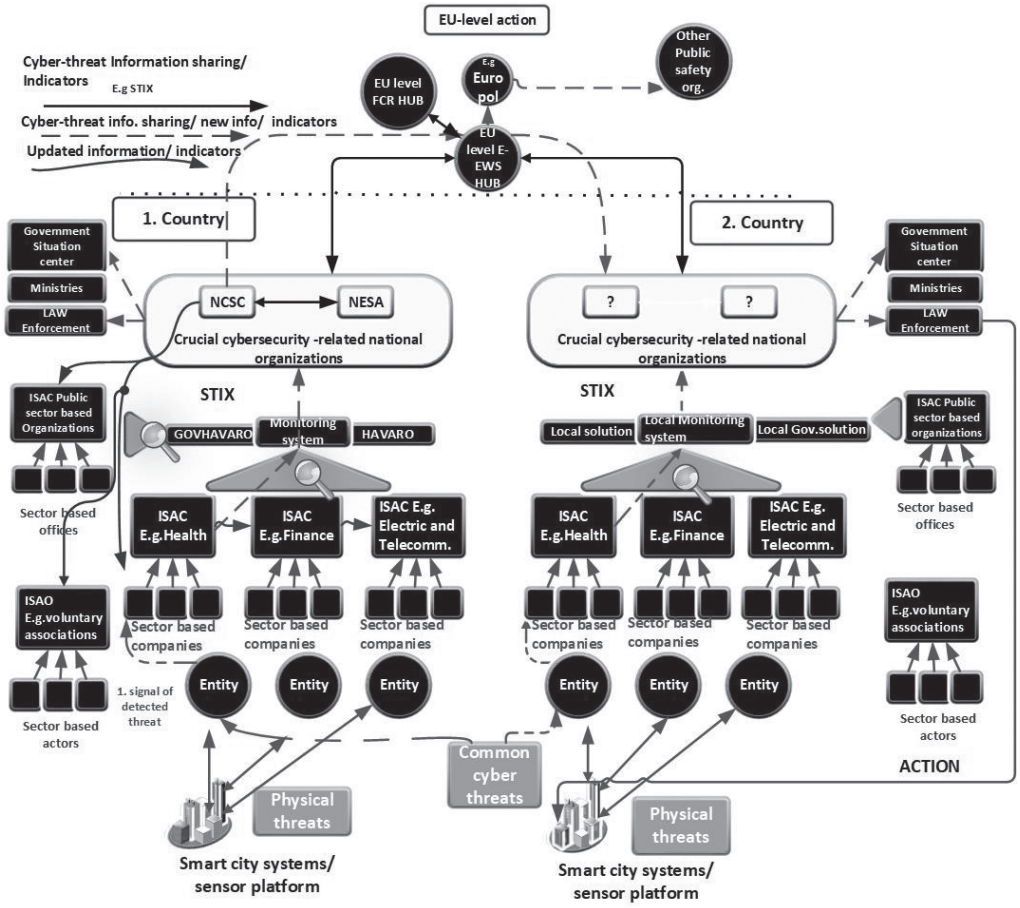


Figure 3: Proposed E-EWS information-sharing model

Figure 3 demonstrates information-sharing relationships and organizational structures concerning information sharing within a centralized hub system (countries, companies, public safety organizations, and other actors). In country number 1 (Finland), identifiers of the national Early Warning System (for example, HAVARO) detect a weak signal of cyberthreat concerning Internet traffic in a multinational enterprise. The national cybersecurity centre of country 2 has not noticed a cyberthreat activity. Automated Information Sharing functionalities produces crucial data for the central EWS hub, which shares relevant information in near real-time to the situation centres (CERT or

CIRT team). Sensitive data will be shared directly to the international public safety organizations and/or to the governments which are associated with the cyberthreat. NCSC of Finland uses a parallel subsystem for public organizations; HAVARO consists of separate early warnings solutions named "GovHavaro" for all public organizations.

Participants do not need to share information directly with each other, but there is a need to establish sector-specific communities—for example, ISAC and ISAO—that collect crucial information concerning the targeted sector of the critical infrastructure. This cybersecurity information is monitored and handled by national CERT or CIRT, and cybersecurity centres will share all new indicators between stakeholders (ISACs). All law enforcement-related information will be shared directly via EWS hub to the public safety authorities, such as EUROPOL or INTERPOL. Centralized EWS hub and sub-hubs are the simplest option for the national Finnish Early Warning System. On the other hand, a big challenge will be who maintains the central hub, and what its governance model would be.

Criticism concerning the use of STIX is justified, as mentioned above, and the problem needs to be rectified. More detailed guidelines, methods, standardization, and compliance with the law create a better operating environment to take advantage of automated indicator exchange.

Despite the invalidated privacy shield decision of the EU Court of Justice, there is a need to strengthen and to be aware of hybrid threats in a wider perspective. Privacy issues are important to protect. It is possible that the content of the privacy shield agreement needs to be changed. The agreement is significant in terms of commerce. Companies will now have to sign 'standard contractual clauses': non-negotiable legal contracts drawn up by Europe, which are used in other countries besides the U.S. (Court of Justice 2020).

References

Apuzzo, M 2019, 'Europe built a system to fight Russian meddling. It is struggling', *The New York Times*, viewed 1 November 2019, <https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html->.

Bolstad, C & Endsley, M 2000, 'The effect of task load and shared displays on team situation awareness, *The 14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society*, Santa Monica, CA, US.

Bromander S, Muller, EM & Jøsang A 2020, 'Examining the "known truths" in cyber threat intelligence – The case of STIX', *Proceedings of the 16th International Conference on Cyber Warfare and Security*, Old Dominion University, Norfolk, VA, US, pp. 493-502.

Court of Justice of the European Union 2020, 'The Court of Justice invalidates decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield', Press release No 91/20, 16 July , viewed 1 June 2020 <https://curia.europa.eu/jcms/jcms/p1_3117870/en/>.

Department of Homeland Security (DHS) 2019, 'Automated Indicator Sharing (AIS)', viewed 1 June 2019, <https://www.us-cert.gov/ais>.

Endsley, MR 1988, 'Design and evaluation for situation awareness enhancement', *Proceedings of the Human Factors Society 32nd Annual Meeting*, pp. 97-101.

ENISA 2017, 'Tools and methodologies to support cooperation between CSIRTs and law enforcement version 1.0' November, Heraklion, GR,

——& ITE 2017, 'Information sharing and analysis centres (ISACs) cooperative models', Heraklion, GR.

European Commission 2013, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,' viewed 3 June 2020, Brussels, BE, < https://eur-lex.europa.eu/procedure/EN/2023 69>.

——2016, 'EU-U.S. Privacy Shield: Stronger protection for transatlantic data flows', Brussels, BE.

——2019, '14. Secure societies: Protecting freedom and security of Europe and its citizens', *Horizon 2020 - Work Programme 2018-2020*.

European Council 2010, 'Internal security strategy for the European Union towards a European security model', General Secretariat of the Council, European Union, Brussels, BE.

European Parliament and the Council of The European Union 2016, 'Regulation (EU) 2016/679 of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation)', *Official Journal* L 119, 4 May, viewed 1 August 2019, <https://eurlex.europa.eu/eli/reg/2016/679/oj>.

EUROPOL 2019, 'Secure Information Exchange Network Application (SIENA)'. viewed 1 August 2019, <https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena>.

Garfinkel, S 2012, 'Digital forensics XML and the DFXML toolset', *Digital Investigation*, vol. 8, pp. 161-74.

GitHub 2019, 'Support your workflow with lightweight tools and features', viewed 7 July 2019, <https://github.com/MISP/MISP-Taxii-Server>.

Hernandez-Ardieta, JL, Tapiador, JE & Suarez-Tangil, G 2013, 'Information sharing models to cooperative cyber defence', *Proceedings of the 5th IEEE International Conference on Cyber Conflict (CyCon) 2013*, pp. 1-28.

