Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
Acronym	ECHO
Number	830943
Type of instrument	Research and Innovation Action
Topic	SU-ICT-03-2018
Starting date	01/02/2019
Duration	48
Website	www.echonetwork.eu

D3.6 ECHO INFORMATION SHARING MODELS

Work package	WP3 EU NETWORK GOVERNANCE MODELS
Lead author	JYRI RAJAMÄKI (LAU)
Contributors	Daniele Cristofori (Z&P), Ilkka Tikanmäki (LAU), Jari Räsänen (LAU), Jussi Simola (LAU), Merlin Bieze (RHEA), Vasilis Katos (BU)
Peer reviewers	Kristine Hovhannisyan (TUT), Consuelo Colabuono (RHEA), Matteo Merialdo (RHEA), Konstantinos Kyriakopoulos (CERTH), Mirjam Kert (GT), Burak Mavzer (VST)
Version	V1.0
Due date	31/10/2019
Submission date	31/10/2019

Dissemination level

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

The work described in this document has been conducted within the ECHO project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830943

Version history

Revision	Date	Editor	Comments
0.1	10/07/2019	Jyri Rajamäki (LAU), Daniele Cristofori (Z&P)	First draft
0.2	31/07/2019	Jussi Simola (LAU), Merlin Bieze (RHEA)	Added acronyms, case Taxonomies for cyber information sharing and case HAVARO,
0.3	01/08/2019	Jussi Simola (LAU)	Added systematic review
0.4	15/8/2019	Jussi Simola (LAU), Jari Räsänen (LAU)	Refinements in introduction, added comparison of cyber information sharing models in US and EU, added regulations for CISE-case and privacy issues
0.5	03/09/2019	Jussi Simola (LAU), Daniele Cristofori (Z&P), Vasilis Katos (BU)	Added case Health information sharing and cross-case conclusions, editorial chances
0.6	27/09/2019	Jyri Rajamäki (LAU)	Refinements in all Sections
0.7	07/10/2019	Jyri Rajamäki (LAU)	Refinements in all Sections
0.8	23/10/2019	Jyri Rajamäki (LAU), Jussi Simola (LAU), Daniele Cristofori (Z&P)	Added Annexes 3-5, refinements in all Sections
0.9	28/10/2019	Jyri Rajamäki (LAU), Jussi Simola (LAU), Daniele Cristofori (Z&P)	Implementing QA comments
1.0	31/10/2019	Jyri Rajamäki (LAU), Vasilis Katos (BU)	Implementing QA comments in Section 5, typo review

List of contributors

The contributors to this deliverable are presented in the following table:

Section	Author(s)
1	Jyri Rajamäki (LAU)
2	Jyri Rajamäki (LAU)
3	Jyri Rajamäki (LAU), Jussi Simola (LAU), Daniele Cristofori (Z&P)
4.1	Merlin Bieze (RHEA)
4.2	Daniele Cristofori (Z&P)
4.3	Jyri Rajamäki (LAU), Ilkka Tikanmäki (LAU), Jari Räsänen (LAU)
4.4	Jyri Rajamäki (LAU)
4.5 – 4.7	Jussi Simola (LAU)
4.8	Mirjam Kert (GT)
5	Vasilis Katos (BU)
6	Jyri Rajamäki (LAU)
Annexes	Jussi Simola (LAU), Jyri Rajamäki (LAU)

Keywords

Early Warning System, ECHO, information sharing, information sharing models, trust models, cybersecurity, case study,

Disclaimer

Executive summary

As part of the ECHO project, the Early Warning System (EWS) is one of four technologies under development. The E-EWS will provide the capability to share information to provide up to date information to all constituents involved in the E-EWS. The development of the E-EWS will be rooted in a comprehensive review of information sharing and trust models from within the cyber domain as well as models from other domains.

This deliverable is the result of a qualitative multiple-case study analysis made in Task 3.2. It consists of theory development by systematic reviews of academic articles, seven case studies, and cross-case conclusions, from which a set of system requirements and features were established to support a model that promotes information sharing among partners, while also meeting regulatory requirements. Moreover, the final analysis includes the requirements for information sharing within and between partners across organisational boundaries as derived from multi-sector analysis. Three of the case studies were presented as research papers at DIGILIENCE conference in October 2019.

This deliverable consists of a comprehensive review of information sharing and trust models from within the cyber domain (n > 50, see Annex 2), as well as models from other domains, such as healthcare, maritime and critical infrastructure protection. This document can be used as input for the ECHO EWS Information sharing model definition that will be required for Task 5.1, Task 5.2 and Task 5.3.

Table of contents

List of figures

List of tables

1. Introduction

1.1 Purpose and scope of the document

As part of the ECHO project, the Early Warning System (EWS) is one of four technology roadmap under development. The E-EWS will provide the capability to share information to provide up to date information to all constituents involved in the E-EWS. E-EWS aims at serving as a security operations support tool enabling the members of the ECHO network (and other new entities at EU level) to coordinate and share information in near real-time. With the E-EWS ECHO stakeholders can retain their fully independent management of cyber-sensitive information and related data management. E-EWS will work as a parallel part of other mechanisms in smart society. The development of the E-EWS will be rooted in a comprehensive review of information sharing and trust models from within the cyber domain.

This deliverable D3.6 consists of a comprehensive review of information sharing and trust models from within the cyber domain, as well as models from other domains, such as, healthcare information sharing) From these models a set of system requirements and features is established to support a model that promotes information sharing among partners, while also meeting regulatory requirements. Deliverable 3.6 defines crucial elements of ECHO Early Warning System, further studied and developed within WP5.

The content of deliverable D3.6 is based on results of analysis of eight case studies carried out in Task 3.2 and cross-case conclusions of them. Moreover, the final analysis includes the requirements for information sharing within and between partners across organisational boundaries as derived from multi-sector analysis.

During the processing of D3.6, three case studies (cf. Annex 3–5) were presented in DIGILINCE 2019 Conference, Sofia, 2–4 October, 2019, and published in a peer-reviewed, open source journal [1].

1.2 Structure of the document

The reporting of D3.6 (see Figure 1) follows the linear-analytic structure of the sequence of subtopics involving the issue being studied, the methods used, a review of the relevant literature, the findings from the collected and analysed data, and the conclusions and implications from the findings. After the introduction, Chapter 2 proposes a used methodology of the deliverable. Chapter 3 handles the theory and how it is built. Chapter 4 present results of the individual case study analysis. Chapter 5 includes cross-case study conclusions and gives system requirements and recommendations. Chapter 6 concludes the deliverable. Annex 1 catalogues literature review sources, Annex 2 lists analysed information sharing and trust models, and Annex 3–5 contain reproduced articles made during Task 3.2.

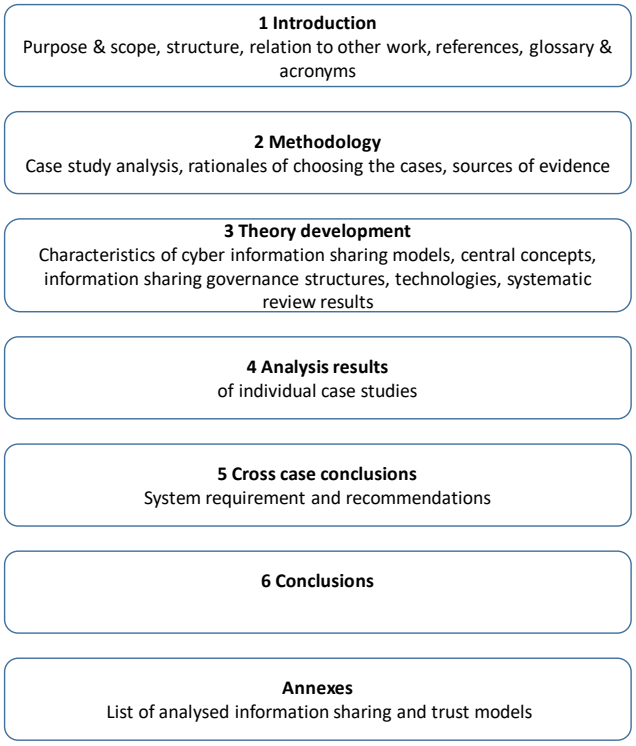

Figure 1: The outline of D3.6

1.3 Relation to other work in the project

The document is made as part of WP 3 and is essentially related to WP 5 work. The results of the analysis in D3.6 are made for use in the development of the E-EWS (WP5).

1.4 Applicable and reference documents

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement 830943 – ECHO	-	1.0	02/04/2019
[PH]	D1.1 Project Handbook	ECHO_D1.1_v1.0	1.41	02/05/2019

Table 1: Applicable documents

The following documents have been consulted for the generation of this document:

Reference	Document Title
[1]	T. Tagarev (ed.), "Digital Transformation, Cyber Security and Resilience," *Information Security,* vol. 43, pp. 1-398, 2019.
[2]	R. K. Yin, *Case study research and applications: Design and methods*, Sixth edition ed., Los Angeles: SAGA Publications, Inc., 2017.
[3]	K. Popper, Conjectures and Refutations: The Growth of Scientific Knowledge, London: Routledge Classics, 2009.
[4]	E. Seshia and A. Sanjit, *Introduction to Embedded Systems, A Cyber-Physical Systems Approach*, 2 ed., MIT press, 2017, p. 2017.
[5]	J. Simola and J. Rajamäki, "Hybrid Emergency Response Model: Improving Cyber Situational Awareness," in *Proceedings of the 16th European Conference on Cyber Warfare and Security*

Reference	Document Title
	(ECCWS), M. S. &. N. Le-Khac, Ed., Reading, Academic Conferences and Publishing International Limited, 2017, pp. 442-451.
[6]	ENISA, "Information sharing and common taxonomies between CSIRTs and Law Enforcement," 2015.
[7]	The Department of Homeland Security (DHS), "Blueprint for a Secure Cyber Future - The Cybersecurity Strategy for the Homeland Security Enterprise," DHS, 2011.
[8]	OECD Legal Instruments, "Recommendation of the Council on the Protection of Critical Information Infrastructures," 30 04 2008. [Online]. Available: https://legalinstruments.oecd.org/en/instruments/121. [Accessed 22 10 2019].
[9]	National Institute of Standards and Technology (NIST), "Guidelines for smart grid cybersecurity In Smart grid cybersecurity strategy, architecture," U.S. Department of Commerce, USA, 2014.
[10]	European Union Agency For Network And Information Security (ENISA), "Programming Document 2019-2021," ENISA, Heraklion, Greece, 2019.
[11]	L. Ladid, J. Armin and H. Kivekäs, "The Finish electronic communications regulator TRAFICOM - A cybersecurity reference model for Europe.," SAINT Consortium/ Traficom., Helsinki, 2019.
[12]	ECSO European Cyber Security Organisation, "About ECSO," 2019. [Online]. Available: https://ecs-org.eu/. [Accessed 2 9 2019].
[13]	ENISA & ITE, "Information Sharing and Analysis Centres (ISACs) Cooperative models," European Union Agency for Network and Information Security, Greece, 2017.
[14]	G. White and R. Lipsey, "ISAO SO Product Outline," ISAO Standards Organization, 2016.
[15]	Electrical Technology, "Internet of Things (IOT) and Its Applications in Electrical Power Industry," 2016. [Online]. Available: http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html. [Accessed 10 8 2019].
[16]	National Institute of Standards and Technology (NIST), "Guide for Conducting Risk Assessments. 800-30," U.S. Department of Commerce, Gaithersburg, 2013.
[17]	National Institute of Standards and Technology (NIST), "Special Publication 800-37 R.2, Risk Management Framework for Information Systems and Organizations," U.S. Department of Commerce, Gaithersburg, 2018.
[18]	The International Organization for Standardization (ISO), "International Standard ISO/IEC 27010:2015. Standard edn.," Switzerland, 2015.
[19]	National Institute of Standards and Technology (NIST), "Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150," U.S. Department of Commerce, Gaithersburg, 2016.
[20]	S. Munk, "Interoperability Services Supporting Information Exchange Between Cybersecurity Organisations1," *AARMS,* vol. 17, no. 3, pp. 131-148, 2018.
[21]	E. M. Sedenberg and J. X. Dempsey, "Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs," 31 May 2018. [Online]. Available: https://arxiv.org/abs/1805.12266. [Accessed 30 March 2019].
[22]	wikia.org, "Technical threat indicator," [Online]. Available: https://itlaw.wikia.org/wiki/Technical_threat_indicator.
[23]	C. Goodwin and J. Nicholas, "A framework for cybersecurity information sharing and risk reduction," [Online]. Available: https://www.slideshare.net/RoyRamkrishna/framework-for-cybersecurityinfosharing-1.
[24]	MITRE Corporation, "Trusted Automated eXchange of Indicator Information — TAXII™ Enabling Cyber Threat Information Exchange," [Online]. Available:. https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf
[25]	MITRE Corporation, "Cyber Information-Sharing Models: An Overview," 2012. [Online]. Available: https://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf
[26]	RSAC contributor, "RSA conference - Threats Are Omnipresent But You Have Options," 11 june 2019. [Online]. Available: https://www.rsaconference.com/industry-topics/blog/threats-are-omnipresent-but-you-have-options.
[27]	P. McGlone, "Threats Are Omnipresent But You Have Options," 11 June 2019. [Online]. Available: https://securityboulevard.com/2019/06/threats-are-omnipresent-but-you-have-options/.
[28]	L. J. Janczewski and W. Caelli, *Cyber Conflicts and Small States*. New York: Routledge, 2016.

Reference	Document Title
[29]	F. Skopik, *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level,* Boca Raton: CRC Press, 2017.
[30]	Johnson, et al., *Guide to cyber threat information sharing*, NIST special publication, NIST, 2016.
[31]	M. He, L. Devine and J. Zhuang, "Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach: Cybersecurity Information Sharing," *Risk Analysis,* 2017.
[32]	Department of Homeland Security, , "NIPP 2013 - partnering for critical infrastructure security and resilience.," DHS, 2013.
[33]	The Department of Homeland Security (DHS), “Automated indicator sharing AIS,” DHS, Washington, U.S, 2019.
[34]	OASIS Cyber Threat Intelligence;DHS, “"TAXII™ version 2.0. committee specification 01," OASIS Open, Tech. Rep. taxii-v2.0-cs01,” OASIS, 2017.
[35]	Cyber Threat Intelligence Technical Committee, “Introduction to TAXII,” 2019. [Online]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro. [Accessed 22 10 2019].
[36]	T. Kokkonen, J. Hautamäki, J. Siltanen and T. Hämäläinen, "Model for Sharing the Information of Cyber Security Situation Awareness between Organizations," *23rd International Conference on Telecommunications,* 2016.
[37]	T. Kokkonen, *Anomaly-Based Online Intrusion Detection System as a Sensor for Cyber Security Situational Awareness System*, Jyväskylä: University of Jyväskylä, 2016.
[38]	The Criminal Intelligence Coordinating Council, "National criminal intelligence sharing plan. Building a national capability for effective criminal intelligence development and the nationwide sharing of intelligence and information," CICC, 2013.
[39]	S. Garfinkel, "Digital forensics XML and the DFXML toolset," *Digital Investigation,* vol. 8, pp. 161-174, 2012.
[40]	A. Rutkowski, et al,, "CYBEX - The Cybersecurity Information Exchange Framework (X. 1500)," *Computer Communication,* vol. 40, pp. 59-64, 2010.
[41]	I. Vakilinia, D. K. Tosh and S. Sengupta, "Privacy-preserving cybersecurity information exchange mechanism," *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS),* pp. 1-7, 2017.
[42]	Sadique, F. et al,, "A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)," *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC),* pp. 493-498, 2019.
[43]	M. Endsley, "Design and evaluation for situation awareness enhancement.," in *Proceedings of the Human Factors Society 32nd Annual Meeting*, 1988.
[44]	M. Endsley and M. Robertson, "Situation awareness in aircraft maintenance teams," *International Journal of Industrial Ergonomic,* vol. 26, pp. 301-325, 2000.
[45]	M. Endsley and M. Robertson, "Training for situation awareness in individuals and teams," in *Situation Awareness Analysis and Measurement*, Mahwah, LEA, 2000.
[46]	C. Bolstad and M. Endsley, "The effect of task load and shared displays on team situation awareness," in *The 14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society*, Santa Monica, CA, 2000.
[47]	L. Ilves, T. . Evans, F. Cilluffo and A. Nadeau, "European Union and NATO Global Cybersecurity Challenges: A Way Forward," *PRISM,* vol. 6, no. 2, 2016.
[48]	B. Shen, *Healthcare and Big Data Management*, Springer, 2017.
[49]	B. E. Dixon, Health Information Exchange, 2016.
[50]	A. Karim, B.-H. Abderrahim, K. Hayat and S. Mostafa, *Big data security and privacy in healthcare: A Review*, Elsevier B.V., 2017.
[51]	A. F. S. Ibrahim, New Secure Solutions For Privacy And Access Control In Health Information Exchange, *Theses and Dissertations--Computer Science*, 47. Available: https://uknowledge.uky.edu/cs_etds/47 2016.
[52]	I. Tikanmäki, "Common Information Sharing on Maritime Domain - A qualitative study on European Maritime Authorities’ cooperation," *International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K),* vol. 3, pp. 283-290, 2017.
[53]	European Commission, "Security in 2020: Meeting the challenge," Publications Office of the European Union 2014, Luxembourg, 2014.