International Organization for Standardization 2011, 'Information technology — Security techniques — Biometric information protection ISO/IEC 24745:2011', viewed 5 July 2020, <https://www.iso.org/standard/52946.html>.

——2015, 'Security techniques information security management for inter-sector and inter-organizational communications', ISO/IEC 27010:2015, viewed 5 July 2020, <https://www.iso.org/standard/68427.html>.

——2019, 'Metadata registries (MDR) — Part 7: Metamodel for data set registration', ISO/IEC 11179-7:2019, viewed 5 July 2020, < https://www.iso.org/standard/68766.html>.

KPMG 2013, 'IDS:N käyttöönotto herättää todellisuuteen', viewed 5 July 2019, <https://www.hackingthroughcomplexity.fi/2013/04/idsn-kayttoonotto-herattaa.html>.

Ladid, L, Armin, J & Kivekäs H 2019, 'The Finish electronic communications regulator TRAFICOM - A cybersecurity reference model for Europe', SAINT Consortium/ TRAFICOM, Helsinki, FI.

Lehto, M, Limnéll, J, Kokkomäki, T, Pöyhönen, J & Salminen, M 2018, '*Kyberturvallisuuden strateginen johtaminen Suomessa* No. 28', *Valtioneuvoston kanslia*, Helsinki, FI.

MITRE Corporation 2018, 'Trusted Automated eXchange of Indicator Information - TAXII™ enabling cyber threat information exchange', U.S Government.

——2019a, 'Common vulnerabilities and exposures', viewed 6 July 2020, <https://cve.mitre.org/cve/cna.html>.

——2019b, 'CVE-details', viewed 6 June 2020, <https://www.cvedetails.com/cve-help.php>.

Munk, S 2018, 'Interoperability services supporting information exchange between cybersecurity organisations', *Academic and Applied Research in Military and Public Management Science*, vol. 17, no. 3, pp. 131-48.

National Cybersecurity Center-Finland (NCSC-FI) 2017, '*Viestintäviraston kyberturvallisuuskeskuksen palvelut*', Brochure Cybersecurity services of the NCSC-FI. Helsinki: TRAFICOM.

——2019, 'Havaro service and FAQ', viewed 5 July 2020, <https://www.kyberturvallisuuskeskus.fi/en/havaro-service>.

NIST 2019, 'National vulnerability database - General information', viewed 1 September 2019, <https://nvd.nist.gov/general>.

OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017a, 'STIX™ version 2.0. Part 2: STIX objects No. stix-v2.0-wd03-part2-stix-objects) OASIS open'.

——2017b, TAXII™ version 2.0. 'Committee specification 01 No. taxii-v2.0-cs01) OASIS Open'.

Secretariat of the Security Committee 2019, 'Finland´s cybersecurity strategy - Government resolution', Ministry of Defense, Helsinki, FI.

Simola, J & Rajamäki, J 2017, 'Hybrid emergency response model: Improving cyber situational awareness', *Proceedings of the 16th European Conference on Cyber Warfare and Security*, University, College, Dublin, IE, pp. 442-51.

United States Department of Commerce 2020, 'The Privacy Shield framework in the United States', viewed 6 July 2020, <https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text>.

White House 2013a, 'Critical infrastructure security and resilience', Presidential Policy Directive, USC.

——2013b, 'Federal register - Improving critical infrastructure cybersecurity, Part III - Executive Order 1363', vol. 77, USC.

IX

SAVING LIVES IN A HEALTH CRISIS THROUGH THE NATIONAL CYBER THREAT PREVENTION MECHANISM CASE COVID-19

by

Jussi Simola, 2022

Chapter in the book titled Cyber Security: Critical Infrastructure Protection

https://doi.org/10.1007/978-3-030-91293-2_12

Saving Lives in a Health Crisis Through the National Cyber Threat Prevention Mechanism Case COVID-19

Jussi Simola

Faculty of Information Technology,

University of Jyväskylä, Jyväskylä, Finland

e-mail: jussi.hm.simola@jyu.fi

Abstract Today's ongoing coronavirus pandemic has shown that our overall public security mechanism in Finland requires a more coherent system that combines different types of sensors with artificial intelligence-based systems. Various states may have a crucial task: creating a common early warning system with a cyber dimension. But first, the decision-making process for public safety administration must be enhanced at the national level. COVID-19 has demonstrated the difficulty of predicting the progression of a pandemic, and nearly every country on earth has faced remarkable challenges from the spread of disinformation. False information has been shared around many public health and safety-related issues—such as how the virus is spread, the usefulness of self-protection, and the side effects of vaccines. Effective early warning tools are needed to prevent the domino effect of misinformation and to ensure the vital functions of society. This research will demonstrate the need for a common emergency response model for Europe to ensure national public safety—along with a technical platform at least for the interface between the countries. Hybrid-influenced incidents require a hybrid response.

Keywords Pandemic · Emergency response · Early warning · Information sharing Situational awareness

1 Introduction

In Finland, the Ministry of Social Affairs and Health (STM) and the Finnish Institute for health and Welfare (THL) are the organizations responsible for ensuring the virus does not spread. Finland's Emergency Response Administration is responsible for the crucial administrative functions around warning and alerting the public.

It is vital to note that the ongoing COVID-19 pandemic crisis constitutes just one version of the emerging viruses that are spreading. In Finland, official reports have shown no crucial weaknesses in the national preparedness level; the society's current state of vital functions is stable. Yet there is a need to enhance, for example, strategic management, political commitment, international activities, situational

awareness, the protection of vital functions, legislation, and strengthening cyber security as a national competitive advantage, and as a part of overall security [32]. The vital functions of society allow it to maintain its resiliency. Meanwhile, the problems that now have emerged in central administration and middle-level administration reflect challenges around reliable information sharing and the use of evidence-based information.

Situational awareness has been lacking, for nearly the entire period of response to the COVID-19 crisis. A concise and easy-to-understand summary of the general guidelines has not been provided to citizens. This is compounded by other challenges. First, legitimate jurisdictional issues have caused political confrontation; the responsibilities of officials and politicians have been unclear for some time. Second, pandemic preparedness plans and action plans will not produce added value if they are not implemented. The political and administrative debate around separation of powers between government ministries has caused major problems in the coordination of decision-making. It is not enough merely to attempt to survive the daily challenges around the virus pandemic, while the potential for new incidents of misinformation, cybercrime incidents or public health crisis increases [50]. For example, the limited patient care capacity of hospitals makes it difficult to cope with a simultaneous accident. Yet government resources are insufficient to be distributed everywhere they are needed.

At present, Finland's social and healthcare system is overloaded. Tens of thousands of patient records were stolen from the Finnish therapy center Vastaamo [33]. The patient records of several officials and politicians have been leaked to the secret Tor network, and victims of such crimes have been subjected to blackmail [33]. Sensitive and personal data must be protected in the Finnish healthcare system and in addition at the European level. Along with grave privacy breaches like these, nearly every country has faced massive challenges due to the spread of misinformation through media and social media. Such misinformation has driven a divergence in people's perceptions and understanding of critical facts around the pandemic—as well as around the response chosen by decision-makers. False information has been shared around crucial public health and safety-related issues, including how the virus is spread, the benefits of self-protection, and vaccinations.

In this chapter, our research problem is formulated in Sect. 2.2. Section 2.3 discusses basic problems around the formation of situational awareness in a pandemic situation. Section 2.4 handles the central concepts of our review. Section 2.5 describes previous studies conducted by the researcher. Section 2.6 presents the findings and Sect. 2.7 provides discussion and conclusions.

2.2 Problem Formulation

The public debate on COVID-19 has pitted economic development and security against each other. Good economic development can help create security, because sufficient wealth provides an opportunity to create well-being and security. Lack of wealth will increase insecurity.

How can we find a balance in the flow of information? Information warfare has created barriers to forming a coherent situational picture of the COVID-19 pandemic. Figure 2.1 illustrates the formation of crisis information nationally among citizens, media (including social media), and states' decision-makers. It also shows the second crucial element: foreign influencers, including the press, scientific researchers, authorities, and politicians.

The overall formation of a situational picture has been notably difficult. Finland's government officials and members of the government have relied heavily on the World Health Organization's (WHO's) statements about the global spread of the COVID-19 pandemic. Yet is it sufficient to use one or two international organizations as sources, to support decision-making at the state level? The WHO predicted an ongoing pandemic a year ago [15]. It has been argued that WHO executives' connections with the Chinese administration would have prevented a rapid, transparent, and effective information exchange with other countries [3]. This is why we need an early warning system, at least at the European level—one that more quickly takes into account changing threat factors across the world. We need to be able to analyze raw data more quickly, we need to be able to find health abnormalities faster.

The fight against cross-border health threats requires excellent preparation and coordinated action—before, during, and after the crisis. We must be able to process and analyze scientific research more quickly. We must also be able to compile data into a sensible map of measures to be taken, and these strategic measures must be implemented quickly enough to suppress crises like pandemics on time. Solutions

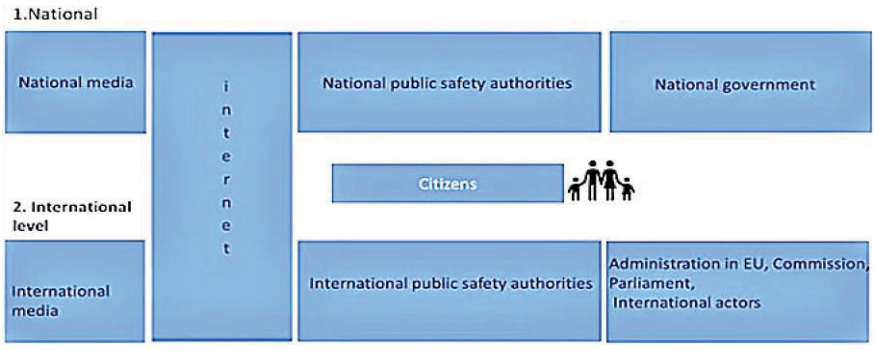


Fig. 2.1 Formation of crisis information

utilizing artificial intelligence can help enormously, in such a rapidly evolving event process.

It is problematic that no separate operational "power team," or even national science adviser, has been used to advise the government of Finland. Italy was left nearly alone in its struggles against COVID-19, despite claims that the EU was acting as one front. While the European Union did not effectively work towards a common goal, it did coordinate some issues concerning all member states and placed a joint order on masks. Yet Finland was left out EC [10]. The availability of protective equipment created an almost warlike situation among different European countries.

The purpose of this publication is to look for those factors and influences that pose obstacles to our preventing the spread of a pandemic. Our focus is on a proposed hybrid model of alarm functions—as seen in Fig. 2.2—taking advantage of the scope of a cyber early warning system [53]. The study particularly emphasizes the decision-making capacity and formation of situational awareness of the Finnish government, the National Institute for Health and Welfare, and the Ministry of Social Affairs and Health. Specifically, we tackle the question of how to reduce the role of disinformation and misinformation in the state-level decision-making process. We explore how it is possible to use a hybrid emergency response model to solve multiple problems around crisis management, especially when several threats occur at the same time. For example, the combined crises of a coronavirus pandemic and cyberattacks can easily overload public safety organizations' workflow. Preventing the domino effect can become still more challenging, if separate or overlapping problem-solving methods are used in crisis management.

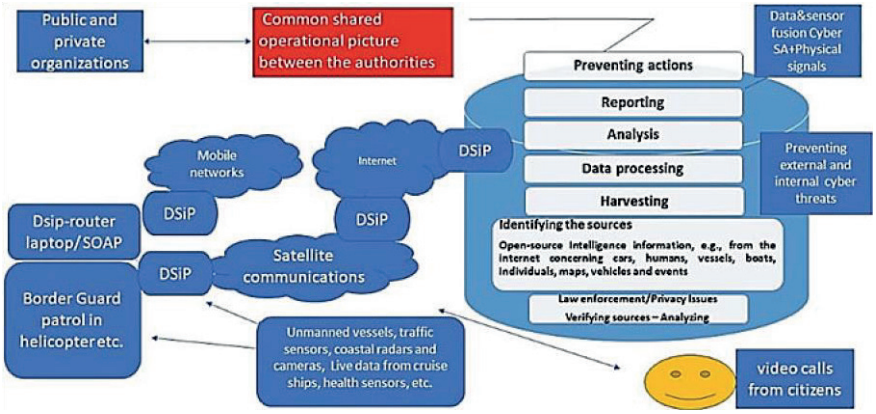


Fig. 2.2 Hybrid emergency response model (HERM)

2.3 Challenges in the Decision-Making Process with COVID-19

As the COVID-19 pandemic has shown, an international cross-border crisis can spread very quickly. It is thus crucial that decision-makers effectively share information—including around the fact that public safety organizations' preparedness levels are not sufficiently high.

2.3.1 Situation in Finland

Finland's citizens noted an enormous lack of correct information around COVID19 at the end of February 2020 [62, 65]. Ministers and responsible authorities failed to immediately offer guidelines for controlling COVID-19. In March 2020, the ministers of social affairs and health did not know how the tasks should be divided between them [20, 31]. Several countries recommended the use of protective masks. Following this, the National Emergency Supply Agency argued that it did not have enough protective masks in stock. Finland did not recommend the use of masks [28], and the masks were later reported to be out of date [35]. Eventually, the Ministry of Social Affairs and Health began to order the masks, but they did not pass the test carried out by VTT Technical Research Centre of Finland [61]. The manager of the Ministry of Social Affairs and Health and The Finnish Institute for Health and Welfare (THL) also held a different view regarding the benefits of using masks [39, 44]. THL recommended the use of masks, but the Ministry of Social Affairs and Health doesn't.

At present, our government employs more political assistants than ever before [56]. Managing the administration is thus becoming cumbersome. State leaders need decision-making support, such as via artificial intelligence tools, to enhance administrative efficiency. External pressure has had marginal effects on the overall decision-making process, except for in the case of a few decision-makers [64]. Information about the pandemic has been made available for the decision-makers, but the response has been slow and little scientific information from abroad has been shared with the public.

In Finland, the guidelines set by the WHO have been interpreted from a national political perspective. Exceptional conditions were imposed, including a separate regional movement restriction, on the Uusimaa region. The purpose was to prevent the COVID-19 from spreading outside the metropolitan area. Despite that, it was possible to fly relatively freely between Finland and other countries for months. The classification of pandemic countries, based on disease quantity, was incomplete. Statements made by a few doctors about the development of the COVID-19 pandemic have also posed challenges to forming a coherent picture of the situation [18, 34]. They believe that by letting the coronavirus rip through the population to infect people, it is possible to achieve so-called herd immunity.

The decisions made by various Nordic countries to prevent the spread of COVID19 have differed and continue to differ. This is also true amongst EU member countries. Sweden began to seek herd immunity for its citizens and allowed the disease to spread almost freely [21]. Finland started by following the Swedish COVID-19 strategy, but its selected strategy changed after the president intervened in the government's decision-making process [64]. After considering the situation—as well as the grounds for declaring a state of emergency by the President of the Republic and the government—the government announced a state of emergency in Finland on 16 March, 2020 [23]. The Finnish Parliament applied the Emergency Powers Act on 18 March, 2020. Regional restrictions were then put into effect, preventing needless travel among the country's regions [60].