Reference	Document Title
[54]	I. Tikanmäki and H. Ruoslahti, "Increasing Cooperation between the European Maritime Domain Authorities," *International Journal of Environmental Science,* vol. 2, pp. 392-399, 2017.
[55]	EUCISE2020, "Deliverable D10.2".
[56]	K. Janhunen, *Valtionhallinnon häiriötilanteiden hallinta - miten VIRT-toimintaa kehitetään?* The Ministry of Finance, Finland, 2015.
[57]	MITRE Corporation, "Common vulnerabilities and exposures.," 2019. [Online]. Available: . https://cve.mitre.org/cve/cna.html.
[58]	MITRE Corporation, "CVE-details," 2019. [Online]. Available: https://www.cvedetails.com/cve-help.php.
[59]	National Institute of Standards and Technology (NIST), "National Vulnerability Database - General Information," 2019. [Online]. Available: https://nvd.nist.gov/general.
[60]	MITRE Corporation, "Common Vulnerabilities and Exposures - CVE and NVD Relationship," 2019. [Online]. Available: https://cve.mitre.org/about/cve_and_nvd_relationship.html.
[61]	J. Robertson and M. Riley, "The big hack: How china used a tiny chip to infiltrate U.S. companies?," 2018. [Online]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.
[62]	S. Shackelford, M. Sulmeyer, A. Deckard, B. Buchanan and B. Micic, "From russia with love: Understanding the russian cyber threat to U.S. critical infrastructure and what to do about it," *Nebraska Law Review,* vol. 96, no. 2, pp. 321-337, 2017.
[63]	R. Caralli, J. Stevens, R. Young and W. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technical report.," U.S. Software Engineer Institute. Carnegie Mellon University, 2007.
[64]	E. Zio and P. Nicola, "Risk-Informed Decision-Making Process," Foundation for an Industrial Safety Culture, Touloise, France, 2012.
[65]	National Aeronautics and Space Administration (NASA), "Considering Risk and Resilience in Decision-Making," National Aeronautics and Space Administration, Hampton, Virginia, 2015.
[66]	National Aeronautics and Space Administration (NASA), *Risk-Informed Decision making Handbook*, Washington: NASA, 2010.
[67]	ECHO, "DPIA pre-assessment Report, v0.2," 2019.

Table 2: Reference documents

1.5 Glossary of acronyms

Acronym	Description
AIS	Automated Information Sharing
AI	Artificial Intelligence
APTs	Advanced Persistent Threats
CCSA	Common Cyber Situational Awareness
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISA	Cybersecurity Information Sharing Act
CSA	Cyber Situational Awareness
CNA	CVE Numbering Authority
CSC	Cyber Security Center
CSIC	Cyber Situation Center
CSIRT	Computer Security Incident Response Teams
CTI	Cyber Threat Intelligence
CYBEX	Cybersecurity Information Exchange Framework
CVE	Common Vulnerabilities and Exposures
CyPR	Cybersecurity Professional Register
CybOX	Structured Cyber Observable eXpression

Acronym	Description
DNS	Domain Name System
DoS	Denial of Service
DHS	Department of Homeland Security
EC3	European Cybercrime Centre
ECSO	European Cyber Security Organisation
ECTF	Electronic Crimes Taskforce
E-EWS	ECHO Early Warning Systems
E-FCR	ECHO Federated Cyber Ranges
EIS	Europol Information System
E-MSAF	ECHO Multi Sector Assessment Framework
ENISA	European union agency for Network and Information Security
FBI	Federal Bureau of Investigation
FSP	Full-Scale Pilot
GA	Grant Agreement
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
H	Humans
HMI	Human-Machine Interface
HERM	Hybrid Emergency Response Model
INDICATOR	Indicator may be used to detect suspicious or malicious cyber activity and represent a set of malicious domains
IoCs	Indicators of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organisations
IIOT	Industrial Internet of Things
IOT	Internet of Things
MAEC	Malware Attribute Enumeration and Characterisation
MCSR	Multiple Case Study Research
MISP	Malware Information Sharing Platform
MS	Member State
NATO	North Atlantic Treaty Organisation
NCCIC	National Cybersecurity and Communications Integration Center
NCSC	National Cyber Security Centers
NDN	National Detection Network
NEC	Non-EU Country
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NRA	National Regulatory Authority
NSA	National Security Authority
NVD	National Vulnerability Database
ORD	Open Research Data
OSINT	Open Source Intelligence
PAP	Permissible Actions Protocol
PH	Project Handbook
PII	Personally Identifiable Information
RAF	Risk Assessment Framework
RMF	Risk Management Framework
SDO	STIX Domain Objects
SA	Situational Awareness
SEB	Stakeholders Expert Board
SIEM	Security Information and Event Management

Acronym	Description
SIENA	Secure Information Exchange Network Application
SIP	Shared Situational Picture
SME	Small- and Medium-sized Enterprises
STIX	Structured Threat Information Expression
TAXII	Trusted Automated eXchange of Indicator Information
TLP	Traffic Light Protocol
TTP	Tactic, technique, or procedure; behaviours and resources that attackers use to carry out their attacks
VPN	Virtual Private Network
WP	Work Package

Table 3: Glossary of acronyms, initialises and abbreviations

2. Methodology

This chapter presents the research method and research process applied in this deliverable. The applied case study method is introduced, along with abductive reasoning as a research approach. The rationales behind the selection of information sharing and trust models as case study subjects are discussed. The units of analysis and the sources of evidence are described.

Figure 2 shows how multiple case study research (MCSR) is applied in the creation of this deliverable. The initial step in designing MCSR consists of theory development, and the next steps are case selection and definition of specific measures in the design and data collection process. Each individual case study consists of a whole study, and then conclusions of each case are considered to be the replication by other individual cases. The individual cases as well as the multiple result should be the focus of a summary report. For each individual case, the report should indicate how and why a particular result is demonstrated. Across cases, the report should present the extent of replication logic, including certain and contrasting results [2].

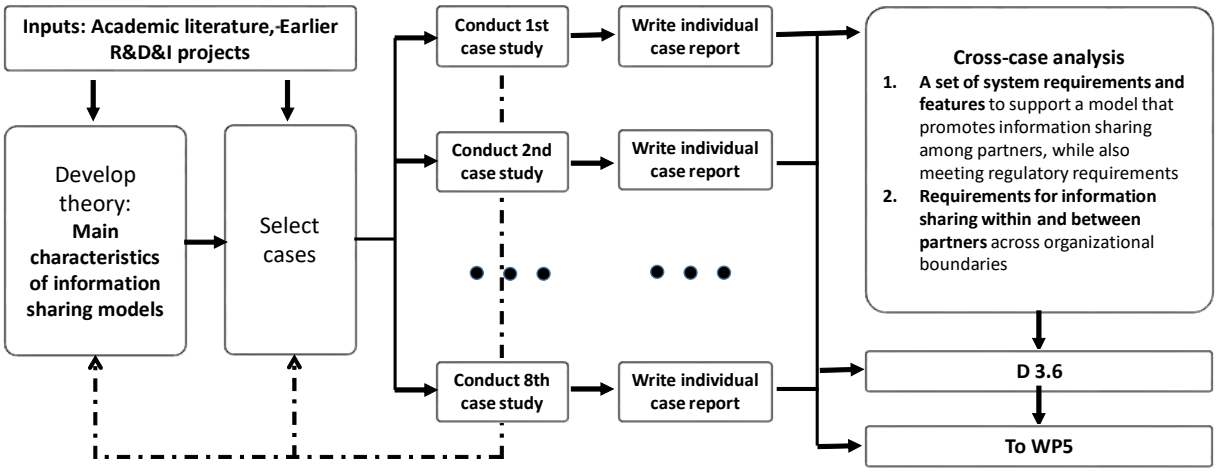

Figure 2: Multiple-case study method of D3.6

2.1 Theory development

The first step in MCSR is the development of a rich theoretical framework that needs to state the conditions under which a particular phenomenon is likely to be found [2].

The theoretical framework of this deliverable forms by way of a systematic review. Collected and analysed materials consist of scientific literatures, research articles and official publications. The research question of the literature review was “What are the main characteristics/features of cyber information sharing and trust models?” In order to capture a reasonably full range of the literature concerning the main features of cyber exchange models, following scientific databases have been used: Database of the JYKDOK library at the University of Jyväskylä (wide database concerning cybersecurity and it provides access e.g. to the IEEE Xplore). The IEEE Xplore library (provides web access to more than 4.5 million documents from publications in computer science and ca. 200 journals and ca. 1700 conference proceedings), Springer link (Database area of engineering contains 17000 books) and AI -tool called IRIS which search engine based on 100 entered keywords. Also, several studies were based on public sources. Analysed information sharing and trust models are listed in Annex 1.

The qualitative analysis was made by using traditional half-manual processing and Glue (Orange3) Python to explore collected database. As a result, the main characteristics of cyber information sharing models were defined. These characteristics were used as embedded units of analysis in the individual case studies.

2.2 Case selection and individual case studies

According to Yin [2], any use of multiple case design should follow a replication, not a sampling logic, and choosing of each case should be made carefully.

In Figure 2, the dashed-line feedback represents a discovery situation, where one of the cases does not suit the original multiple-case study design. This kind of a discovery stands for a need to reconsider the original theoretical foundations. This means redesign should take place before proceeding further, and in this view the replication approach represents a way of generalising that uses a type of test called falsification or refutation, which is the possibility that a theory or hypothesis may be proven wrong or falsified [3].

This multiple case study is made up of following individual case studies:

- Analysis results from the ECHO partners' research, development and innovation work in earlier projects, from which taxonomies for cyber information sharing are defined (Section 4.1).
- Analysis of sensitive information sharing models from other domains; health information sharing (Section 4.2), and maritime information sharing (Section 4.3).
- Analysis of inter-sector cyber information sharing models; critical Infrastructure protection (Section 4.4), and smart cities (Section 4.7).
- Analysis of national cyber security cooperation networks and info sharing models; HAVARO cyber threat prevention mechanism in Finland (Section 4.5).
- Analysis of information sharing and trust models within the cyber domain; comparison of cyber information sharing models in the US and EU (Section 4.6).
- Synergies of information sharing needs with EWS and FCR (Section 4.8).

The sources of evidence used in the individual case studies consist of documentation, archival records, interview, direct observations, participant-observation, and physical artefacts. From these, two to four multiple sources of evidence were used in every individual case study.

Every individual case study is reported separately as a conference paper (cf. ANNEX 3-5) and/or via ECHO SharePoint (cf. [PH] for more information about ECHO SharePoint).

2.3 Cross-case conclusions

Cross-case conclusion were made via a document analysis exercise of the preceding sections and a selection of literature sources. The final analysis includes the requirements for information sharing within and between partners across organisational boundaries as derived from multi-sector analysis.

3. Theory development

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 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 [4].

There are separate local situation centres for emerging situations, emergency response systems, separate cyber threat functions in national and EU level. All works mainly without synergy [5]. Separate functionalities situation centres produce more potential vulnerabilities for vital functions. Therefore, it is important to develop functionalities in ecosystem and gather relevant data for the next generations’ early warning solutions.

How to create connection between old-fashioned procedures and new preventive or (predictive) cyber functions concerning preventive cyber-threat procedures? How to combine and share relevant data between stakeholders? What kind of information sharing solutions already exist? How to improve response and procedures in case of a hybrid incident? The problem concerns whole ecosystem. The theory development has been carried out via a systematic literature review of scientific articles about cyber information sharing, and it is going to find out the answers for these questions.

The structure of the chapter: Firstly, the central concepts and organisations with regard to this deliverable are defined. Secondly, main characteristics of information sharing models are presented. Thirdly, we discuss cybersecurity information sharing governance structures. Fourthly, some sharing technologies for cybersecurity information are presented. Fifth section deals with the theory about situational awareness, and finally some remarks are discussed that came up during literature review.

3.1 Central concepts and organisations

Alert and detection system

Alert and detection system produces information, which may alert other players to 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 within the company, in its own devices. The information on situation awareness provided by the system increases understanding about the organisation’s own and general state of information security.

CSIRT (Computer Security Incident Response Team) or CERT (Computer Emergency Response Team)

An organisation 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 organisations, academic institutions or other private body with incident response capabilities [6]. 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 infrastructure (CI) 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. 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 [7]. That smart network will integrate information and communication technologies with the power-delivery infrastructure.

Critical Information Infrastructure Protection (CIIP)

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” [8].

Cyber Threats in Critical Infrastructure

Cyber threats include denial of service (DoS), unauthorised vulnerability probes, botnet command and control, data exfiltration, on-purpose data corruption 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 a long period of time. Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications [9].

National Institute of Standards and Technology (NIST) classifies cyber-physical attacks into three broad sections [9]. Table 4 presents these classifications.

Type of attacks	Influence	Example of threat progress
Cyber informed physical attacks	Allows an enemy or attackers to plan and execute an improved or enhanced physical attack.	Attackers who would like to destroy components within a substation though and they are not sure which substation or components would have the greatest impact. They could try to access confidential/sensitive information or aggregate unprotected information by cyber and they could then physically attack that specific substation and lines.
Cyber-attacks enhancing physical attacks	An enemy uses cyber means to improve the impacts of a physical attack by either making the attack more harmful with greater consequences or interfering with restoration efforts by increasing the duration of the attack.	An enemy tampering with the integrity of protective relay settings prior to a physical attack on power lines. The tampered settings allow the failure to progress into impacts on a wider segment of the grid although the original settings were designed to contain the effects of a failure.
Use of a cyber-system to cause physical harm	An enemy uses a cyber-system that controls physical equipment or units in such a manner to cause physical harm/damage.	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 adversary could turn on the ignition source, potentially causing an explosion (the burner management system for a natural gas generator).

Table 4: Classification of cyber-physical attacks

Carefully done cyber, physical and operational security planning and implementations can minimise these impacts of cyber-physical attacks. Defensive measures that can be used to minimise the likelihood of successful cyber-attacks and physical attacks will also work to minimise the impacts of a cyber-physical attack [9].

The European Union Agency for Network and Information Security (ENISA)

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security (NIS) expertise for the EU, its member states, the private sector and Europe's citizens. ENISA develop with these groups' advice and recommendations on good practice in information security. It supports and assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA provides recommendations on cybersecurity, supports policy development and its implementation, and collaborates with other operational teams throughout Europe [10].

National Regulatory Authority (NRA)

National Regulatory Authorities can play different roles in relation to cybersecurity. In Finland, the tasks are; steering and supervision of telecoms operators' operations, information security and preparedness, for example, monitoring compliance with the information security regulation, steering and supervision of strong electronic identification and the provision of qualified certificates, for example, monitoring compliance and carrying out annual audits of certification authorities providing qualified certificates [11].

The European Cyber Security Organisation (ECSO)

The European Cyber Security Organisation (ECSO) represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership. 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 and the European Free Trade Association and H2020 associated countries [12].