Only one technical solution is currently in use for COVID-19 prevention. The Finnish Corona Blinker, "Koronavilkku"—an application developed by Solita and the Finnish Institute for Health and Welfare—was released in August 2020 [54]. Soon after, crucial problems were found in the app's ability to track infected people. When a person infected with coronavirus reported their infection to the app, the warning failed to reach other users of the app. Another crucial problem was the delay between a user reporting an infection and the app's recording of it. A one week delay slows or prevents infection chain tracing [63]. Another challenge to infection tracing is that users do not have to inform the app when they learn they have COVID-19.

There is also an online service called "omaolo". You can do an online medical check-up for COVID-19 symptoms on the internet, if you suspect you have a coronavirus infection [8]. It is free of charge and the service guides the patient to take a test or go to a hospital, if there is a need.

2.3.2 Case Vastaamo

As mentioned above, tens of thousands of patient records were stolen from the Finnish psychotherapy center Vastaamo [40]. Criminals can use stolen personal data in many ways. For example, they can try to blackmail or otherwise influence the victims. Finland's National Bureau of Investigation (KRP) has received over a thousand reports of offenses connected to the hacking and blackmailing case revolving around Vastaamo [41].

Kanta produces digital services for the social welfare and healthcare sector in Finland. According to [30], each organization associated with Kanta services has at least one Kanta-access point. Access to the service can either be carried out as an organization's activity or implemented by the organization. That means, the Kanta subscriber has an integration solution through which several systems, organizational units, or organizations are connected to the Kanta services. The purpose of the integration solution is to route messages to application servers that may be located in different organizational units or organizations. It is also possible to connect to the

service via an external access point. In this model, the organization has joined the Kanta services through a Kanta access point implemented by an intermediary.

The organization may have externalized information system (e.g., a shared information system as a SaaS), messaging, and/or communications to an intermediary. There can be several access points (and server certificates) if, for example:

- the organization's units are directly connected to Kanta services from different information systems, without a centralized integration solution (messaging solution);
- the organization's reception services (for example, receipt of renewal requests) are located on a server other than that from which its systems connect to Kanta services [30].

Valvira is a national agency operating under the Ministry of Social Affairs and Health. Vastaamo is a service provider approved and supervised by Valvira. Its information system is part of the Category B systems regulated by law, for which the law does not require an external assessment of data security. Vastaamo's patient information system was developed by Vastaamo itself. It is one of 260 social and health care information systems that are monitored by the authorities only if there are particular information security-related reasons to suspect problems, or if the service provider requests it [48].

Class B patient information systems are registered with Valvira under the Customer Information Act. They may be purchased as commercial products or manufactured by the company itself. According to Valvira, their monitoring is very limited due to resource problems. It is possible that patient information from Kanta could also be stored in a private register, allowing just one healthcare professional at a time—and one who is in a care-giving role with the patient—to process patient data.

2.4 Central Concepts

This section introduces the central concepts related to the research framework and defines the meaning of the concepts, and used terminology.

2.4.1 Artificial Intelligence

Artificial intelligence (AI) is part of a system that engages in intelligent behavior by analyzing the environment and taking multiple actions—with a dimension of autonomy—to achieve specific goals [9]. AI-based systems can be software-based and act in the virtual world (e.g., image analysis software, search engines, shape and face recognition systems). AI can also be embedded in hardware devices (e.g., advanced robots, autonomous cars, unmanned vehicles, drones or Internet of Things applications) [9].

An *Intelligent Agent* (IA) is an entity that produces decisions. This allows, for example, for the performance of specific tasks for users or applications. An IA has the ability to learn during the process of performing tasks. Its two main functions are perception and action. Intelligent Agents form a hierarchical structure that comprises different levels of agents. A multi-agent system is one that consists of a number of agents interacting with one another [58] in combinations that can help solve challenging societal problems. An IA can behave in three ways: reactively, proactively, and socially [58].

2.4.2 Legislation and Regulation

Per the Emergency Powers Act, if Finland's government—in liaison with the President of the Republic—finds that exceptional circumstances exist in the country, a government decree can be issued to apply the provisions of this act (commissioning regulation). Said decree may be issued for a fixed period [13].

The ISO/IEC 27001 formally specifies an Information Security Management System (ISMS). This comprises a suite of activities concerning the management of information risks called "information security risks" in the standard ISO [27]. Information security management is an essential part of management, which should be supported by the management system. Information security ensures the confidentiality of information, as well as its availability and integrity.

ISO 27799:2016 defines guidelines for organizational information security standards and information security management practices—including the selection, implementation, and management of controls—taking into consideration the organization's information security risk environment(s). It defines guidelines to support the interpretation and implementation of the health informatics of the ISO/IEC 27002 and is a companion to the international standard ISO [26].

ISO/IEC 27032:2012 guides enhancing the state of cybersecurity, along with drawing out the unique aspects of that activity and its dependencies on other security domains—in particular: information, network, internet security, and critical information infrastructure protection (CIIP) ISO [24].

ISO/IEC 9001:2015 provides practical guidance on managing the total service produced for the customer. It also enables the healthcare organization to demonstrate that it meets customer satisfaction requirements and develops customer satisfaction by managing the risks of the operating environment International Organization for Standardization [25].

2.4.3 Situational Awareness

The Ministry of Defence of Finland [45] describes situational awareness as decision-makers' and their advisors' understanding of what has happened, the circumstances under which it has happened, the goals of the different parties, and the possible development of events. All of these are needed to make decisions on a

specific issue or range of issues. A general definition of situational awareness is the perception of the elements in the environment within time and space, the comprehension of their meaning, and the projection of their status into the near future [12].

According to [14], cyber situational awareness is a subset of situational awareness—it comprises the part of situational awareness that concerns the cyber environment. Such situational awareness can be reached, for example, by the use of data from IT sensors (intrusion detection systems, etc.) that can be fed to a data fusion process or that can be interpreted directly by the decision-maker.

2.4.3.1 Command and Control

A command center is any place that is used to provide a centralized command for some purpose. An incident *command center* is located at or near an incident, to provide localized on-scene command and support from the incident commander. Mobile *command centers* may be used to enhance emergency preparedness and back up fixed command centers. Command centers may also include Emergency Operations Centers (EOC) or Transportation Management Centers (TMC).

Supervisory Control and Data Acquisition (SCADA) systems are basically Process Control Systems (PCS) that are used for monitoring, gathering,and analyzing real-time environmental data—whether from a simple office building or a complex nuclear power plant. PCSs are designed to automate electronic systems based on a predetermined set of conditions, such as traffic control or power grid management [16].

According to [16], SCADA systems' components may involve operating equipment such as valves, pumps, and conveyors that are controlled by energizing actuators or relays. Local processors communicate with the site's instruments and operating equipment—including a Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED), and Process Automation Controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment. SCADA also consists of instruments in the field or a facility that sense conditions such as power level, flow rate, or pressure. Short-range communications involve wireless or short cable connections between local processors, instruments, and operating equipment. Long-range communications between local processors and host computers cover a wide area—using such methods as satellites, microwaves, frame relays, and cellular packet data. The host computer acts as the central point of monitoring and control. This is where a human operator can supervise the process, as well as receive alarms, review data, and exercise control. The system may consist of automated or semi-automated processes. A Networked Control System (NCS) is a control system where in the control loops are closed through a communication network. The defining feature of an NCS is that control and feedback signals are exchanged

among the system's components, in the form of information packages, through a network CSPC [4, 49].

RIDM is a risk-based decision-making process that provides a defensible basis for making decisions. It also helps to identify the greatest risks and to prioritize efforts to minimize or eliminate them. Risk-informed decision-making (RIDM) is a deliberative process that uses a set of performance measures, together with other considerations, to "inform" decision-makers' choices [66, 36].

2.4.3.2 Management of Situational Awareness at the National Level

The Ministry of Finance of Finland is responsible for the steering and development of the state's information security [45, 50]. Government situation centers ensure that Finland's state leaders and central government authorities are kept continuously informed. Finland's government situation centre was set up in 2007. It is responsible for alerting the government, permanent secretaries, and heads of preparedness—and for calling them to councils, meetings, and negotiations at exceptional times—as required by a disruption or a crisis.

The ministries must submit the situational picture for their entire administrative branch to the government situation center and notify the center of any security incidents in their field of activity. In urgent situations, the government situation center also receives incident reports for security incidents directly from the authorities. The government situation center also follows public sources and receives situational awareness information, in its role as the national focal point for certain institutions of the European Union and other international organizations.

2.4.4 Elements of Critical Infrastructure

Very often, Critical Infrastructure is defined from the view of the public sector despite it also consists private personnel and their activities as well as public operators of assets, systems, and networks. A very common public-private partnership approach ensures cooperation and information exchange intended to protect vital functions of the society. The human, physical and cyber assets provide many critical services that are necessary for a secure society.

2.4.4.1 Classification of the Critical Infrastructure in the United States

In the United States, critical infrastructure refers to those systems and assets, whether physical or virtual, that are deemed so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health, or safety, or any combination of those matters [46].

The U.S. Department of Homeland Security identifies 16 different sectors for the classification of critical infrastructure [7]:

1. Chemical,
2. Commercial facilities,
3. Communications,
4. Critical manufacturing,
5. Dams,
6. Defense industrial base,
7. Emergency services,
8. Energy,
9. Financial services,
10. Food and agriculture,
11. Government facilities,
12. Healthcare and public health,
13. Information technology,
14. Nuclear reactors, materials, and waste,
15. Transportation systems, and
16. Water wastewater system

Cyber threats—such as, for example, phishing attempts, blackmailing attempts, and hacking incidents—are an ever-changing threat to cyber systems across the sectors.

According to the National Institute of Standards and Technology NIST [38], the framework applied in the U.S. is also well suited to Finland. The risk management framework consists of three elements of critical infrastructure (physical, cyber, and human), which are explicitly identified and should be integrated throughout the steps of the framework. The critical infrastructure risk management framework supports a decision-making process, which critical infrastructure actors or partners collaboratively undertake to inform their selection of risk management actions. It has been designed to provide flexibility for use in all sectors, across geographic regions and by various partners. It can be tailored to dissimilar operating environments and applies to all threats [7].

The risk management concept enables the critical infrastructure actors to focus on those threats and hazards that are likely to cause harm and to employ approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience, by identifying and prioritizing actions to secure the continuity of essential functions and services and support enhanced response and restoration [7].

According to the Department of Homeland Security [7], the first point recommends setting *infrastructure goals and objectives*, which are supported by objectives and priorities developed at the sector level. To manage critical infrastructure risk effectively, actors and stakeholders must identify the assets, systems, and networks that are essential to their continued operation, considering

associated dependencies and interdependencies. This dimension of the risk management process should also identify *information and communications technologies* that facilitate the provision of essential services.

The third point recommends *assessing and analyzing risks*. These risks may comprise threats, vulnerabilities, and consequences. A threat can be a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Vulnerability-based risk may occur due to a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. A consequence can be the effect of an event, incident, or occurrence. *Implementing* risk management activities means that decision-makers prioritize activities to manage critical infrastructure risk based on the criticality of the affected infrastructure, the costs of such activities, and the potential for risk reduction. The last element, measuring effectiveness, implies that the critical infrastructure actors evaluate the effectiveness of risk management efforts within sectors and at national, state, local, and regional levels by developing metrics for both direct and indirect indicator measurement [7].

2.4.4.2 Smart Grid System and the Internet of Things

The Internet of Things (IoT) connects systems, sensors, and actuator instruments to the broader internet. The IoT allows things to communicate and exchange control data and other necessary information, while executing applications towards a machine goal [11].

The idea of the Internet of Things was developed in parallel to Wireless Sensor Networks (WSN). Sensors are everywhere: in our vehicles, in our smartphones, in factories controlling CO_2 emissions, and even in the ground monitoring soil conditions in vineyards. A WSN can generally be described as a network of nodes that cooperatively sense and may control the environment, enabling interaction between persons or computers and the surrounding environment. The development of WSNs was inspired by military applications—notably, for surveillance in conflict zones [2].

The Internet of Things is an emerging paradigm of internet-connected things that allows physical objects or things to connect, interact, and communicate with one another—similarly to the way humans talk via the web in today's environment. It connects systems, sensors, and actuator instruments to the broader internet [11].

The IoT allows things to communicate and exchange control data and other necessary information, while executing applications towards machine goal. The Internet of Things (IoT) is also impacted by the industrial sector, especially for industrial automation systems in which internet infrastructure makes it possible to gain extensive access to sensors, controls and actuators, with the intention of increasing efficiency [11].

Cybersecurity risks should be addressed as organizations implement and maintain their smart grid systems. According to the National Institute of Standards and Technology NIST [37], the smart grid system provides the most efficient electric network operations based on information received from consumers.

A smart grid system may involve a discrete IT system of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A smart grid system may also consist of operational technologies (OT) or industrial control systems (ICS), including SCADA systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLCs) [5, 37].

The Industrial Internet of Things (IIOT) collects data from connected devices(i.e., smart connected devices and machines) in the field or plant. It then processes this data, using sophisticated software and networking tools. The entire IIOT requires a collection of hardware, software, communications and networking technologies [11].

2.4.4.3 Intelligence Solutions for Public Safety Organizations

Open-Source Intelligence (OSINT) is any unclassified information, in any medium, that is generally available to the public—even if its distribution is limited or only available upon payment. OSINT is defined as the systematic collection, processing, analysis and production, classification, and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security ATP [1, 17, 43].

Social Media Intelligence (SOCMINT) identifies social media content in particular as both a challenge and opportunity for open-source investigations [55]. BigData is associated with OSINT and includes processes for the analysis, capture, research, sharing, storage, visualization, and safety of information. Big Data offers the ability to map standards of behavior and tendencies [47]. The availability of worldwide satellite photography, often of high resolution, on the web (e.g., Google Earth Pro) has expanded open-source capabilities into areas formerly available only to major intelligence services [14]. In the proposed hybrid emergency response model [52, 53] OSINT and SOCMINT features are integrated into the automated HERM as a part of an AI-driven decision support tool.

Threat information is any information related to a threat, which might help an organization protect itself against a threat or detect the activities of an actor [29]. Indicators are used to detect and defend against threats. These include the(IP)address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, or a Uniform Resource Locator that references malicious content. Tactics, techniques, and procedures (TTPs) describe the behavior of an actor. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism, or exploitative strategy. Security alerts are vulnerability notes. Threat Intelligence reports are

documents describing threat-related information that is transformed, analyzed, or enriched to provide important context for the decision-making process. Tool configurations are recommendations for using mechanisms that support the automated collection, exchange, processing, analysis, and use of threat-related information. They may comprise information on how to install and use a rootkit detection utility or on how to create, for example, router access control lists (ACLs) [29].

2.5 Previous Works

The multi-methodological approach that has been used in previous studies [52, 53] consists of four case study research strategies [42]:

1. theory building,
2. experimentation,
3. observation, and
4. systems development.

[59] identifies five components of research design for case studies:

1. the questions of the study,
2. its propositions, if any,
3. its unit(s) of analysis,
4. the logic linking the data to the propositions, and
5. the criteria for interpreting the findings.

According to [22] (Chap. 2), information systems and organizations are complex, artificial, and purposefully designed. Such a problem-solving paradigm must lead to an artifact that solves the identified problem. This review concentrates on comparing how the proposed emergency model [52, 53] suits a pandemic situation in which information warfare is an ongoing process. Scientific publications, articles, and literary material have been comparatively reviewed with this aim. The review subject comprises the public safety organizations, procedures, and vital functions of Finland society.