Information Sharing and Analysis Centres (ISACs)

ISAC is collaboration community created for sector-specific national or international information sharing. Information Sharing and Analysis Centres 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 [13].

Information Sharing and Analysis Organisation (ISAO)

An ISAO is any entity or collaboration created or employed by public- or private sector organisations, 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. Unlike ISACs, ISAOs are not sector-affiliated and they are for any sector or community. Being a member of an ISAO does not require of being a part of functions vital for society [14].

Industrial Internet of Things (IIOT)

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. The major area where IOT deals with energy management systems is the smart grid. IOT extends the benefits of smart grid beyond the automation, distribution and monitoring being done by the utilities [15].

RAF (Risk Assessment Framework)

A risk assessment framework (RAF) is an approach for prioritising and sharing information about the security risks posed to an information technology organization. According to National Institute of Standards and

Technology (NIST) [16], the purpose of risk assessments is to inform decision makers and support risk responses by

- identifying relevant threats to organisations or threats directed through organisations against other organizations;
- identifying vulnerabilities both internal and external to organisations;
- impact to organisations that may occur given the potential for threats exploiting vulnerabilities and
- likelihood that harm will occur. The result is a determination of risk.

RMF (Risk Management Framework)

The RMF is a structured and flexible process for managing security and privacy risk that includes information security categorisation; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring [17].

Standard ISO/IEC 27010:2015

ISO/IEC 27010:2015 “Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications” is a key component of trusted information sharing. It 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)

Tactics, techniques, and procedures describe the behaviour of an actor. Tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower level, highly detailed descriptions in the context of a technique [19].

Threat Information

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 indicators, TTPs, security alerts, threat intelligence reports, and tool configurations [19].

3.2 Characteristics of cyber information sharing models

Goal of Cyber Threat Intelligence Sharing is to create an ecosystem where actionable cyber threat intelligence is automatically shared in real-time to enable real-time defence, the detection, prevention and mitigation of cyber threats before or as they occur.

The five issues to be solved are:

1. What to share?
2. With whom to share?
3. Why to share?
4. What are the main challenges of threat information sharing?
5. How to share? (Sharing architectures; Sharing methods; Exchange methods; Mechanisms of sharing)

Below, these issues are addressed.

3.2.1 What to share?

There are different types of cybersecurity-related information that could be shared to improve cybersecurity defences and incident response. Munk [20] divides this information into four major groups: information related to events, to vulnerabilities, to threats, and other information. Sedenberg’s and Dempsey’s [21] division includes incidents (including attack methods), best practices, tactical indicators, vulnerabilities, and defensive

measures. According to them, organisations are engaged in sharing tactical indicators ("indictors of compromise", IOCs). IOCs are artefacts that relate to a particular security incident or attack, such as filenames, hashes, IP addresses, hostnames, or a wide range of other information. Cybersecurity defenders may use IOCs forensically to identify the compromise or defensively to prevent it [21]. As a summary, cyber threat information is any information related to a threat (Indicators of compromise, TTPs, Security alerts, etc.) that might help an organisation to protect itself against a threat or detect the activities of potential or actual threat actor:

- *Indicators of Compromise (IoCs):* Indicators are technical artefacts or observables (an observable is an event, benign or malicious, on a network or system) that suggest an attack is imminent or is currently under way, or that a compromise may have already occurred. Examples of IoCs include unusual outbound network traffic, anomalies in privileged-user account activity, suspicious registry or system file changes. Other examples: IP addresses, specific strings of data, and file hashes, exploit toolkits or payloads. IoCs are specific, common, and repeatable forms of information that readily lend themselves to anonymization, standardisation, and rapid forms of distribution. These indicators can be effectively anonymised to obscure the target of an attack. Sharing this kind of information poses low risk of disclosure of personal information or sensitive company and customer information. Technical threat indicators account for the vast majority of threat information that is available. Significant gains can be achieved through automated sharing of technical indicators. [22]
- *Security alerts:* Security alerts, also known as bulletins, advisories, and vulnerability notes, are brief, usually human-readable, technical notifications regarding current vulnerabilities, exploits, and other security issues. Security alerts could originate from sources such as CSIRTs, SIRTs, commercial security service providers, and security researchers.
- *TTPs:* Tactics, techniques, and procedures could describe an actor's tendency to use a specific malware, attack tool, or delivery mechanism.
- *Tool configurations*: Tool configurations are recommendations for setting up and using tools that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.
- *Threat intelligence reports:* Threat intelligence reports are generally documents that describe TTPs, actors, types of systems and information being targeted, and other threat related information that provides 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.

3.2.2 With whom to share?

Organisations that collect and share knowledge and experiences typically do this to improve defensive capabilities.

Actors involved are:

- *Governments and Public safety organisations* have to defend their own classified and unclassified systems, fight cybercrime, and decrease the cybersecurity risk.
- *Private critical infrastructure:* it is important to protect critical infrastructures to ensure critical national interests like public health and defence.
- *Business enterprises:* Business companies have an interest in preserving the security of sensitive information (customer and supplier data, trade secrets, contract information, etc.).
- *IT companies:* IT companies have an interest in preserving the security and integrity of their products. They often share information with regard to vulnerabilities in products or services to make sure that security firms can create solutions to fix them, or they may produce and distribute software updates that remedy vulnerabilities for their customers.

- *IT security firms*, computer forensics experts, antivirus and antimalware vendors and penetration testers, collect and sell cybersecurity information.
- *Security researchers* study cyber incidents and find vulnerabilities in software, hardware, and services through academic work. They usually help to mitigate threats and remedy weaknesses. [23]

3.2.3 Why to share?

An organisation that has faced an attack acquires valuable information on cyber threats that is potentially useful to other organisations. This information can help an organisation to identify, assess, monitor, and respond to cyber threats. Organisations that share cyber threat information can improve their own security postures as well as those of other organisations. Information sharing among private and public entities is a powerful mechanism to better understand a constantly changing environment and learn in a holistic way about serious risks, vulnerabilities and threats, as well as solutions.

In particular, there are some key points regarding the why to share:

- *Improved preventive functions:* Development of the cyber-ecosystem among smart societies require faster response against hybrid-threats. For example, IIOT sets challenges for the critical infrastructure protection in industrial sector. Near real-time information sharing requires further developed sensor- and signal techniques.
- *Enhanced threat understanding:* By sharing threat information, organisations gain a better understanding of the threat environment and can use threat information to enhance their cybersecurity and risk management practices. Using shared information, organisations are able to identify affected platforms or systems, implement protective measures, enhance detection capabilities, and more effectively respond and recover from incidents based on observed changes in the current threat environment.
- *Knowledge maturation:* When seemingly unrelated observations are shared and analysed by organisations, those observations can be correlated with data collected by others. This enrichment process increases the value of information by enhancing existing indicators and by developing knowledge of actor TTPs that are associated with a specific incident, threat, or threat campaign. Correlation can also impart valuable insights into the relationships that exist between indicators.
- *Increase the degree of protection:* organisations that act upon the threat information they receive by re-mediating threats to themselves afford a degree of protection to those who are yet unprotected (i.e., who have either not received or not acted upon the received threat information) by reducing the number of viable attack vectors for threat actors, thus reducing vulnerability.
- *Greater defensive agility*: Actors continually adapt their TTPs to try to evade detection, circumvent security controls, and exploit new vulnerabilities. Organisations that share information are often better informed about changing TTPs and the need to rapidly detect and respond to threats.
- *Improve cyber defence*: Similar attack methods are used against a wide range of targets so, sharing information can help organisations to improve their cyber defence and leverage the resources expended by others to improve the value of their investments. The approach, where one organisation's detection becomes another's prevention, is a modern sophisticated concept that strengthens the organisations' security in advance.
- *Improve awareness*: Information sharing enables organisations to leverage the collective knowledge, experiences, and analytic capabilities of their partners within a community of interest, thereby enhancing the defence capabilities of multiple organisations. Even a single contribution (a new indicator or observation about a threat actor) can increase the awareness and security of an entire community.
- *Build trust:* The ability to repeat ad hoc exchanges over time builds trust and an expectation that parties will act in a consistent and repeatable way that minimizes harm and maximizes protection.

3.2.4 What are the main challenges of threat information sharing?

- *Establishing trust:* Nothing else but the trust is at first. Trusted relationships form the basis for information sharing but require effort to establish and maintain. Ongoing communication through regular in-person meetings, phone calls, or social media can help accelerate the process of building trust. Trusted relationships foster confidence that information provided will be acted upon and that it will be protected and/or shared appropriately. Although trust is powerful, it is also fragile and, if broken, can have devastating consequences for all parties. Furthermore, trust is impossible to effectively legislate. So, given the complexity of the cybersecurity threats, a private and public collaborative approach to information sharing is called for. Laws can compel incident reporting, but they do not increase trust or collaboration, nor do they reduce risks.
- *Achieving Interoperability:* Standardised data formats and transport protocols are important building blocks for interoperability and help enable the secure, automated exchange of structured threat information among organisations, repositories, and tools. Adopting specific formats and protocols, however, can require significant time and resources, and the value of these investments can be reduced if sharing partners require different formats or protocols.
- *Protecting sensitive but unclassified information:* Disclosure of sensitive information, such as intellectual property, trade secrets, or other proprietary information can result in financial loss, violation of sharing agreements, and loss of reputation. The unauthorized disclosure of information may disrupt an ongoing investigation, jeopardize information needed for future legal proceedings, or disrupt response actions such as botnet takedown operations. Organisations should apply handling designations to shared information and implement policies, procedures, and technical controls to actively manage the risks of disclosure of sensitive but unclassified information.
- *Protecting classified information:* Information received from government sources may be marked as classified, making it difficult for broader number of organisations to use. It is also expensive and time-consuming for organisations to request and maintain the clearances needed for ongoing access to classified information sources.

There are many reasons why entities may restrain to participate in cyber information sharing, including the potential liability that could result from sharing internal cyber threat information with other private companies or the government.

More broadly, the legal issues surrounding cybersecurity information sharing – whether it is with regard to sharing between two private companies or the dissemination of cyber intelligence within the government are complex.

It is important to create a legal framework for sharing cyber information. The issues of what, with whom, and for what (for what purposes) that information can be shared are necessary to be defined. Also, it is necessary to determine the whole scope and overall goals of cyber security legislation itself.

3.2.5 How to share? Sharing architectures

There are few existing cybersecurity information sharing architectures and frameworks for the warning systems within public organisations divided into main groups as Figure 3 illustrates. MITRE [24] categorises information sharing models in three main models. Fourth model comprises combination of the others.

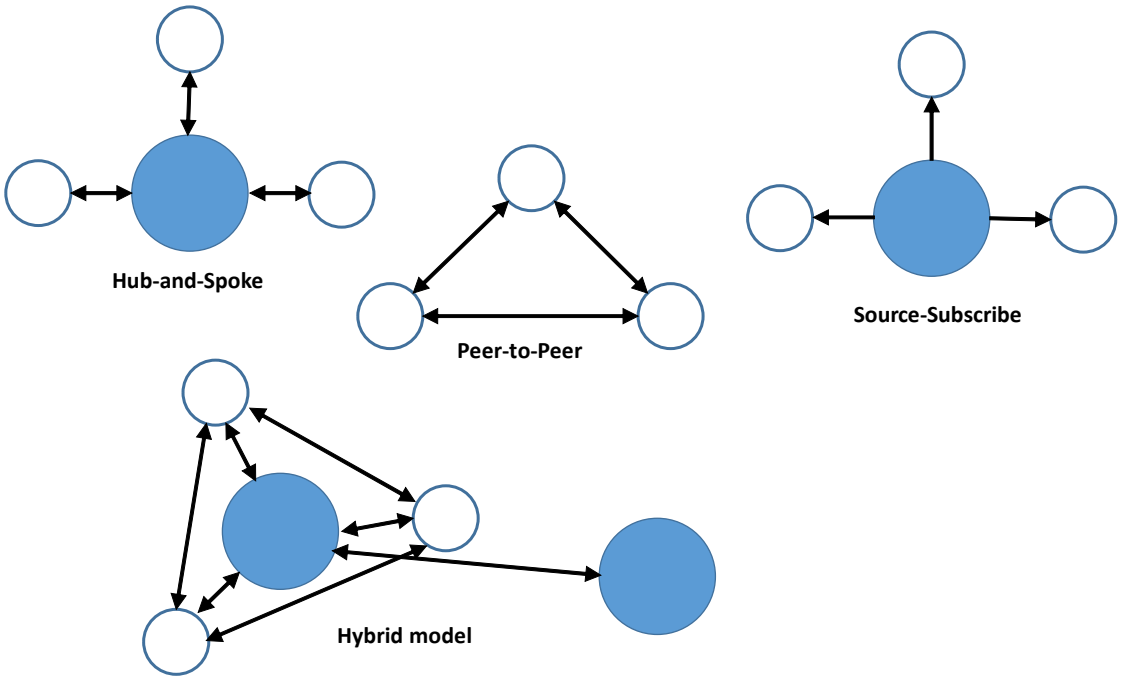

Figure 3: Traditional classification of information sharing models

Hub-and-Spoke

Hub-and-Spoke architecture, according to what The MITRE Corporation said in [25], has a central hub that receives data from the participating members (the spokes). The hub can either redistribute the incoming data directly to other members or provide value-added services and send the new information to the members. With this approach, the hub acts as a clearinghouse that can facilitate information sharing while protecting the identities of the members. In addition, the hub may provide value by combining information from multiple members, by adding its own data, or by conducting extra analyses on the members' data. Spokes can produce and/or consume information from the Hub. [25]

Example of private sector associations that use and hub and spoke model are *Information Sharing and Analysis Centers* (ISACs) that are non-profit organisations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis. [25] These bodies operate in a hub-and-spoke model in which members from a certain industry or region gather to share cyber threat data to centrally located analysts, who enrich and disseminate intelligence back to the community. [26]

In the ISAC model, businesses can engage to exchange security information on phishing campaigns, malware attacks, systems vulnerabilities or other threats in order to strengthen each other with indicators and prevent incidents before they can impact the broader group. These communities typically adopt rules to manage the dissemination of the information, allowing anonymous sharing to protect companies' reputation. [27]

An example of network that use hub and spoke model is the Dutch National Detection Network (NDN). The National Detection Network (NDN) is a collaboration for a better and faster detection of digital dangers and risks. By sharing information about threats, parties can take appropriate measures timeously as part of their own responsibility, to limit or to prevent possible damage. [28]

NDN focuses on two distinct target groups:

- Private companies in industries that are considered crucial for the proper functioning of Dutch society. Examples of such industries are energy, water, and telecommunications.

- Departments and agencies of the Dutch national government, e.g., the ministries and executive bodies such as the tax and customs administration.

NDN employs the MISP platform for all automated exchange of (technical) threat information. NDN was set up as a centralised service facilitated by centralized technical infrastructure (hub–spoke architecture). This approach was chosen to ensure that the uptake of the community would not be hindered by practical obstacles.