The first purpose of this qualitative review was to analyze pandemic-related management and information-sharing risks, along with the formation of situational awareness, from the view of continuity management. We apply the modified risk assessment framework in this review. The second purpose was to find any hidden administrative and managerial-related state-level risks that are outside the official risk classification. A simple process model helps identify those fundamental hidden management-related factors that affect to the implementation process of the next-generation emergency response model proposed by [52].

2.6 Findings

In Finland, as we have seen, more than one factor influences the decision-making process at the state level. We have local and regional level administrations that form situational awareness from the view of their territorial region; decision-makers then share regional instructions and guidelines with the people. There are local corona teams that are responsible for regional security. Currently, tasks are separate from the government at the regional level and the members of the government do not give absolute commandments, such as mandatory instructions for using masks. Yet the continued lack of clarity around the workflow is a crucial barrier, when the purpose is to share relevant information with the right audience at the right time. It has been seen previously that labor movement or trade unionism can produce an agitating counterforce, by means that are not ethically valid. If the challenges to fighting the COVID-19 pandemic emerge from the nation's citizens, then the fundamental problems lie more deeply within the constructs of society.

Finland does not have an operative command and control institution for unexpected crises. The president of Finland leads foreign policy with the government, but there is no operative commander role for the president in the country's internal affairs. The ongoing COVID-19 crisis has shown that there is a lack of information exchange—both between the authorities and between the authorities and politicians. Yet citizens have likewise been kept unaware of the guidelines that should be followed. For small- or medium-sized social and healthcare companies, information security is based on self-monitoring. Public healthcare organizations also base their oversight of these operations on self-monitoring. The National Supervisory Authority for Welfare and Health (Valvira) supervises, for example, private sector licensing, healthcare, social welfare, legal protection, legal rights, and technologies [57]. A single staff member is responsible for supervising all issues like information security and privacy protection, around the Kanta-register [19].

This is not enough—especially since criminals may use private information in a variety of extremely dangerous ways. For example, criminals may try to affect the decision-making process by blackmail. A major information-sharing problem seen in the Vastaamo case was the fact that a data breach had occurred nearly two years before it was detected. There are no crucial privacy issue-related barriers to using the proposed hybrid emergency response model within a smart city infrastructure. When an alarm-based early warning procedure for data leakage is automatized, it offers possibilities to enhance privacy protection and other protective functions [51]. The proposed hybrid emergency response solution may also use sensors called flu-sensors, which can transfer data in real time from a public area—for example, from a shopping center—to the Hybrid Emergency Response Center. Data about virus particles might then indicate a need for mall closure, the early warning would allow this to be carried out immediately.

2.7 Discussion and Conclusions

By comparing different countries, crucial factors influencing the formation of information sharing can be found. For example, Finland is almost the only country in Europe that does not use scientist experts as advisors in the decision-making process at the state level. If decision-makers keep their eyes open, they can find massive amounts of research from foreign sources on how the coronavirus spreads and how its spread can be prevented.

First, there is a fundamental need to regulate new guidelines for the higher level crisis management and command relationships for exceptional circumstances. Temporary provisions should be made for emergency situations, which may require imposing restrictions on citizens. There must be one incident team whose leader is from the central government. This leader should take control when adjutants and instructors have too much information to share, since it is difficult to gather the correct information from a large amount of the data in a time of crisis. To date, there have been too many assistants involved in the decision-support mechanism at the state level.

In the future, it is necessary to begin using artificial intelligence solutions to support decision-making. The proposed next-generation hybrid emergency model uses artificial tools to generate information for decision-makers. Algorithm-based decision-support and decision-making mechanisms make the system effective. As Fig. 2.3 illustrates, the crucial factors in the hybrid risk management framework are risk-informed decision-making (define risks and information), continuity risk management (handle risks continuously), and hybrid emergency response solutions (emergency operations). Because human beings are still decision-makers, people are responsible for the decisions they have made. Yet it is possible to combine human-based guidelines for risks and AI-driven decision-making [6].

This solution offers two possibilities to use automation. At the first level, automated protection functions are connected to semi-public spaces (e.g., shopping centers) and public open places (e.g., gardens). For example, a health sensor called "flu" may start an evacuation process if it observes several deviations from the guideline values. At the second level, an AI-aided decision support mechanism outputs analytical reports for the state level decision-makers. This level will greatly enhance the decision-making process, since the need for assisting staff will be reduced in high-level decision-making.

As mentioned above and illustrated in Fig. 2.4, the authorities' information sharing process must move towards automated functions. Still, it is an important western tradition that a parliament is democratically elected by the country'scitizens.

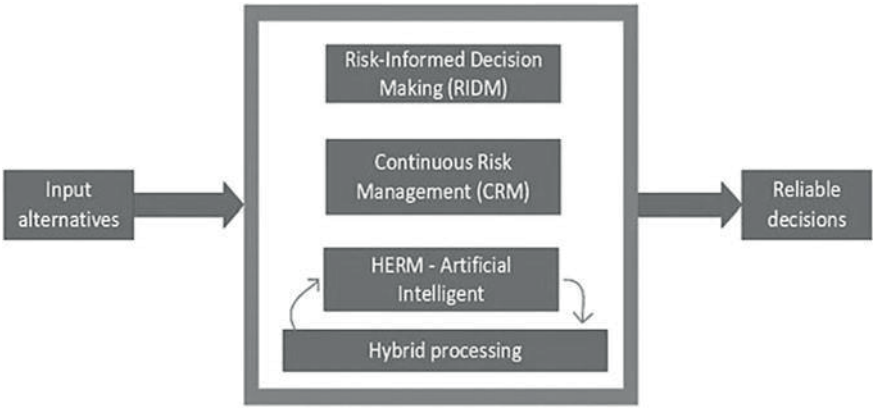


Fig. 2.3 Reliable decision-making process

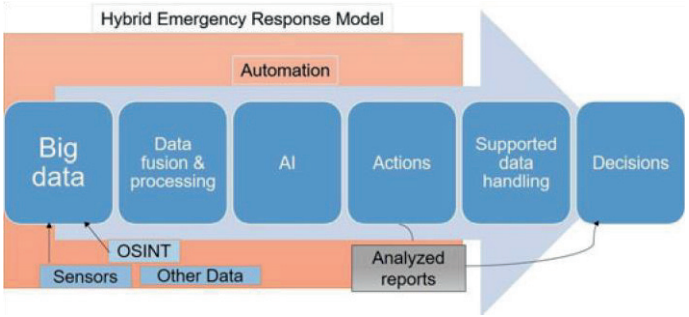


Fig. 2.4 HERM with artificial intelligence

At present, politicians' desire to maintain high levels of control over their decision-making ability may prevent the utilization and usefulness of the proposed smart hybrid emergency model. Many decision-makers want political aspects and opinions to be more represented than rational decisions. Yet Finland's politicians and other high-level decision-makers should take into consideration that cyber preparedness, operational preparedness, and reliability of decision-making are not separate parts of continuity management.

It is possible to combine operational, management, and strategic level decision support functions into a single entity. This does not mean combining all elements in one physical location. If fundamental risk factors—such as a pandemic that presents domino effects from many angles—are not recognized, then technical early warning solutions become useless. It is thus a fundamental societal requirement that a decision support mechanism be developed in jointly with the crisis management system.

It is not enough for the government of Finland to use just one international source (WHO), when they try to maintain the international level of situational awareness. Legislation around privacy issues does not cause permanent obstacles to using sensing elements (e.g., sensors) in the hybrid emergency response model. It is necessary to rationalize organizational responsibilities, for the development of overall security. A human is an individual with limited observation capability and overlapping data transmission limits the effective cooperation between politicians and authorities.

HERM's nearly tireless data handling and transmission capacity can help prevent communication problems among the authorities. Embedding preventive functions against unexpected threats in the emergency response model is an essential part of overall security, in situation awareness management and critical infrastructure protection. In particular, the analysis of global research data regarding COVID-19 can be automated. We need more detailed, standardized information systems and rules for all information systems that handle sensitive information. All that is needed is the political will to exploit intelligence solutions.