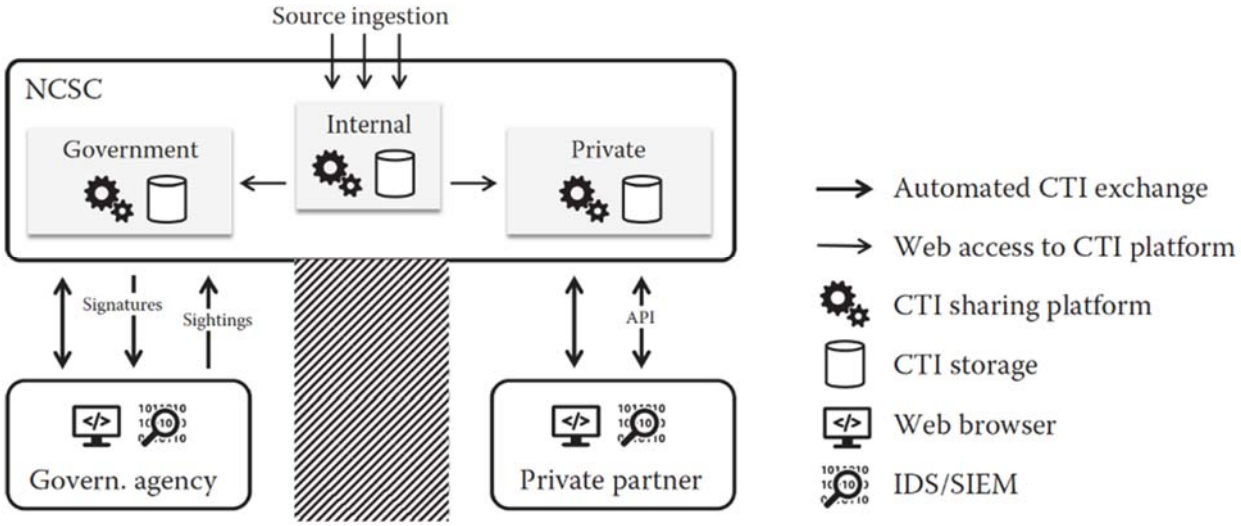

Figure 4: A national detection network

Other examples of organisations that use hub and spoke model are national CERTs, DHS AIS, US-CERT, Electronic Crimes Taskforce (ECTF), FBI's e-guardian and ECS.

Advantages: This is a cost-effective model for crowdsourcing additional security but among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis. [27]

Challenges: According to what The MITRE Corporation said in [25], the entire system relies on the functioning of the hub, which makes the system vulnerable to delays and systemic failures. If the hub is not working well, then the entire information-sharing mechanism will not work well. The more members that participate in the exchange, the more information will be sent to the hub for processing, filtering, analysis, and distribution. While more information can provide greater analytic insight, it can also increase the burden on the hub and possibly introduce delays into the system. Because the most valuable information is often time-sensitive, delays in distribution can reduce the benefits of the information-sharing mechanism. Finally, a hub-and-spoke model can be expensive. The more "value-added" services are provided by the hub, the more it will cost. If the costs are borne by the members, then those fees will become requirements for entry into the exchange. If those fees are high, they may preclude certain companies from joining the group. [25]

According to what The MITRE Corporation said in [25], a related challenge is that sharing information in this model requires a high degree of trust in the hub. It may be difficult to create a hub-and-spoke structure around either a for-profit company or a government agency. In the former case, there may be natural conflict-of-interest issues and/or members may be reluctant to share information with another company that is trying to maximize profits while acting as a trusted third party. In the latter case, companies may be reluctant to share information directly with a government agency, due to fears of information being leaked or disclosed by *Freedom of Information Laws requests* that allow access by the general public to data held by national governments. In addition, there are cultural barriers that often lead companies to distrust the government. Companies need to feel that the benefits they gain by sharing sensitive information with the government must outweigh the risks;

often, this barrier is not crossed. For this reason, it is important that common rules and regulations have been implemented.

Peer-to-peer

This model is defined generally by the ability of any member of a community to interact and share with any other member, rather than going through a central hub.

According to what The MITRE Corporation said in [25], because information is shared among participants, there must be trust relationships among all members of the exchange or the model will not work well. One way to build an atmosphere of trust is to design the information exchange to a specific mission. This will create an environment where members face common threats. They will seek to share information and focus the community around those threats. Having a specific mission makes it easier to define membership and provide direction. Furthermore, trust in a community is a function of how much members believe that other members support the same mission, respect the community rules, and are willing to participate on a reciprocal basis. Thus, building an information-sharing system for a specific mission can maximize trust, if it is implemented properly. In addition, trust is facilitated and strengthened through face-to-face meetings and individuals who have a long history of personal rapport. It is important that the information-sharing model develop vetting requirements and procedures to facilitate the introduction of new members and to maintain communication among existing members. The security, speed, and convenience of these communication mechanisms will vary with the mission and requirements of the organisation. [25]

Peer-to-peer networks can be especially beneficial for smaller communities or when members only interact with a part of a community. They may also be especially beneficial for those whose members have asymmetrical trust relationships or share under highly dynamic conditions that often change based upon content, current threat, and so on.

An example of a peer-to-peer sharing community is the ETIS CERT-SOC Telco Network. ETIS, the community for telecom professionals, is a membership-based organisation that facilitates collaboration among European telecom providers. Its member base covers a substantial portion of the European telco landscape. Early 2013, ETIS established the so-called CERT-SOC Telco Network, comprised of security operations and incident response specialists in the various member organisations. A key activity of this group is the exchange of threat information and incident response experiences. [29]

The telco group used the MISP platform to establish its automated threat exchange channels.

Very important telecommunication players like Proximus, Kpn, Swisscom and A1 Telekom Austria joined to CERT-SOC Telco Network.

Advantages: Because members share directly with each other, information dissemination is quick and can be easily scaled to many participants. A peer-to-peer model can also be inexpensive, because there is no need to pay for a central hub. On the other hand, this model does not contain built in “value-added” services; the only information that is flowing between members is the data collected and analysed by the members. This places a premium on sharing the right kinds of information.

The greatest benefit would be derived from sharing intrusion attempt information (i.e. information about incidents, regardless of actual intrusions).

There are many good reasons for sharing intrusion attempt information:

- *It is less sensitive than other types of data.* Information about attempted intrusions is less revealing that information about successful intrusions. Other members will not know if the attempts were successful; therefore, they cannot draw conclusions about a given company’s vulnerabilities or its information security capabilities;
- *It can be disseminated quickly*. Because intrusion attempt information requires less sanitization and analysis than other types of incidents, it can be shared quickly with other members. Timeliness is critical because adversaries adapt their tactics and techniques quickly;

- *It is actionable*. Intrusion attempt information can be acted upon in a timely fashion. If one organisation alerts other organisations that it has detected a specific type of malware or a particular type of social engineering attack, other organisations can look for similar patterns. This can be done quickly, without revealing sensitive information to each other.

Challenges: a challenge is the difficulty managing many trust relationships when community membership grows. To scale effectively, members must agree on a common taxonomy for incident information and a template for sharing relevant information while making information anonymous and removing sensitive data. A related challenge of a post-to-all information exchange is that members must have infrastructures that protect and support the communication of relevant information and processes that allow for identifying and acting on high-priority incidents. If such infrastructures and processes place a heavy burden on member organisations, they will be reluctant to exchange information. Information security staffs are often incredibly busy; therefore, the information sharing process must be easy. That is one reason why introducing automation can be beneficial. If a company can receive an alert in a format that can be ingested and interpreted by a computer, then the people involved can focus on analysing and evaluating response actions. [25]

Then redundant sharing of the same information may be more likely in this model, and it may lead to inefficient "churn" depending upon technology and other conditions.

The peer to peer model is challenging and multi complex model to manage in an international environment and can create an unnecessarily confusing operating environment.

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 [24].

Hybrid

An information exchange could use a peer-to-peer model for the exchange of intrusion indicators while sending incident-response data to a centralized hub. This hub could conduct analysis on the data coming from multiple organisations to produce analytic reports for all to use. A second option would allow members of the information exchange to send the same data to each other and to a central hub. [25]

A hybrid model can also mean that there are two or more hubs on EU level. This means strengthening of the national hub. A European hub would be the main hub but there would be sub-hubs at national level. Interpol and other supranational organisations that investigate crime also need data for crime prevention. For this reason, too, one centralized hub may become too challenging.

Advantages: the benefit would be the ability to act on time-sensitive data through direct, collaborative sharing while leveraging the value of the hub's ability to collect, synthesize, and analyse data across the membership and disseminate findings in the longer term.

The hybrid model extends the ability to exchange sensitive data to and among public safety authorities quickly. It also allows to select alternative data sharing paths if for one reason or another, the main line of information sharing does not work.

Challenges: establishing and running a hybrid arrangement is difficult. The mechanics of sharing information across two different architectures can become complicated, and the governance of such a model can be a challenge. In addition, the costs associated with an exchange using a hybrid model will be greater than those for an exchange that relies on a single model. [25]

In any case, the hybrid model cannot be implemented directly to state infrastructure but the first cycle of generating hybrid model is the Hub and Spoke model. Controlled development into a hybrid model also means

that national challenges and cultural differences have been resolved. Development of this information sharing model as part of continuity management is highlighted at EU level.

3.2.6 How to share? Sharing methods

Publish-subscribe

The publish-subscribe method for sharing threat intelligence consists of a producer who publishes information on a regular or irregular basis, and whose publications are individually subscribed by one or more community members. This approach can be applied in either the peer-to-peer or the hub-and-spoke sharing models. In the case of a peer-to-peer network, a producer could, for example, automate cyber threat indicator sharing into a repository from which other members pull feeds, or a producer can post to a message board/forum and subscribers receive alerts. In the case of the hub-and-spoke model, the publisher may be the hub and the producers (members) could submit to the hub for processing, usually to verify, refine, de-duplicate, or correlate with other known threat intelligence, before publishing it out to the subscriber base. One of the benefits of the publish-subscribe method in a hub-and-spoke model is the ability to aggregate and analyse information in a central location and then publish a richer, more complete picture of an incident or actor. This is very useful in a rapidly evolving environment when many participants may be sharing different observations and analyses.

Crowdsourcing

Crowdsourcing occurs when members collectively contribute to a discussion thread, an automated cyber threat sharing repository, or another system to organically transform granular threat data into more coherent threat intelligence. By virtue of participating in crowdsourcing the intelligence picture, the information is also shared with members. Like the publish-subscribe method above, crowdsourcing can take place in both peer-to-peer and hub-and-spoke networks, the key distinction being the presence of a central party directing the crowdsourcing through the hub, versus true organic freewheeling among the community. Both, of course, can be very effective. One of the benefits of crowdsourcing is that regular social interactions among members help to build trust and strengthen the community.

3.2.7 How to share? Exchanges methods

Organisations can exchange information any number of ways. The four most commonly used, according to what Cristin Goodwin and J. Paul Nicholas said in [23], are formalized, security clearance-based, trust-based, and ad hoc. In almost all situations, the method of exchange determines which actors can be included and it defines the scope of the program. Therefore, when designing an exchange, it is important to determine the method that best corresponds to the group membership and its goals.

Formalized exchanges

A formalized exchange is one based on an agreement, such as a non-disclosure agreement, legal contract, or a membership agreement. Its conditions identify the parties and often state what information is to be exchanged, how it can be used, and how its confidentiality will be protected. One example of a formalized exchange is the Microsoft Active Protections Program (MAPP), a program for security software providers that currently brings together more than 80 partners. Members of MAPP receive security vulnerability information from the Microsoft Security Response Center (MSRC) in advance of the monthly security updates from Microsoft. This information enables them to give their customers updated protections, such as antivirus software, network-based intrusion detection systems, or host-based intrusion prevention systems. Another example is the Asia Pacific Computer Emergency Response Team, a membership-based organisation established to enhance cooperation among more than 30 CERTs in the Asia Pacific region. [23]

Security clearance-based exchanges

Certain information-exchange programs, especially those involving intelligence services, need to exchange classified and other sensitive information through protected channels, sometimes directly with a single party. A security clearance-based exchange represents a subset of a formalized exchange, one that is narrower in scope and participation. In the long term, the security clearance process builds trust between participants. However, it can also severely constrain the actors involved, such as limiting participants to those of a particular country—a challenging requirement in a global market. Getting private sector participants cleared can be difficult and slow and is made even more complex by the international workforces found in large technology companies. Such classified exchange is more likely to be successful when involving defence contractors or other entities which are accustomed to working with classified material. [23]

Trust-based exchanges

Trust-based groups are often closed groups of like-minded cybersecurity actors who inform one another on an ad hoc basis when they see security issues of common concern. They work on the principle that trust is extended to unknown members through chains of trusted relationships with other known members. They generally do not have formal agreements or contracts covering the exchange of information between members, but they may implement systems like the Traffic Light Protocol (TLP). The TLP uses a color-coded system to identify those with whom information may be shared, thus signalling originator's intent and easing fears about the extent of disclosure. The TLP also speeds information exchange, since recipients intrinsically know with whom they can share that information—without having to refer to the originator for permission to share it. Systems to establish and maintain trust among members can range from simple nominations by existing members to rigorous vouching and vetting systems. Trust is often afforded to individuals and not directly to the organisations for which they work. This means that, if an individual leaves an organisation, the organisation may not have the right to nominate another representative. Trust is built among participants based on their contributions, collective actions, and shared experiences. [23]

Ad hoc exchanges

Episodic or ad hoc information sharing often occurs in response to particular events, such as a new challenge or crisis, and is often of limited duration. This type of sharing is highly relevant and very focused on solving a particular set of problems. When successful, it can lay the foundation for more organized exchanges. [23]

3.2.8 How to share? Mechanisms of sharing

An information exchange may use multiple mechanisms, depending on the nature of the information, actors involved, and the issues being addressed. To identify the most appropriate mechanism, the levels of automation required, and the format of the information being exchanged need to be considered. According to what Cristin Goodwin and J. Paul Nicholas said in [23], information exchange mechanisms are two: Person-to-person exchange mechanism and machine-to-machine mechanism.

Person-to-person exchanges

Many information exchanges are person-to-person exchanges of unstructured information. The most common mechanisms are email and phone calls, although encrypted email and web portals may also be used. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC)4 and the US CERT allow participants to submit threat data that they collect through a web portal. Another example is the UK self-help portal for small communities, "Warning, advice and reporting point" (WARP),5 which is based on ISO 270106 and which encourages information sharing. Such an exchange mechanism is potentially valuable because it can handle large amounts of data and can allow participants to anonymously submit information. However,

the challenge with person-to-person exchanges is that they are difficult to scale, requiring significant personal relationships with history and trust to facilitate the exchange of information. [23]

Machine-to-machine exchanges

Among security professionals, there is currently a lot of focus on developing systems that automate the exchange of information. It is believed that such systems enable actors not only to identify information important to them more quickly, but also to automate mitigations to threats as they occur. In the United States, recent examples of machine-to-machine information exchanges include: the Security Event System and its Collective Intelligence Framework component, from the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC); Public Regional Information Security Event Management (PRISEM), from the state of Washington; and the Enhanced Cybersecurity Services (ECS) offered by the US Department of Homeland Security (DHS). Microsoft Interflow10 is a security and threat information exchange platform for professionals working in cybersecurity that works with a similar set of principles. It uses industry specifications, such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), to create an automated, machine-readable feed of threat and security information that can be shared across industries and groups in near real time. This can help reduce cost and increase the speed of defense by automating processes that are currently often performed manually. [23]

3.3 Cyber information sharing governance structures

Annex 3 has a section that discusses cyber information sharing governance structures. Its Table 1 introduces some articles with regard to cyber situational awareness information sharing, and Table 2 presents the taxonomy on information sharing models developed by Sedenberg and Dempsey [21]. They identify the following different cyber information sharing models:

- Government-centric is centralised model where one central organisation may share the information exchange or perform processing to enrich the data to others [30], [31]. The Department of Homeland Security is one kind of hierarchical Government-centric organisation. The central infrastructures use open, standard data formats and transport protocol [30].
- Sector-based Information Sharing and Analysis Centers (ISACs) are examples of Government-Prompted, Industry-Centric Sharing Models. 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 (NIPP13) [32]. The National Cybersecurity and Communications Integration Center (NCCIC) works in close coordination with all of the ISACs via the National Council of ISACs. 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 on their own initiative without government intervention to coordinate information sharing. These information exchanges can be tailored to fit the specific needs of their members [21].
- Individual-Based Groups are small online communities of peers to share sensitive information with the goal of combat attacks immediately. These groups require a high degree of trust [21].
- 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.

- Proprietary Products and Commercialised Services consists e.g. 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 [21].

3.4 Sharing Technologies for Cyber Security Information

Table 3 of Annex 3 presents the most popular technical standards for sharing cybersecurity information required in cyber situational awareness.

The U.S Department of Homeland Security uses a system called Automated Indicator Sharing (AIS)[1] for providing the bidirectional sharing of the cyber security threat indicator information. AIS participants are connect to the DHS-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 them to exchange indicators with the NCCIC as Figure 5 illustrates. Participants receive and can share DHS-developed indicators that they have observed during their own network defence efforts. DHS will then share these indicators to all AIS participants [33].

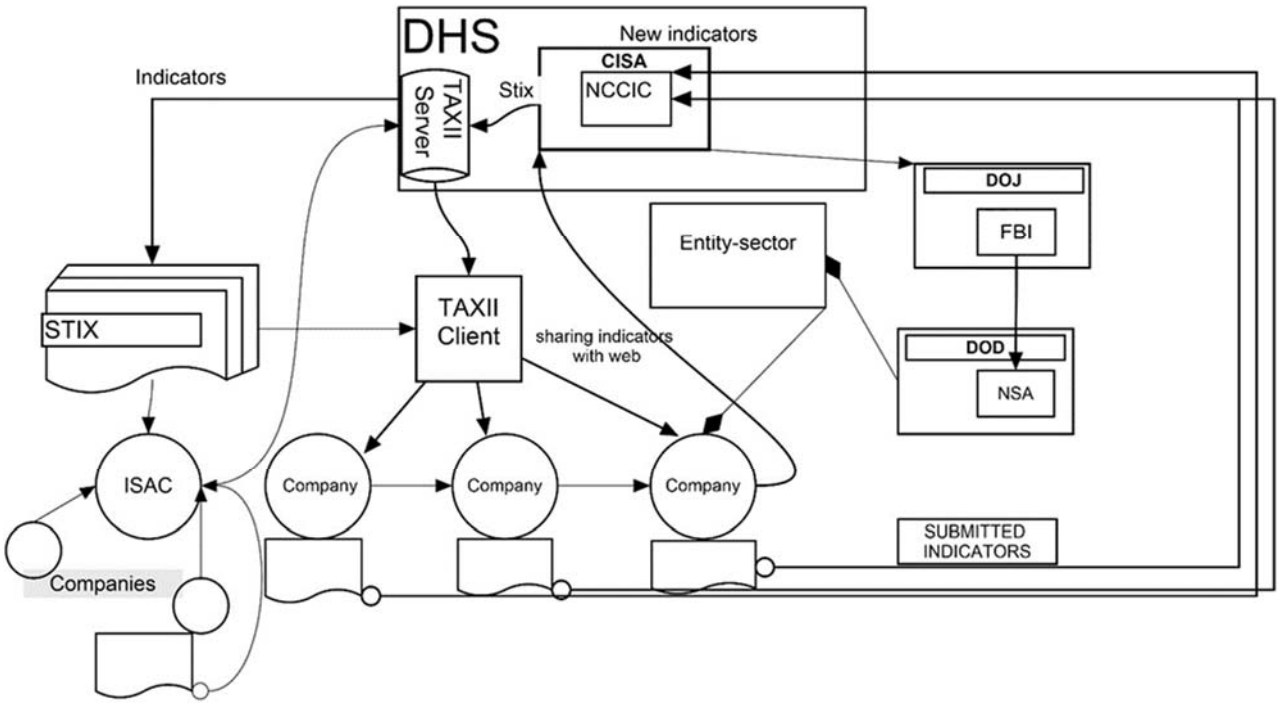

Figure 5: Cyber information sharing model in the U.S.A

Stakeholders who share indicators through AIS will not be identified as the original source of those indicators to other participants unless they affirmatively consent to the disclosure of their identity. Senders are anonymous unless they want DHS to share it. Indicators are not validated by DHS as the emphasis is on velocity and volume: our partners tell us 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. The U.S. Government also need useful information about indicators [33].

AIS utilises 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

[1] https://www.us-cert.gov/ais

serialisation format that enables organisations to exchange Cyber Threat Intelligence (CTI) in a consistent and machine-readable manner. TAXII is an application layer protocol used to exchange CTI over HTTPS. Figure 1 of Annex 3 presents the architecture of STIX, and its Figure 2 demonstrates STIX use cases where also cyber security information sharing between organisations is implemented

OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society. It defines twelve STIX Domain Objects. Attack Pattern is a type of TTP that describes ways threat actors attempt to compromise targets. Campaign is a grouping of adversarial behaviours that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets. Course of Action is an action taken to either prevent an attack or respond to an attack. Then Identify Individuals, organisations, or groups, as well as classes of individuals, organizations, or groups. Indicator means a pattern that can be used to detect suspicious or malicious cyber-activity. Intrusion Set is a grouped set of adversarial behaviours and resources with common properties believed to been organised by a single threat actor. 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. Observed Data means conveys information observed on a system or network (e.g., IP address). Report consists 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.

TAXII is the main transport mechanism for cyber-threat information represented in STIX. As Figure 6 shows, collection based communications means the situation when a single TAXII client makes a request to a TAXII server and the TAXII Server carry 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 application programming interface root. Stakeholder may share indicators with DHS through an ISAC or an ISAO without TAXII client [34].

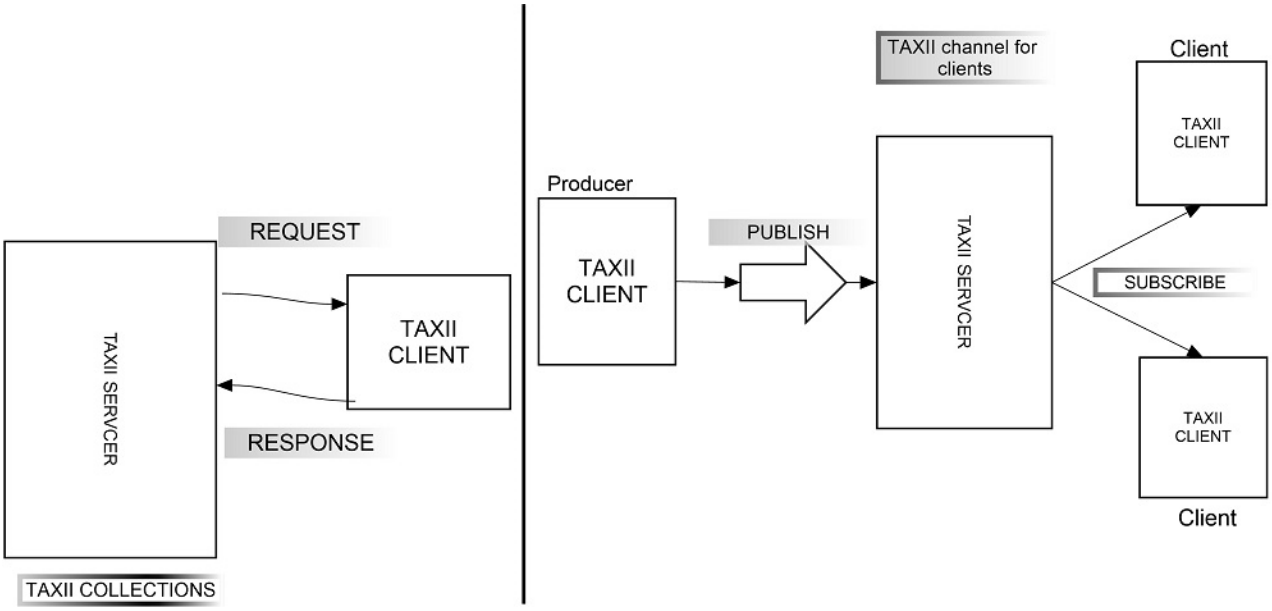

Figure 6: Flow of cyber threat information in TAXII (Modified from [35])

Kokkonen, et al. [36] implement and evaluate a model for creating the information sharing communities for the cyber security situational awareness information. The model is presented and discusses in Annex 3.

Traffic Light Protocol (TLP) facilitates a four-colour category for information sharing (red, amber, green, white). Red means "not for disclosure, restricted to participants only" and the meaning of white is "disclosure is not

limited". The TLP categories can be applied as a part of information sharing rules and topology construction for filtering data between organisations [37].

3.4.1 Information sharing methodologies between CERTS/ CSIRTS and Law Enforcement

Enhancing cooperation between EU member states, EU agencies and related Network and Information Security (NIS) communities as CERTS is also a crucial part of the cyber-ecosystem. It is not enough that small closed groups share information with each other without synergy to public safety organisations.

The main goal of the Europol Information System (EIS) is to be the reference system for offences, individuals involved, and other related data to support EU Member States, Europol and its cooperation partners in their fight against organised cybercrime, terrorism, and other forms of serious crime. For example, European Cybercrime Centre (EC3) as a part of Europol uses open source Malware Information Sharing Platform (MISP) [6].

MISP is a tool for information sharing about malware samples and related malicious campaigns related to specific malware variants. It offers architectural flexibility allowing the utilisation as a centralised platform (e.g. CIRCL and FIRST instances), but also as a decentralised (peer-to-peer) platform[2]. MISP project designed the Permissible Actions Protocol (PAP) to indicate how the received information can be used.

Europol's Secure Information Exchange Network Application (SIENA) has been established to allow EU Member States to communicate and share intelligence. SIENA is a Virtual Private Network (VPN) designed to enable 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.

In USA, National Information Exchange Model 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 [38].

The Federal Bureau of Investigation (FBI) hosted InfraGard's Secure Web Portal allows secure messaging that promotes communication among members. Memberships give access to iGuardian, the FBI's cyber-incident reporting tool designed specifically for the private sector. InfraGard membership allows also 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, DHS, and the National Infrastructure Protection Plan [32].

Digital Forensics XML toolset is intended to represent the following types of forensic data [39]:

- Metadata describing the source disk image, file, or other input information.
- Detailed information about the forensic tool that did the processing (e.g., the program name and where the program was compiled, linked libraries).
- The state of the computer on which the processing was performed (e.g., 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.

[2] https://misp-project.org/

The Cybersecurity Information Exchange Framework (CYBEX) will advance the development of automating cybersecurity information exchange. CYBEX Forensics domain is an operation domain that supports law enforcement operations by collecting evidences. 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 [40].

CYBEX-P and Privacy-Preserving Cybersecurity Information Exchange mechanism are modified from CYBEX and both based on an information sharing platform with a robust operational and administration structure. Privacy-Preserving Cybersecurity Information Exchange mechanism enables the organisations to share their cybersecurity information without revealing their identities [41]. 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 prevent future cyber-attacks. 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 the 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 [42]. 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 [42].

When the aim is to share essential information between stakeholders as soon as possible, information sharing must be automatized.

3.5 Shared situational awareness

Theory of Situational Awareness (SA) is discussed in Annex 4, in which e.g. Endsley's [43] situational awareness model is presented (Figure 2 of Annex 4). Annex 4 considers also the general requirements for situation awareness. But what the terms "shared situational awareness means"? Public safety actors like European law enforcement agencies need common shared situational picture for the cross-boarding tasks in a way that operational co-operation be based on reliable platform.

According to [44], good team SA dependent on team members understanding the meaning of the shared information between them. This means that teams need to share pertinent data and the higher level of SA [44], [45]. According to [20], cooperation between cybersecurity organisations based on effective and efficient exchange of information. Information interoperability is the joint capability of different actors like persons, organisations and groups necessary to ensure exchange and common understanding of information needed for their successful [20]. Humans are not as good at processing large volumes of data, quickly and consistently. Flexible autonomy should provide smooth, simple, seamless transition of functions between human and the system [43].

Shared (cyber) Situational Awareness is closely related to (cybersecurity) information exchange, because without trusted information sharing a common situation or situational awareness is insufficient [46]. The development of shared Situational Awareness consists four factors as follows [46]:

1. Shared SA requirements (team members degree to understand which information is needed by other team members),
2. Shared SA devices (communications),
3. shared SA mechanism (shared mental models) and
4. Shared SA processes (effective team processes for sharing relevant information).

3.6 Remarks

The literature review indicates that “cyber security information sharing” is not precisely defined in the area of cyber security. As mentioned above, the structures of the information sharing models are generally very sector-specific and created in different environments. There is a need for a common early warning solution. Usually a word “warning” means also preventive functions as US intelligence services operates. The fight against hybrid threats means not only preventing cyber-attacks, 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 major hybrid incident must be directly shared to the national participant’s e.g. cyber security 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 primary importance. The essential information should process to the desired shape for the participants. In the future cyber-defence operations are more integrated and automated according to local capabilities, authorities and mission needs. Shared common operational picture means that real time communication link from local level to nation and EU level exist. A common cyber situational awareness is needed for both operating CPS and for emergency and crisis management. There should be the connection between cyber situational awareness and emergency management.

When developing an early warning system at the EU level, three requirements exist: 1) The possibility that some EU Member State may leave an early warning system; 2) engaging participants in the values of western world; and 3) the possibility of joining Cyber Threat Warning System to NATO Cyber Situational Awareness Solutions. These factors have a direct link to sharing confidential information.

It is important to take into account how national Cyber Security Centres cooperate with other organisations within critical infrastructure in national level. The states departments of the United States work closely together in the fight against threats in the field of cyber security. The organisations of public administration in European Union work together more formally. This is important noticed when cyber security expertise is being strengthened. The fundamental problems of the European community must be solved before permanent solutions can be built. However, this does not prevent the development of operating models, but this factor must be taken into account when developing new systems. Firstly, confidence between member states must be on a stable basis.

What are those fundamental differences of administrative functions between European Union and The United States? Mainly there are more similarities than differences. Legislation and regulation between USA and EU are coming closer with each other. NIS directive in EU will help to develop next generation early warning systems. USA and EU have made quite fundamental agreements to generate a common base for fluent information sharing.

As Ilves et.al [47] mentioned there is no crucial barriers to increase collaboration concerning early warning solutions between US, NATO and EU. US’s Cyber security sharing act and Europe´s directive on Network and Information Security (NIS) have similar goals. In addition to this, EU and NATO signed a technical arrangement in 2016 to increase information sharing between the NATO Computer Incident Response Capability and EU Computer Emergency Response Team [47].

Public safety actors like European law enforcement agencies need common shared situational picture for the cross-boarding tasks in a way that operational co-operation will be based on reliable platform.

4. Analysis results

This section present the analysis results of individual case studies carried out in Task 3.2 of the ECHO project.

Section 4.1 *Taxonomies for cyber information sharing* is based on analysis results from the ECHO partners' research, development and innovation work in earlier projects. It provides a definition of taxonomies as used in the cyber domain for cyber information sharing model for collaborative incident response.

Health information sharing was selected as an example of sensitive information sharing models from other than cyber domain. Section 4.2 analyses Health Information Exchange (HIE) methods and models, and studies, for example, how to share and analyse the detected physiological profiles.

Section 4.3 analyses the information sharing models applied in maritime domain. The main research question is "how can cyber information sharing models be understood in maritime domain?"

Section 4.4 analyses inter-sector cyber information sharing models in critical infrastructure protection. It studies how the cyber situational awareness of an organisation can be developed; how do the organizations exchange their cyber security related information; and how an organisation's cybersecurity capability can be utilised more extensively?

Section 4.5 analyses cyber threat prevention mechanisms in Finland. It finds out the pros and cons of the national HAVARO system, and studies what are the factors (requirements), which effect for implementing national EWS system to common early warning ecosystem in EU level. Every EU member country has its own system for monitoring and protecting cyber domain among vital functions.

Section 4.6 compares information sharing between US and EU emphasising cyber information sharing models in US. In addition, it handles legislative factors, organisational factors and features of the models.

Effects of national fundamental risks to the international trust warning system and information sharing policy are crucial factors within smart societies. Political decision makers are elective, and also many of highest authorities are chosen based on political selection criteria. Hybrid or cyber influencing can create instability to the society in many ways, one key aim is to influence political decision-making. In practice, this means that there is a need to integrate organisational, administrative and operative functions. A trust model with cyber information sharing in CIP is a part of the preventive early warning solution. Secure national and international decision making needs a trust model. Section 4.7 studies these questions.

The E-EWS and E-FCR are two of the four vital technologies developed within the ECHO project. Both can exploit each other in order to maximise their capabilities and offerings to the users. Section 4.8 deals with the synergies of information sharing needs with E-EWS and E-FCR.

4.1 Taxonomies for cyber information sharing

This section provides a definition of taxonomies as used in the cyber domain for cyber information sharing model for collaborative incident response. These taxonomies can be used as a reference for model design and as a source for cross-case conclusions in Section 5.