The ongoing and tremendously challenging COVID-19 crisis requires us to powerfully leverage our common will—to change the dream of digitalization into concrete actions. The proposed model for smart cities offers solutions to many problems and

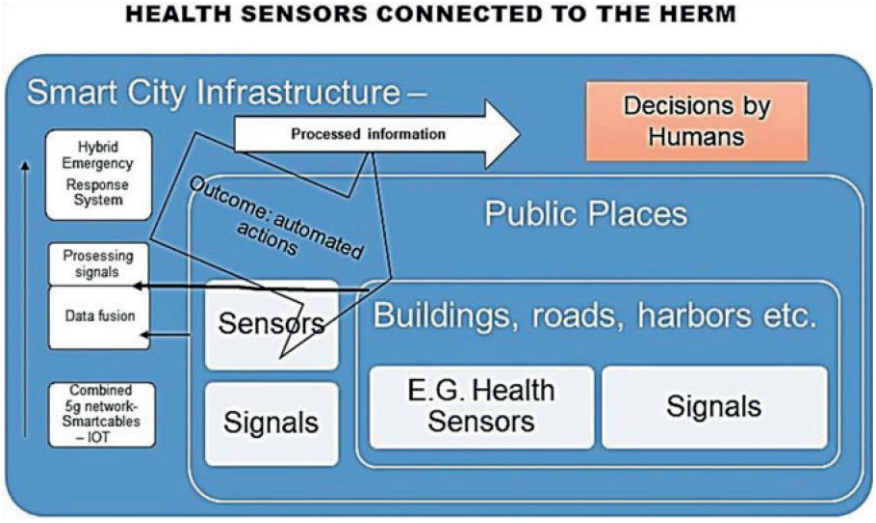


Fig. 2.5 Predictive health sensors in a smart city

questions, as Fig. 2.5 shows. The model may use health sensors, as well as traffic sensors, in a predictive way.

References

1. ATP (2012) Open-source intelligence. Army Techniques Publication No. 2–22.9, Department of the Army, Washington, DC
2. Bröring A, Echterhoff J, Jirka S, Simonis I, Everding T, Stasch C, Liang S, Lemmens R (2011) New generation sensor web enablement. Sensors 11(3):2652–2699
3. Buranyi S (2020) The WHO v coronavirus: Why it can´t handle the pandemic. The Guardian, https://www.theguardian.com/news/2020/apr/10/world-health-organization-who-vcoronavirus-why-it-cant-handle-pandemic. Accessed 10 Dec 2020
4. CSPC (2014) Securing the U.S. electrical grid. Center for the Study of the Presidency &Congress
5. Chong C, Kumar S (2003) Sensor networks: Evolution, opportunities, and challenges. ProcIEEE 91(8):1247–1256
6. Colson E (2019) What AI-driven decision making looks like. Harvard Business Review, https:// hbr.org/2019/07/what-ai-driven-decision-making-looks-like. Accessed 10 Dec 2020
7. DHS (2013) NIPP 2013: Partnering for critical infrastructure security and resilience. U.S.DepartmentofHomelandSecurity,https://www.cisa.gov/publication/nipp-2013-partnering-criticalinfrastructure-security-and-resilience
8. DigiFinland (2020) Welcome to take care of your health and well-being in Omaolo. DigiFinland Oy, https://www.omaolo.fi/. Accessed 10 Dec 2020
9. EC (2018) Artificial intelligence for Europe. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2018) 237, European Commission
10. EC (2020) Coronavirus: commission delivers first batch of 1.5 million masks from 10 million purchased to support EU healthcare workers. Press release, European Commission
11. ElecTech (2016) Internet of Things (IOT) and its applications. Electrical Technology, http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-inelectrical-power-industry.html. Accessed 8 Nov 2016
12. Endsley MR (1988) Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 32(2):97–101
13. Finlex (2011) Emergency powers act 1552/2011. Finnish Ministry of Justice
14. Franke U, Brynielsson J (2014) Cyber situational awareness: A systematic review of the literature. Comput Secur 46:18–31
15. GPMB (2019) A world at risk: Annual report on global preparedness for health emergencies.Global Preparedness Monitoring Board
16. Gervasi O (2010) Encryption scheme for secured communication of web-based control systems.Journal of Security Engineering 7(6):609–618
17. Glassman M, Kang MJ (2012) Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Comput Hum Behav 28(2):673–682
18. Harjumaa M (2020) HUSin Järvinen purkaisi koronarajoituksia: ”Pitäisi yrittää saada sitäväestönosaa sairastamaan, jolle tauti ei todennäköisimmin ole vaarallinen”. Yle, https://yle.fi/ uutiset/3-11318716. Accessed 10 Dec 2020

19. Hautanen S (2020) IS: Yksi mies vastaa 260 sote-yrityksen tietoturvan valvonnasta. Verkkouutiset,https://www.verkkouutiset.fi/is-yksi-mies-vastaa-260-sote-yrityksen-tietoturvan-valvonnasta/#2fb860b4. Accessed 10 Dec 2020
20. Hemmilä I, Salminen V (2020) Oikeuskansleri moittii ministeriöiden yhteistyötä keväänsuojavarustehankinnoissa—STM:ssä epäselvyyttä myös ministerien työnjaosta. Suomenmaa,https://www.suomenmaa.fi/uutiset/oikeuskansleri-moittii-ministerioiden-yhteistyota-kevaansuojavarustehankinnoissa-stmssa-epaselvyytta-myos-ministerien-tyonjaosta-2/. Accessed 4 Dec 2020
21. Henley J (2020) Sweden's Covid-19 strategist under fire over herd immunity emails.TheGuardian,https://www.theguardian.com/world/2020/aug/17/swedens-covid-19-strategist-under-fireover-herd-immunity-emails. Accessed 10 Dec 2020
22. Hevner A, Chatterjee S (2010) Design research in information systems: theory and practice.Springer
23. HkiTimes (2020) Finland to close borders to non-essential travel at 12 am on Thursday.HelsinkiTimes, https://www.helsinkitimes.fi/finland/finland-news/domestic/17450-finlandto-closeborders-to-non-essential-travel-at-12am-on-thursday.html. Accessed 10 Dec 2020
24. ISO (2012) ISO/IEC 27032:2012: Information technology, security techniques, guidelines for cybersecurity. International Organization for Standardization (ISO), https://www.iso.org/standard/44375.html
25. ISO (2015) ISO 9001:2015: Quality management systems, requirements. International Organization for Standardization (ISO), https://www.iso.org/standard/62085.html
26. ISO (2016) ISO 27799:2016 Health informatics, information security management in health using ISO/IEC 27002. International Organization for Standardization (ISO), https://www.iso.org/standard/62777.html
27. ISO (2017) ISO/IEC 27001: Information security management systems. International Organization for Standardization (ISO), https://www.iso.org/isoiec-27001-information-security. html
28. Jaskari K (2020) Ministeriö ei aio jatkossakaan suositella kangasmaskien käyttöä julkisillapaikoilla. Yle, https://yle.fi/uutiset/3-11305744. Accessed 10 Dec 2020
29. Johnson C, Badger L, Waltermire D, Snyder J, Skorupka C (2016) Guide to cyber threat information sharing. NIST Special Publication 800–150, National Institute of Standards and Technology (NIST)
30. Kela (2020) Tekniset liittymismallit Kanta-palveluihin. Ohje, Kanta-palvelut, Kela, https://www.kanta.fi/documents/20143/106828/Tekniset+liittymismallit+Kanta-palveluihin.pdf/a057c34a-f822-71fd-b2df-097245d582ee
31. Lakka P (2020) IS selvitti Pekosen ja Kiurun ministeriön kaaosta—ainakin nämä 5 syytävaikuttivat taustalla: "Suksi lipsunut koko matkan". Ilta-Sanomat, https://www.is.fi/politiikka/ art2000006482234.html. Accessed 10 Dec 2020
32. 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, Valtioneuvoston kanslia
33. Lyngaas S (2020) Why the extortion of Vastaamo matters far beyond Finland—and how cyber pros are responding. CyberScoop, https://www.cyberscoop.com/finland-vastaamo-hackresponse/. Accessed 10 Dec 2020
34. Mediuutiset (2020) Lääkäri: Aletaan tartuttaa koronaa hallitusti hoitohenkilökuntaan immuniteetin saamiseksi. Mediuutiset, https://www.mediuutiset.fi/debatti/laakari-aletaan-tartuttaakoronaa-hallitusti-hoitohenkilokuntaan-immuniteetin-saamiseksi/dfbc96a4-c757-44e9-988 d38cf093a7e8b. Accessed 5 May 2020