The cyber domain information sharing model is comprised of multiple taxonomies to capture as much of the collaborative incident response workflow as possible in a normalised model.

The cyber information sharing model which is presented here is based on public taxonomies in support of a collaborative incident response.

4.1.1 Source information taxonomies

A list of the public taxonomies that were used as source for the cyber information sharing model for collaborative incident response is presented below.

- Structured Threat Information eXpression (STIX™)

  Structure language for cyber threat intelligence for sharing storing and analysed in a consistent manner. Lead by the OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) developments are ongoing.

  STIX 1.1.1: https://stixproject.github.io/about/

  STIX 2.0: https://oasis-open.github.io/cti-documentation/

- Malware Attribute Enumeration and Characterization (MAEC™)
  MAEC 5.0: https://maecproject.github.io/

- Incident Categories
  FIRST CASE Classification: www.first.org

- Traffic Light Protocol (TLP)
  TLP 1.0: https://www.first.org/tlp/

4.1.2 Shared coordination ticket

The cyber information sharing model within the cyber incident handling domain is based on two types of data;

- Unstructured information which can be shared in the context of wiki pages, or using an open-source tool such as MITRE ATT&CK.

- Structured information that is shared as reference data (i.e. STIX, CVE) and tickets to handle ongoing cyber incidents in a shared coordination mode.

Structured reference data entries are gathered from (public) repositories and shared with all participants in an effort to provide a global unified view on the current threats and vulnerabilities.

Tickets are shared as part of a collaborative incident response. The shared ticket is used to share the contained information across the organisational boundary. The shared fields of the ticket can be extended during the handling of the ticket. These groups of fields are specifically tailored to record information related to the ticket and are known as facets.

A shared ticket is comprised of the following fields as Table 5 illustrates:

Field	Description	Value type
Template	The template that defines the ticket fields and workflow	Template definition
Title	The name of the ticket	Text
Description	Description of the ticket	Text
Security Classification	The security classification of the ticket	Text
Handler	The assigned user to handle the ticket	The handler of the ticket
State	The workflow state of the ticket	Shared workflow state
Shared with	List of organisation the ticket is shared with	Sharing partners

Field	Description	Value type
Traffic Light Protocol	Distribution classification	**Source: Traffic Light Protocol FIRST** TLP: RED, TLP: AMBER, TLP: GREEN, TLP: WHITE
Category	Ticket categories	**Source: Incident category vocabulary STIX 1.1.1** Exercise/Network Defense Testing, Unauthorised Access, Denial of Service, Malicious Code, Improper Usage, Scans/Probes/Attempted Access, Investigation **Source: Incident Categories FIRST** Denial of service, Forensics, Compromised Information, Compromised Asset, Unlawful activity, Internal Hacking, External Hacking, Malware, Email, Consulting, Policy Violations

Table 5: Cyber-information sharing model for collaborative incident response fields

Next to ticket base fields, additional shared information includes reference links to reference information entries, attachments, and comment entries.

4.1.3 Shared Facets

A shared ticket can be extended with additional fields to allow more specific recording of contextual values; these groups of fields are called facets. The facets used for the cyber-information sharing model for collaborative incident response are detailed below.

Affected Assets

Record affected assets in the context of a ticket.

Field	Description	Value type
Name	The name of the affected asset	Text
Description	Description of the affected asset	Text
Security Classification	The security classification of the affected asset	Text
Location	The location of the asset	Text
Asset Type:	The type of asset	**Source: Asset type vocabulary STIX 1.1.1** Backup, Database, DHCP, Directory, DCS, DNS, File, Log, Mail, Mainframe, Payment switch, POS controller, Print, Proxy, Remote access, SCADA, Web application, Server, Access reader, Camera, Firewall, HSM, IDS, Broadband, PBX, Private WAN, PLC, Public WAN, RTU, Router or switch, SAN, Telephone, VoIP adapter, LAN, WLAN, Network, Auth token, ATM, Desktop, PED pad, Gas terminal, Laptop, Media, Mobile phone, Peripheral, POS terminal, Kiosk, Tablet, Telephone, VoIP phone, User Device, Tapes, Disk media, Documents, Flash drive, Disk drive, Smart card, Payment card, Media, Administrator, Auditor, Call center, Cashier, Customer, Developer, End-user, Executive, Finance, Former employee, Guard, Helpdesk, Human resources, Maintenance, Manager, Partner, Person, Unknown

Field	Description	Value type
		Source: System Type Vocabulary STIX 1.1.1 Enterprise Systems, Enterprise Systems - Application Layer, Enterprise Systems - Database Layer, Enterprise Systems - Enterprise Technologies and Support Infrastructure, Enterprise Systems - Network Systems, Enterprise Systems - Networking Devices, Enterprise Systems - Web Layer, Enterprise Systems - VoIP, Industrial Control Systems, Industrial Control Systems - Equipment Under Control, Industrial Control Systems - Operations Management, Industrial Control Systems - Safety, Protection and Local Control, Industrial Control Systems - Supervisory Control, Mobile Systems, Mobile Systems - Mobile Operating Systems, Mobile Systems - Near Field Communications, Mobile Systems - Mobile Devices, Third-Party Services, Third-Party Services - Application Stores, Third-Party Services - Cloud Services, Third-Party Services - Security Vendors, Third-Party Services - Social Media, Third-Party Services - Software Update, Users, Users - Application And Software, Users - Workstation, Users - Removable Media

Table 6: Affected asset facet fields

Data Exfiltration

Record information concerning data exfiltration.

Field	Description	Value type
Description	Description of the exfiltration	Text
First recorded exfiltration	When was the first exfiltration event recorded	Datetime
Containment achieved	When was the containment achieved	Datetime
Containment actions	The actions taken	Text
Exfiltration Targets	Targets of the exfiltration	Text

Table 7: Data exfiltration facet fields

Forensic Analysis

Record results of forensic analysis.

Field	Description	Value type
Type of Analysis	The type of analysis requested	**Source: Analysis types MAEC** static, dynamic, combination
Initial compromise time	When was the initial compromise recorded	Datetime
Last activity	Time of the last recorded activity	Datetime
Detailed results	The detailed results of the analysis	Text

Table 8: Forensic analysis facet fields

Impact Assessment

Record assessment of impact.

Field	Description	Value type
Impact effects	The possible effects of an incident.	**Source: incident effect vocabulary STIX 1.1.1** Brand or Image Degradation, Loss of Competitive Advantage, Loss of Competitive Advantage - Economic, Loss of Competitive Advantage - Military, Loss of Competitive Advantage - Political, Data Breach or Compromise, Degradation of Service, Destruction, Disruption of Service / Operations, Financial Loss, Loss of Confidential / Proprietary Information or Intellectual Property, Regulatory, Compliance or Legal Impact, Unintended Access, User Data Loss
Asset losses	The level of asset-related losses that occurred in the Incident, including lost or damaged assets, stolen funds, cash outlays, etc	**Source: impact rating vocabulary STIX 1.1.1** None, Minor, Moderate, Major, Unknown
Business-mission disruption	The level of business or mission disruption impact that occurred in the Incident including unproductive man-hours, lost revenue from system downtime, etc.	**Source: impact rating vocabulary STIX 1.1.1** None, Minor, Moderate, Major, Unknown
Response and Recovery Cost	The level of response and recovery related costs that occurred in the Incident including cost of response, investigation, remediation, restoration, etc.	**Source: impact rating vocabulary STIX 1.1.1** None, Minor, Moderate, Major, Unknown
Impact Level	The subjective level of impact	**Source: impact qualification vocabulary STIX 1.1.1** Insignificant, Distracting, Painful, Damaging, Catastrophic, Unknown

Table 9: Impact assessment facet fields

Indicator of Compromise

Record the indicators of compromise.

Field	Description	Value type
Name	The name of the IOC	Text
Description	Description of the IOC	Text
IOC Type	The type of the IOC	**Source: Indicator Type Vocabulary STIX 1.1.1** Malicious E-mail, IP Watchlist, File Hash Watchlist, Domain Watchlist, URL Watchlist, Malware Artifacts, C2, Anonymization, Exfiltration, Host Characteristics, Compromised PKI Certificate, Login Name, IMEI Watchlist, IMSI Watchlist **Source: Indicator Label STIX 2.0** Anomalous-activity, Anonymization, Benign, Compromised, Malicious-activity, Attribution

Table 10: Indicator of compromise facet fields

Malware

Record malware information.

Field	Description	Value type
Name	Name of the malware	Text
Description	Description of the analysis to be performed	Text
Initial compromise	When was the initial compromise	Datetime
Containment achieved	When was malware containment achieved	Datetime
Restoration achieved	When was full restoration achieved	Datetime
References	References to information for this malware	Text
Removal actions	Course of action, mitigation steps	Text
Characteristics	The characteristics attributed to the malware under analysis	**Source: Malware Type Vocabulary STIX 1.1.1** Automated Transfer Scripts, Adware, Dialer, Bot, Bot - Credential Theft, Bot - DDoS, Bot - Loader, Bot - Spam, DoS / DDoS, DoS / DDoS - Participatory, DoS / DDoS - Script, DoS / DDoS - Stress Test Tools, Exploit Kits, POS / ATM Malware, Ransomware, Remote Access Trojan, Rogue Antivirus, Rootkit **Source: Malware Label STIX 2.0** Adware, Backdoor, Bot, ddos, Dropper, Exploit-kit, Keylogger, Ransomware, Remote-access-trojan, Resource-exploitation, Rogue-security-software, Rootkit, Screen-capture, Spyware, Trojan, Virus, Worm **Source: Malware Labels MAEC** adware, appender, backdoor, boot-sector-virus, bot, cavity-filler, clicker, companion-virus, data-diddler, ddos, downloader, dropper, exploit-kit, file-infector-virus, file-less, fork-bomb, greyware, implant, keylogger, kleptographic-worm, macro-virus, malware-as-a-service, mass-mailer, metamorphic-virus, mid-infector, mobile-code, multipartite-virus, parental-control, password-stealer, polymorphic-virus, premium-dialer-smser, prepender, ransomware, remote-access-trojan, resource-exploiter, rogue-security-software, rootkit, scareware, screen-capture, security-assessment-tool, shellcode, spyware, trackware, trojan, virus, web-bug, worm

Table 11: Malware facet fields

Malware Analysis

Record results of malware analysis.

Field	Description	Value type
Name	Name of the malware	Text
Description	Description of the analysis to be performed	Text
Analysis Results	The detailed results of the analysis	Text

Field	Description	Value type
Initial compromise	When was the initial compromise	Datetime
Containment achieved	When was malware containment achieved	Datetime
Restoration achieved	When was full restoration achieved	Datetime
References	References to information for this malware	Text
Removal actions	Course of action, mitigation steps	Text
Type of Analysis	The type of analysis to be performed	**Source: Analysis types MAEC** static, dynamic, combination
Characteristics	The characteristics attributed to the malware under analysis	**Source: Malware Type Vocabulary STIX 1.1.1** Automated Transfer Scripts, Adware, Dialer, Bot, Bot - Credential Theft, Bot - DDoS, Bot - Loader, Bot - Spam, DoS / DDoS, DoS / DDoS - Participatory, DoS / DDoS - Script, DoS / DDoS - Stress Test Tools, Exploit Kits, POS / ATM Malware, Ransomware, Remote Access Trojan, Rogue Antivirus, Rootkit **Source: Malware Label STIX 2.0** Adware, Backdoor, Bot, ddos, Dropper, Exploit-kit, Keylogger, Ransomware, Remote-access-trojan, Resource-exploitation, Rogue-security-software, Rootkit, Screen-capture, Spyware, Trojan, Virus, Worm **Source: Malware Labels MAEC** adware, appender, backdoor, boot-sector-virus, bot, cavity-filler, clicker, companion-virus, data-diddler, ddos, downloader, dropper, exploit-kit, file-infector-virus, file-less, fork-bomb, greyware, implant, keylogger, kleptographic-worm, macro-virus, malware-as-a-service, mass-mailer, metamorphic-virus, mid-infector, mobile-code, multipartite-virus, parental-control, password-stealer, polymorphic-virus, premium-dialer-smser, prepender, ransomware, remote-access-trojan, resource-exploiter, rogue-security-software, rootkit, scareware, screen-capture, security-assessment-tool, shellcode, spyware, trackware, trojan, virus, web-bug, worm
Behaviours	The behaviours attributed to the malware under analysis	**Source: Behaviors MAEC** access-premium-service, autonomous-remote-infection, block-security-websites, capture-camera-input, capture-file-system-data, capture-gps-data, capture-keyboard-input, capture-microphone-input, capture-mouse-input, capture-printer-output, capture-system-memory, capture-system-network-traffic, capture-system-screenshot, capture-touchscreen-input, check-for-payload, check-language, click-fraud, compare-host-fingerprints, compromise-remote-machine, control-local-machine-via-remote-command, control-malware-via-remote-command, crack-passwords, defeat-call-graph-generation, defeat-emulator, defeat-flow-oriented-disassembler, defeat-linear-disassembler, degrade-security-program, denial-of-service, destroy-hardware, detect-debugging, detect-emulator, detect-installed-analysis-tools, detect-installed-av-tools, detect-sandbox-environment, detect-vm-environment, determine-host-ip-address, disable-access-rights-checking, disable-firewall,

Field	Description	Value type
		disable-kernel-patch-protection, disable-os-security-alerts, disable-privilege-limiting, disable-service-pack-patch-installation, disable-system-file-overwrite-protection, disable-update-services-daemons, disable-user-account-control, drop-retrieve-debug-log-file, elevate-privilege, encrypt-data, encrypt-files, encrypt-self, erase-data, evade-static-heuristic, execute-before-external-to-kernel-hypervisor, execute-non-main-cpu-code, execute-stealthy-code, exfiltrate-data-via-covert channel, exfiltrate-data-via- -dumpster-dive, exfiltrate-data-via-fax, exfiltrate-data-via-network, exfiltrate-data-via-physical-media, exfiltrate-data-via-voip-phone, feed-misinformation-during-physical-memory-acquisition, file-system-instantiation, fingerprint-host, generate-c2-domain-names, hide-arbitrary-virtual-memory, hide-data-in-other-formats, hide-file-system-artifacts, hide-kernel-modules, hide-network-traffic, hide-open-network-ports, hide-processes, hide-registry-artifacts, hide-services, hide-threads, hide-userspace-libraries, identify-file, identify-os, identify-target-machines, impersonate-user, install-backdoor, install-legitimate-software, install-secondary-malware, install-secondary-module, intercept-manipulate-network-traffic, inventory-security-products, inventory-system-applications, inventory-victims, limit-application-type-version, log-activity, manipulate-file-system-data, map-local-network, mine-for-cryptocurrency, modify-file, modify-security-software-configuration, move-data-to-staging-server, obfuscate-artifact-properties, overload-sandbox, package-data, persist-after-hardware-changes, persist-after-os-changes, persist-after-system-reboot, prevent-api-unhooking, prevent-concurrent-execution, prevent-debugging, prevent-file-access, prevent-file-deletion, prevent-memory-access, prevent-native-api-hooking, prevent-physical-memory-acquisition, prevent-registry-access, prevent-registry-deletion, prevent-security-software- -from-executing, re-instantiate-self, remove-self, remove-sms-warning-messages, remove-system-artifacts, request-email-address-list, request-email-template, search-for-remote-machines, send-beacon, send-email-message, send-system-information, social-engineering-based-remote-infection, steal-browser-cache, steal-browser-cookies, steal-browser-history, steal-contact-list-data, steal-cryptocurrency-data, steal-database-content, steal-dialed-phone-numbers, steal-digital-certificates, steal-documents, steal-email-data, steal-images, steal-password-hashes, steal-pki-key, steal-referrer-urls, steal-serial-numbers, steal-sms-database, steal-web-network-credential, stop-execution-of-security-software, suicide-exit, test-for-firewall, test-for-internet-connectivity, test-for-network-drives, test-for-proxy, test-smtp-connection, update-configuration, validate-data, write-code-into-file **Source: Common Attributes MAEC** applicable-platform, archive-type, autonomy, backdoor-type, cryptocurrency-type, encryption-algorithm, erasure-scope,file-infection-type, file-

Field	Description	Value type
		modification-type, file-type, frequency, infection-targeting, network-protocol, port-number, persistence-scope, propagation-scope, targeted-application, targeted-file-architecture type, targeted-file-type, targeted-program, targeted-sandbox, targeted-vm, targeted-website, technique, trigger-type, user-privilege-escalation type, vulnerability-id-cve, vulnerability-id-osvdb

Table 12: Malware analysis facet field

Policy Violation

Record violated policies.

Field	Description	Value type
Description	Description of the policy violation	Text
First Occurrence	When did the policy violation first occur	Datetime
User ID	The user identification number recorded as part of the policy violation	Text
Username	The username recorded as part of the policy violation	Text
User contact information	The user contact information	Text
Response actions	Description of the actions taken	Text

Table 13: Policy violation facet fields

Point of Contact

Record point of Contact details.

Field	Description	Value type
Type	Type of the PoC	Issue Reporter, Point of Contact
Name	The (full) name of the PoC	Text
Contact information	The PoC contact information	Text
Role Description	A description of the role of the PoC	Text
Organisation name	The name of the organization of the PoC (if applicable)	Text

Table 14: Point of contact facet fields

4.1.4 Shared workflow

A ticket for coordination and collaboration is governed by a shared workflow as shown in Figure 7. The ticket workflow is simple to ensure cross-boundary applicability to multiple organisations. The originating organization is in control of the workflow state for the coordination ticket.

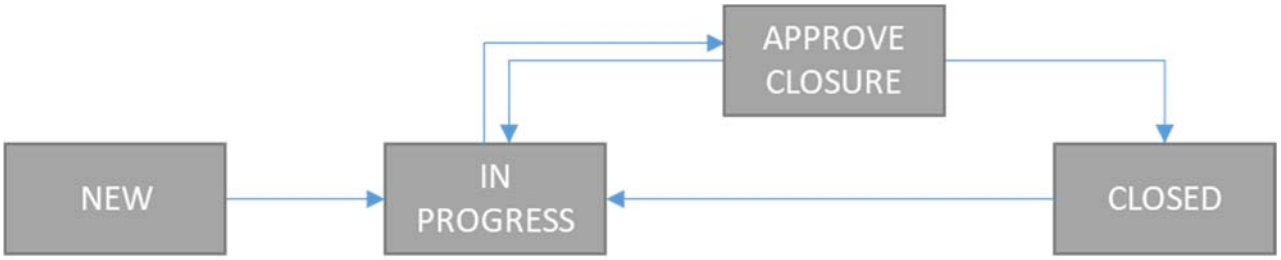

Figure 7 Shared ticket workflow

A coordination ticket starts in the NEW state. In this state the ticket is being prepared in advance of sharing. Once a coordination ticket is moved to the IN-PROGRESS state the ticket is shared with the selected partners. While in this state the sharing partners collaborate on the ticket handling. Once the ticket has been handled it is moved to the APPROVE CLOSURE state. In this state the shared ticket is inspected by the originating organisation to ensure compliancy and that it is ready to be closed. At this stage the ticket might be set back to IN PROGRESS or moved on to the CLOSED state.

A shared ticket that is CLOSED is in a read-only state. The originating organisation can reopen the ticket by setting it back IN PROGRESS if required.

4.2 Health information sharing

In 2019, millions of people are collecting and real-time monitoring remotely their vital signs, such as blood pressure and respiratory rate, or other physiological data such as the posture and gait, the skeletal muscle movement (electromyogram or electromyography, EMG), temperature, sleeping, and brain activity (electroencephalograms, EEG), skin hydration, blood oxygen level, medication ingestion, eye moving tracking (electrooculogram, EOG), on everyday devices like smartwatches and iPhones. These physiological signals from smart wearable sensors are collected, stored, and analysed with smartphone and cloud computing for the further applications to the disease management and healthcare.

The pipeline of collection of physiological data from wearable sensors and mining these data for healthcare wisdoms is scratched in Figure 8.

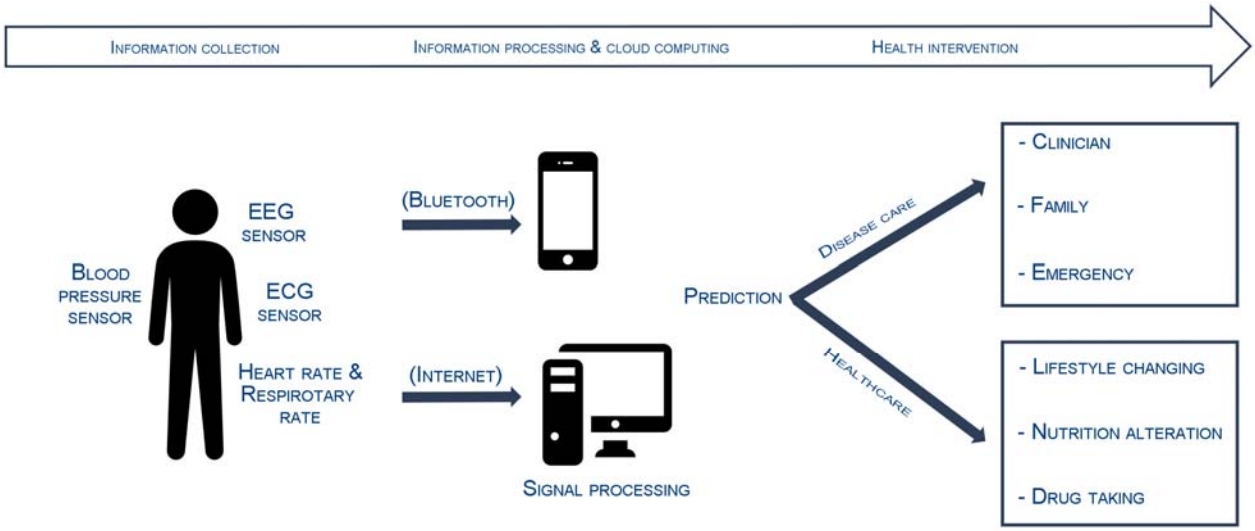

Figure 8: The pipeline of physiological data collection to healthcare wisdoms

In the new era, an increasing number of patients are going online to access information about their health and talk to other patients with a shared condition. Many patients share advice and details about their treatments and symptoms with one another as well as researchers. Clinical trial researchers increasingly use the Internet for recruiting subjects, communicating with participants, and even collecting data. [48]

4.2.1 Health Information Exchange (HIE)

Health Information Exchange (HIE) refers to the electronic transmission of health care data among facilities and professionals within a particular community, area, or hospital. In other words, HIE is the ability to appropriately access and securely share patients' health information between different HealthCare Organizations (HCOs) according to national standards. It involves healthcare and government institutions, health information organizations, and qualified health care providers. The purpose of HIE development is to improve healthcare delivery by offering reliable and secure ways to access and retrieve health information among diverse systems. It is an inherent part of the health information technology infrastructure as it aims to improve data gathering and medical care.

While nowadays most medical information is still gathered through written records and is stored in paper form, HIE managed to develop three main methods to innovate current healthcare procedures. These methods are defined as: consumer-mediated exchange, directed exchange, and query-based exchange:

- Consumer-mediated exchange is done by providing patients with access to their own electronic records, thus allowing them to track their health conditions, determine whether there is erroneous billing or medical data, and update their self-reports;
- Directed exchange is conducted when a healthcare organization transfers such vital information as lab test results and medication dosage to other specialists involved in the care of the same patient;
- Query-based exchange usually occurs in unplanned medical care when a healthcare organization needs the previous health records of a new patient. This is done by requesting access to these records through the HIE system.

A patient's medical records should follow him or her wherever and whenever needed, despite barriers that may occur due to the involvement of multiple facilities in different geographic areas. Thus, current HIE governance should be done through effective collaboration between entities while considering implementation costs. Unfortunately, not all facilities are able to afford electronic exchange, and this is why this issue should be further addressed by both reducing the overall cost of HIE and searching for substantial financial support for the development of the system. Furthermore, governance policies and models should be introduced and constantly updated to efficiently manage the system and solve arising issues. Finally, since health-related information is too private to be retrieved by non-professionals, HIE relies on secure data transfer among various electronic systems. This is why HIE should be done with regards to privacy policies, strictly limiting the access to patients' records in order to prevent any outsider from gaining unauthorized access to the system. The information should be exchanged among entities without leaking out of the system, which may occur because of the faults of the system itself or liability issues.

Governance

Governance in the context of Health Information Exchange (HIE) refers to the establishment and oversight of a common set of behaviours, policies, and standards that enable trusted, electronic HIE among a set of participants. Before data can be shared, the parties involved must establish a governing body with a set of broad and representative stakeholders. The governing body defines what data will be shared, how they will be shared, and under what circumstances they will be shared. The governing body creates a governance framework to ensure compliance with legal, technical, and operational requirements related to the protection, use, and disclosure of Protected Health Information (PHI). Data sharing agreements codify the policies and procedures established by the governing body. These elements are essential for competing health care organizations to agree to share data. As outlined in Figure 9, a governance framework begins with the

formation of a governing body, which creates policies and procedures and establishes a series of data sharing agreements.

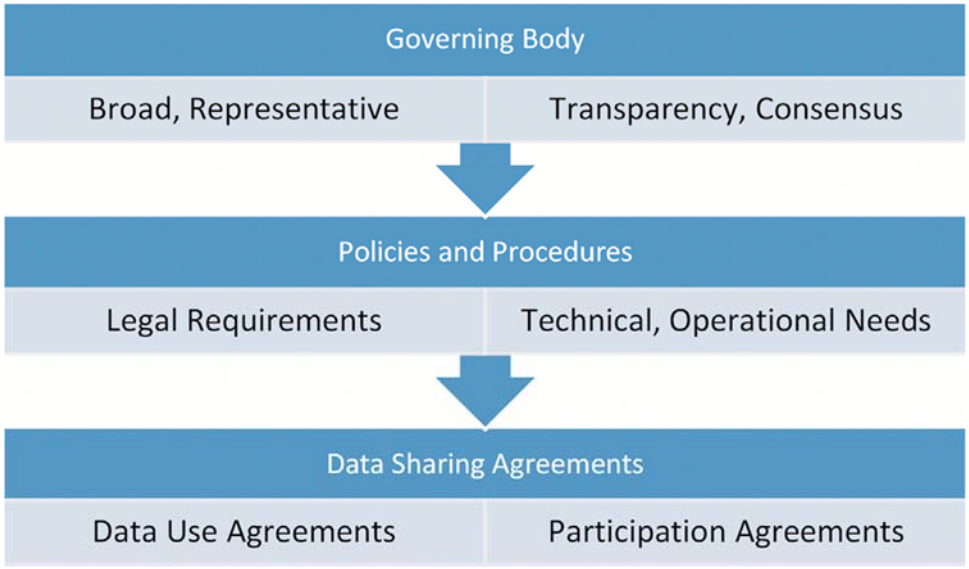

Figure 9: A governance framework for Health Information Exchange

As the volume and type of data exchanged expands, the importance of governance grows. The governance framework must be able to scale, sustain, and respond over time. A governance framework requires active engagement with participating organizations to establish transparency and achieve consensus. Governance is important for all types of Health Information Organizations (HIOs), but it is more critical as membership diversity, approved use cases, and the geographic footprint of the HIO expands. [49]

Data sharing agreements must be specific enough to constrain the use of shared data to specific use cases. However, such agreements also need to be flexible enough to incorporate new use cases as they are approved or modified. Creating these agreements is not easy in the early stages of establishing HIE. For this reason, formal governance may be deferred as the exchange develops and the use cases are being defined and approved. As policies are developed and procedures are defined, formal governance processes should also develop. Formal contracting agreements provide the necessary controls and protections for all participating stakeholders.

Governance describes how data are handled, shared, used, and secured. It creates a mechanism for monitoring compliance with the policies and procedures of the exchange. The HIO must be trusted to provide information to improve the safety, efficiency, and effectiveness of patient care. For this reason, trust agreements are critical to successful governance programs.

HIOs create a set of contractual documents, referred to as trust agreements because they engender trust amongst the parties involved in the agreements. Trust agreements include documents such as Data Use Agreements and Participation Agreements.

Data security

Healthcare organizations store, maintain and transmit huge amounts of data to support the delivery of efficient and proper care. Nevertheless, securing these data has been a daunting requirement for decades. Complicating matters, the healthcare industry continues to be one of the most susceptible to publicly disclosed data breaches. In fact, attackers can use data mining methods and procedures to find out sensitive data and release it to public and thus data breach happens. While implementing security measures remains a complex process, the stakes are continually raised as the ways to defeat security controls become more sophisticated.

As a result, it is crucial that organizations implement healthcare data security solutions that will protect important assets while also satisfying healthcare compliance mandates.

Various technologies are in use for protecting the security and privacy of healthcare data. Most widely used technologies are [50]:

1. **Authentication**: Authentication is the act of establishing or confirming claims made by or about the subject are true and authentic. It serves a vital function within any organization: securing access to corporate networks, protecting the identities of users, and ensuring that a user is who he claims to be. Most cryptographic protocols include some form of endpoint authentication specifically to prevent man-in-the-middle (MITM) attacks. For instance, Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. Several versions of the protocols are in widespread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voice- over-IP (VoIP). One can use SSL or TLS to authenticate the server using a mutually trusted certification authority. Additionally, Bull Eye algorithm can be used for monitoring all sensitive information in 360°. This algorithm has been used to make sure data security and manage relations between original data and replicated data. It is also allowed only authorized person to read or write critical data. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at the entry of every access.
2. **Encryption**: Data encryption is an efficient means of preventing unauthorized access of sensitive data. Its solutions protect and maintain ownership of data throughout its lifecycle, from the data center to the endpoint (including mobile devices used by physicians, clinicians, and administrators) and into the cloud. Encryption is useful to avoid exposure to breaches such as packet sniffing and theft of storage devices. Healthcare organizations or providers must ensure that encryption scheme is efficient, easy to use by both patients and healthcare professionals, and easily extensible to include new electronic health records. Furthermore, the number of keys hold by each party should be minimized. Although various encryption algorithms have been developed and deployed relatively well (RSA, Rijndael, AES and RC6, DES, 3DES, RC4, IDEA, Blowfish ...), the proper selection of suitable encryption algorithms to enforce secure storage remains a difficult problem.
3. **Data Masking**: Masking replaces sensitive data elements with an unidentifiable value, but is not truly an encryption technique so the original value cannot be returned from the masked value. It uses a strategy of de-identifying the data sets or masking personal identifiers such as name, social security number and suppressing or generalizing quasi identifiers like data-of-birth and zip-codes. Thus, data masking is one of the most popular approach to live data anonymization. K-anonymity first proposed by Swaney and Samrati protects against identity disclosure but failed to protect against attribute disclosure. Truta et al. have presented p-sensitive anonymity that protects against both identity and attribute disclosure. Other anonymization methods fall into the classes of adding noise to the data, swapping cells within columns and replacing groups of k records with k copies of a single representative. These methods have a common problem of difficulty in anonymizing high dimensional data sets. A significant benefit of this technique is that the cost of securing a big data deployment is reduced. As secure data is migrated from a secure source into the platform, masking reduces the need for applying additional security controls on that data while it resides in the platform.
4. **Access Control**: Once authenticated, the users can enter an information system but their access will still be governed by an access control policy which is typically based on the privilege and right of each practitioner authorized by patient or a trusted third party. It is then, a powerful and flexible mechanism to grant permissions for users. It provides sophisticated authorization controls to ensure that users can perform only the activities for which they have permissions, such as data access, job submission, cluster administration, etc. A number of solutions have been proposed to address the security and access control concerns. Role-Based Access Control (RBAC) and Attribute-Based Access Control

(ABAC) are the most popular models for EHR. RBAC and ABAC have shown some limitations when they are used alone in medical system.