35. Mäntymaa E, Mäntymaa J (2020) Sairaalat saivat varmuusvarastoista vuosia sitten vanhentuneita hengityssuojaimia—”Ihan kuranttia ei kaikki tavara ole ollut”, sanoo HUS-johtaja. Yle, https://yle.fi/uutiset/3-11286164. Accessed 10 Dec 2020
36. NASA (2010) Risk-informed decision making handbook (NASA/SP-2010-576). Technical report,NASA. https://ntrs.nasa.gov/api/citations/20100021361/downloads/20100021361.pdf. Accessed 10 Dec 2021
37. NIST (2010) Guidelines for smart grid cybersecurity. In: Privacy and the smart grid, vol 2. NISTIR 7628, National Institute of Standards and Technology (NIST)
38. NIST (2018) Framework for improving critical infrastructure cybersecurity. Version 1.1,National Institute of Standards and Technology (NIST)
39. Natri S (2020) THL:n pääjohtaja kehottaa suomalaisia pukemaan kangasmaskin julkisillapaikoilla—”Näin oireeton tartuttaja suojelee muita”. Yle, https://yle.fi/uutiset/3-11305102. Accessed 10 Dec 2020
40. NewsNowFin (2020) Maria Ohisalo: Vastaamo cyber attack and blackmail demands “serious, outrageous and cowardly”. News Now Finland, https://newsnowfinland.fi/crime/mariaohisalo-vastaamo-cyber-attack-and-blackmaildemands-serious-outrageous-and-cowardly. Accessed 10 Dec 2020
41. NewsNowFin (2020) Vastaamo hacking and blackmail: 25,000 police reports filed. News NowFinland, https://newsnowfinland.fi/crime/vastaamo-hacking-and-blackmail-25000-police-reports-filed. Accessed 10 Nov 2020
42. Nunamaker J Jr, Chen M, Purdin T (1990) Systems development in information systems research. J Manag Inf Syst 7(3):89–106
43. Nurmi P (2015) OSINT: Avointen lähteiden internet-tiedustelu. Kehitysprojektin raportti,Aaltoyliopisto
44. Ollila A (2020) Lääkintöneuvos Pälve tyrmää Kirsi Varhilan näkemykset maskien käytönesteistä. Uusi Suomi, https://puheenvuoro.uusisuomi.fi/aveollila1-2/laakintoneuvos-palve-tyr maakirsi-varhilan-nakemykset-maskien-kayton-esteista/. Accessed 10 Dec 2020
45. PM (2010) Yhteiskunnan turvallisuusstrategia: Valtioneuvoston periaatepäätös 16.12.2010. Puolustusministeriö, Helsinki
46. PPD (2013) Critical infrastructure security and resilience. Presidential Policy Directive PPD21, U.S. White House Office
47. dos Passos DS (2016) Big Data, data science and their contributions to the development of the use of open source intelligence. Electronic Journal of Management & System 11(4):392–396
48. Ranta E (2020) Tällainen yritys on tietomurron kohteeksi joutunut Vastaamo. Ilta-Sanomat, https://www.is.fi/taloussanomat/art-2000006699437.html. Accessed 30 Nov 2020
49. Robles RJ, Kim T (2010) Communication security for SCADA in smart grid environment.In: DNCOCO’10: proceedings of the 9th WSEAS international conference on data networks, communications, computers,pp36–40.WorldScientificandEngineeringAcademyandSociety (WSEAS), Stevens Point, WI
50. SecComm (2017) Security Strategy for Society. Government resolution, Security Committee, Helsinki
51. Simola J (2020) Privacy issues and critical infrastructure protection. In: Benson V, Mcalaney J (eds) Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, pp 197–226
52. Simola J, Rajamäki J (2017) Hybrid emergency response model: improving cyber situational awareness. In: Scanlon M, Le-Khac N (eds) ECCWS 2017—proceedings of the 16th European conference on cyber warfare and security. Academic Conferences and Publishing International, pp 442–451
53. Simola J, Rajamäki J (2018) Improving cyber situational awareness in maritime surveillance.In: Josang A (ed) ECCWS 2018—proceedings of the 17th European conference

on cyber warfare and security, pp 480–488. Academic Conferences and Publishing International
54. Solita (2020) The Finnish Covid-19 app Koronavilkku has been downloaded a million times already! Solita, https://www.solita.fi/en/the-finnish-covid-19app-koronavilkku-has-been-downloaded-million-times/. Accessed 10 Dec 2020
55. Trottier D (2015) Open source intelligence, social media and law enforcement: Visions, constraints and critiques. Eur J Cult Stud 18(4–5):530–547
56. Uosukainen R, de Fresnes T (2020) Poliitikot tulevat ja menevät, virkamiehet pysyvät—käynnissä on kamppailu siitä kenellä valta on. Yle, https://yle.fi/uutiset/3-11186910. Accessed 10 Dec 2020
57. Valvira (2020) Organizational structure. Valvira, https://www.valvira.fi/web/en/valvira/organisational_structure. Accessed 20 Oct 2020
58. Wooldridge M (2009) An introduction to multiagent systems, 2nd ed. Wiley
59. Yin RK (2017) Case study research and applications: design and methods, 6th ed. SAGE, Thousand Oaks, CA
60. Yle (2020) Daily: Gov't not planning to extend Uusimaa border closure. Yle, https://yle.fi/uutiset/osasto/news/daily_govt_not_planning_to_extend_uusimaa_border_closure/11303010. Accessed 10 Dec 2020
61. Yle (2020) Finland: Chinese face masks fail tests. Yle, https://yle.fi/uutiset/osasto/news/finland_chinese_face_masks_fail_tests/11298914. Accessed 10 Dec 2020
62. Yle (2020) Finland's first coronavirus case confirmed in Lapland. Yle, https://yle.fi/uutiset/osasto/news/finlands_first_coronavirus_case_confirmed_in_lapland/11182855. Accessed 10 Dec 2020
63. Yle (2020) Friday's paper: problem with corona alert app, more countries on restricted list, .drugs in the countryside, Yle. https://yle.fi/uutiset/osasto/news/fridays_papers_problem_with_corona_alert_app_more_countries_on_restricted_list_drugs_in_the_countryside/11586606. Accessed 10 Dec 2020
64. Yle (2020) President Niinistö defends role in coronavirus crisis. Yle, https://yle.fi/uutiset/osasto/news/president_niinisto_defends_role_in_coronavirus_crisis/11303872. Accessed 12 Dec 2020
65. Yle (2020) Two possible coronavirus cases in northern Finland. Yle, https://yle.fi/uutiset/osasto/news/two_possible_coronavirus_cases_in_northern_finland/11173752. Accessed 10 Dec 2020
66. Zio E, Pedroni N (2012) Risk-informed decision-making processes: an overview. Foundation for an Industrial Safety Culture, Touloise, https://www.foncsi.org/fr/publications/cahierssecurite-industrielle/overview-of-risk informed-decision-making-processes/CSI-RIDM.pdf. Accessed 15 Dec 2020