Data privacy

Recent years have seen the emergence of advanced persistent threats, targeted attacks against information systems, whose main purpose is to smuggle recoverable data by the attacker. Therefore, invasion of patient privacy is considered as a growing concern in the domain of big data analytics, which make organizations in challenge to address these different complementary and critical problems. In fact, data security governs access to data throughout the data lifecycle while data privacy sets this access based on privacy policies and laws which determine, for example, who can view personal data, financial, medical or confidential information. An incident reported in the Forbes magazine raises an alarm over patient privacy. In the report, it mentioned that Target Corporation sent baby care coupons to a teen-age girl unbeknown to her parents. This incident impels big data to consider privacy for analytics and developers should be able to verify that their applications conform to privacy agreements and that sensitive information is kept private regardless of changes in the applications and/or privacy regulations. Privacy of medical data is then an important factor which must be seriously considered.

More than ever it is crucial that healthcare organisations manage and safeguard personal information and address their risks and legal responsibilities in relation to processing personal data, to address the growing thicket of applicable data protection legislation. Different countries have different policies and laws for data privacy. Data protection regulations and laws in some of the countries along with salient features are listed in the Table 15.

Country / Union	Law	Salient Features
U.S.A	HIPAA Act, Patient Safety and Quality Improvement Act (PSQIA) and HITECH Act	The HIPAA privacy rule declares a set of standards, which describe how healthcare providers keep, store, protect, and share patients' health information. The HIPAA security rule defines security standards to protect the privacy of individuals' electronic Protected Health Information (e-PHI). It specifically mentions the requirements of ensuring the confidentiality, integrity, and availability of all e-PHI created, received, maintained or transmitted. It also requires the identification and protection of e-PHI against anticipated threats to the security or integrity of the information.
EU	European Data Protection Directive 95/46/EC	Protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data.
Canada	Personal Information Protection and Electronic Documents Act ('PIPEDA')	Individual is given the right to know the reasons for collection or use of personal information, so that organizations are required to protect this information in a reasonable and secure way.
UK	European Data Protection Directive 95/46/EC, Data Protection Act (DPA)	After Brexit, UK will be considered as a so called secure third country, under the scope of GDPR. DPA provides a way for individuals to control information about themselves. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.
Russia	Russian Federal Law on Personal Data	Requires data operators to take "all the necessary organizational and technical measures required for protecting personal data against unlawful or accidental access".

Table 15: Data protection laws in some of the countries

Differentiation between security and privacy

Security and privacy in big data are important issues. Privacy is often defined as having the ability to protect sensitive information about personally identifiable health care information. It focuses on the use and governance of individual's personal data like making policies and establishing authorization requirements to ensure that patients' personal information is being collected, shared and utilized in right ways. While security is typically defined as the protection against unauthorized access, with some including explicit mention of integrity and availability. It focuses on protecting data from pernicious attacks and stealing data for profit. Although security is vital for protecting data but it's insufficient for addressing privacy. Table 16 focuses on additional difference between security and privacy [50].

Security	Privacy
Security is the "confidentiality, integrity and availability" of data	Privacy is the appropriate use of user's information
Various techniques like Encryption, Firewall, etc. are used in order to prevent data compromise from technology or vulnerabilities in the network of an organization	The organization can't sell its patient/user's information to a third party without prior consent of the user
It may provide for confidentiality or protect an enterprise or agency	It concerns with patient's right to safeguard their information from any other parties
Security offers the ability to be confident that decisions are respected	Privacy is the ability to decide what information of an individual goes and where to

Table 16: Differentiation between security and privacy

EHR standards

Standards in representing EHRs are important in that they provide a common language and a set of anticipations to enable interoperability among systems and devices. The standards for EHRs are aimed at increased coordination of care. There are groups formed to harmonize the challenges faced by shared Electronic Health Record systems. The groups include: HL7 (Health Level Seven International), which is responsible for developing a standard for the clinical document architecture and templates, openEHR, which deals with the technical activities like architecture, implementation projects, and clinical activities like archetypes, standard activities, and CEN (a standardization committee for Europe dealing with EHR communication standards). The following standards derived from the above groups should be observed when presenting Electronic Health Record systems:

1. EHRs should have the ability to generate, send, obtain and present standardized evolution of care documents.
2. EHRs should have the ability to offer electronic prescription, reconciliation between patients' past and present medical information, incorporation of laboratory test outcomes, and creation of patients' care summaries.
3. EHRs should be capable of working with standardized documents, which is referred to as interoperability.
4. EHRs must have the ability to use the consolidated clinical document architecture (CCDA) for the transfer of care documents summaries.

HIE architectures

Since the role of HIE is to provide care facilities with the ability to circulate EHRs among varied medical information systems, HIE systems can have centralized, federated or patient-controlled architectures.

The centralized HIE system, also referred to as the consolidated model, involves storing all health information in a single data repository or warehouse (e.g., cloud). Each member of the centralized HIE system (hospitals, clinics, and other health care stakeholders) is expected to transmit patients' health information to the remote repository, where the information is securely stored. The health information is continuously updated through interfaces connected directly to each healthcare organization's information repository in order to improve security and confidentiality. These interfaces usually allow for unaltered patient information flow to the central authority. Whenever a member organization requests access, it is subjected to pre-defined unique patient identifiers before being authorized.

The federated structure requires local patient information storage at each healthcare organization to ensure a higher level of data security and privacy. Data are captured and maintained separately within disparate hospital, clinic, and other data repositories then queried on demand when they are needed for individual care or a population level analysis. To access the information the entity must be a member of an association, and at the same time, must commit itself to sharing the information with other members of the network. The participants in this model are often held responsible for ensuring that information is accessed by the authorized members only. In other words, when a health system interconnects its affiliates, we refer to this as Federated HIE because the exchange is only within the membership group. For example, the U.S. Department of Veterans Affairs (VA) operates 153 medical centers as well as 909 ambulatory care and community-based outpatient clinics across the United States and its territories. In the early 2000s, the VA interconnected its facilities using a software program referred to as VistaWeb. [51]

In contrast to the centralized and federated models of HIE, in which the principal design is HIE between providers and other health system stakeholders, patient-controlled or "consumer-mediated" forms of HIE have been proposed. In patient-controlled forms of HIE, health care consumers are responsible for either (1) depositing their health records into consumer-controlled data repositories referred to as "health record banks" or (2) downloading their medical records onto secure disk drives or "smart cards" that can be carried with them as they traverse the health system. While these approaches have an advantage of being patient-centered meaning patients would be in control of their data, critics argue that such models face a number of challenges including cost, sustainability, and scalability similar to other HIE approaches. [49]

ICT systems

HIE, according to what Dixon, Brian E. said in [49], necessitates electronic transfer between ICT systems. Therefore, ICT systems need technical methods for facilitating exchange of information. In ICT speak, there must be a sender and a receiver. For example, a laboratory information system (LIS) sends lab test results to an EHR system to record the results in a patient's records. Yet a LIS can also receive an order to perform a lab test from an EHR system. These electronic transactions provide the technical foundation for HIE. Almost any ICT system in health care can be either a sender or a receiver depending on the scenario. Therefore, the potential configuration of technical networks involving ICT is many. Regardless of which ICT systems are involved in HIE or the direction in which information flows, there will be senders and receivers. [49]

Transactions or messages

Electronic transactions in health care can be conceived of as messages between two people or organizations. In the physical world, messages take the form of envelopes and packages. Envelopes and packages come in all shapes, sizes, and weights. So do electronic transactions. For example, electronically transmitting information that a particular patient has arrived at the clinic and is waiting to see the doctor is akin to putting a single, small piece of paper into a small envelope. Exchanging a discharge summary is like sending a multiple page document in a large envelope. This transaction requires additional "overhead" or structure so that the receiving ICT system can interpret the information inside the envelope. Still greater requirements are needed for the exchange of an MRI scan which includes large, detailed images. A special envelope would be necessary to protect the image from getting bent or damaged in transit. Similarly, ICT systems would require a specialized, structured message and sufficient storage as well as transport capacity for transferring the MRI

images. Specialized, structured messages are referred to in the HIE world as technical standards. When ICT systems can send and receive messages, we say they can interoperate or possess interoperability. [49]

Content or Payload

Inside of messages are contents such as patient demographics, lab results, images. ICT speak sometimes refers to contents as payloads. While in transit from one ICT system to another, the technologies that facilitate the transport do not care about the contents inside the message. However, for the information exchanged to be stored and used by the receiving ICT system (as well as the system's users—humans), ICT systems need methods for understanding the message contents. In HIE we refer to these methods as data standards, which we say create semantic interoperability between ICT systems. [49]

4.2.2 What kind of data could be detected by the wearable sensors?

The Traditional Methods for Physiological Data - Collection and Analyses

Human health states are always associated with some basic physiological indices such as body temperature, blood pressure, heart rate, pulse, respiratory rate, ECG, EEG, EOG, EMG, etc. Traditionally, these data are often checked and collected periodically when the patients visit hospitals. Special conditions and devices are often needed. The collection of the dynamic physiological data is often time-consuming, labor-intensive, and costly. The analyses of these data are often statistically averaged to identify the patterns at the population level, as described in Figure 10.

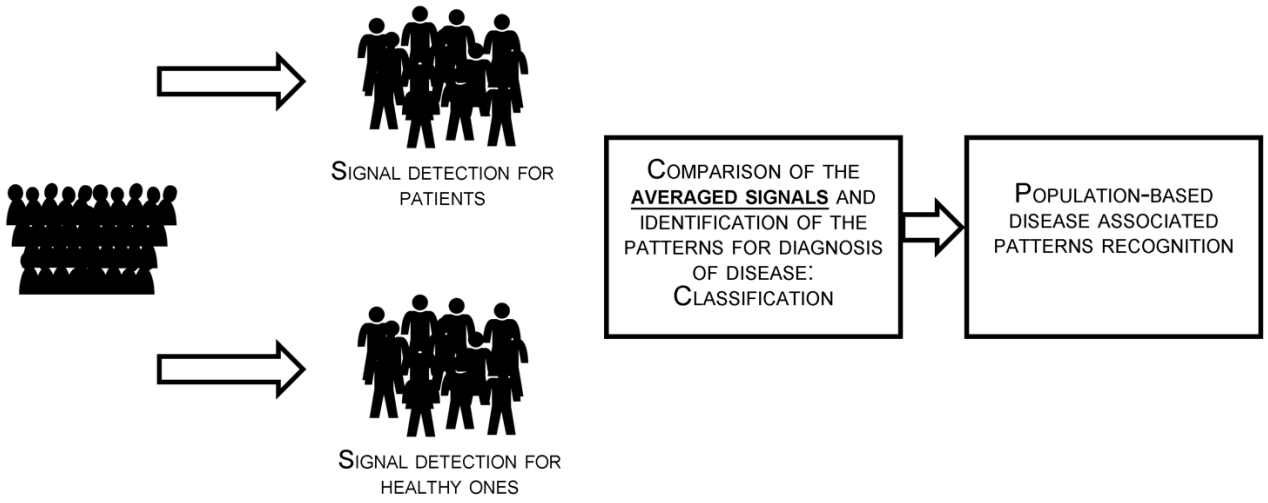

Figure 10: Cohort data collection and statistical analysis to identify healthcare-associated factors

The advantage of this traditional method is that it can identify general physiological patterns at population level and it could provide facts, evidence, and reference for the policy making and disease screening. But it will be not precise when applied to individuals since the averaged indices are not personalized. [48]

The Longitudinal Self-Measurements Wearable - Sensors and the Smartphone-Based Cloud Computing for Data Storage, Extraction, and Analysis

In the past two decades, the popularization of wearable sensors and smartphone is changing of our life rapidly. The whole-body monitoring by wearable sensors is becoming more and more practical. We nowadays have

the potential to monitor the whole body's physiological signals for disease prevention from head to foot. In the head part, we can use wearable sensors to detect the brain activity by electroencephalograms (EEG) for monitoring of epilepsy, fatigue, mental stress, anxiety states, etc. The eye's movement could be measured with electrooculogram (EOG) to monitor older adults and patients with Parkinson's disease. The facial expression could be detected for emotional recognition; the gait and balance and the fall risk could be detected to monitor the foot part. The other detectable physiological signals of the human body include the electrocardiogram (ECG) for the heart rhythm, electromyogram (EMG) for skeletal muscle movement, etc. All these physiological signals could be detected and applied to the monitoring of a wide spectrum of diseases.

Comparing to the traditional methods, the wearable sensors are cheap and convenient. It could be applied to both patients and health individuals, and the data could be collected in real time, dynamic, and personalized as shown in Figure 11. The volume of these physiological data will be accumulated very fast. With different sensors, we will have diverse data formats, and the velocity of the data generating will be also high. So, the physiological data from the wearable sensors possess distinct characterization of big data. All the tools and methods for big data management therefore could be applied here for the big physiological data storage, extraction, and analysis.

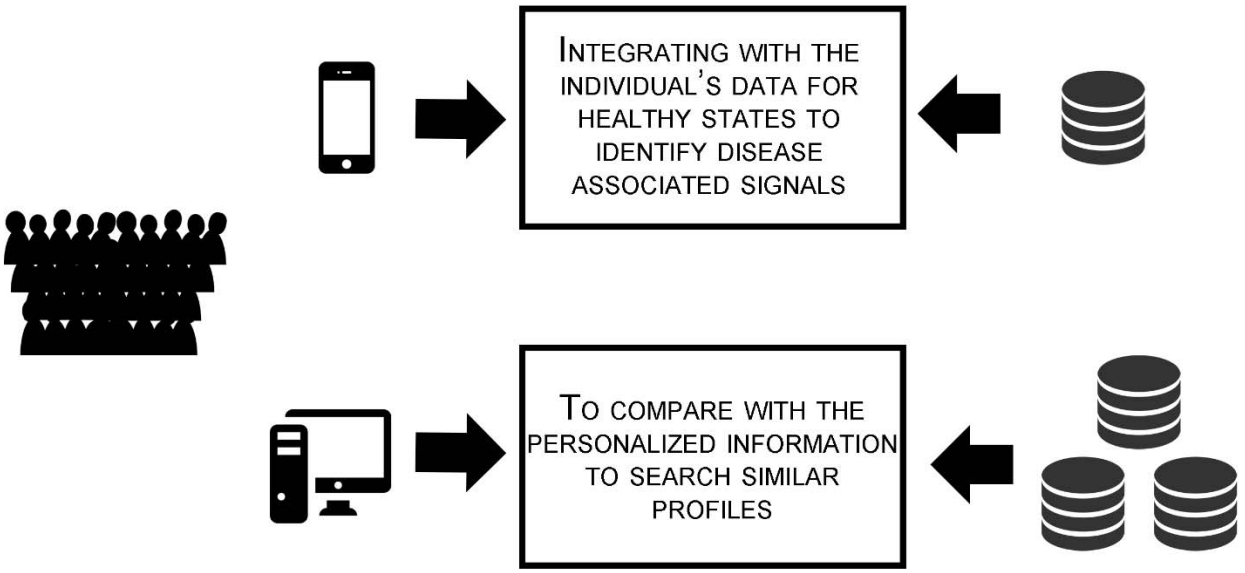

Figure 11: Real-time and personalized analyses of longitudinal measurements by wearable sensors

Thanks to the cloud computing technologies, the big physiological data could be stored, extracted, or even get analysed results from the cloud with smartphone linked to the internet. The cloud computing providers can offer a user different service including software tools (SaaS), platforms (PaaS), and infrastructure (IaaS). As displayed in Figure 11, the detected personalized data could be collected, accumulated, and stored in cloud databases as reference data. A personalized physiological data could be compared to the reference data to find similar profiles and then screen better treatment strategies. The individual's previous health data or disease data could also be applied to the diagnosis and treatment of complex diseases. This smartphone-based cloud service was reported to be used to manage type 1 diabetes (T1D) and chronic obstructive pulmonary disease (COPD) patients with comorbidities. [48]

4.2.3 How to share and analyse the detected physiological profiles?

Data Standardization and the Privacy of Personal Physiological Information

Data standardization is important to the exchange and sharing of big data between researchers, companies, organizations, and other data users. The physiological data could be generated from different resources with various structures, formats, or terminologies. Ontology-based standardization is the first step to make these diverse data sharable and reusable as Figure 12 illustrates.

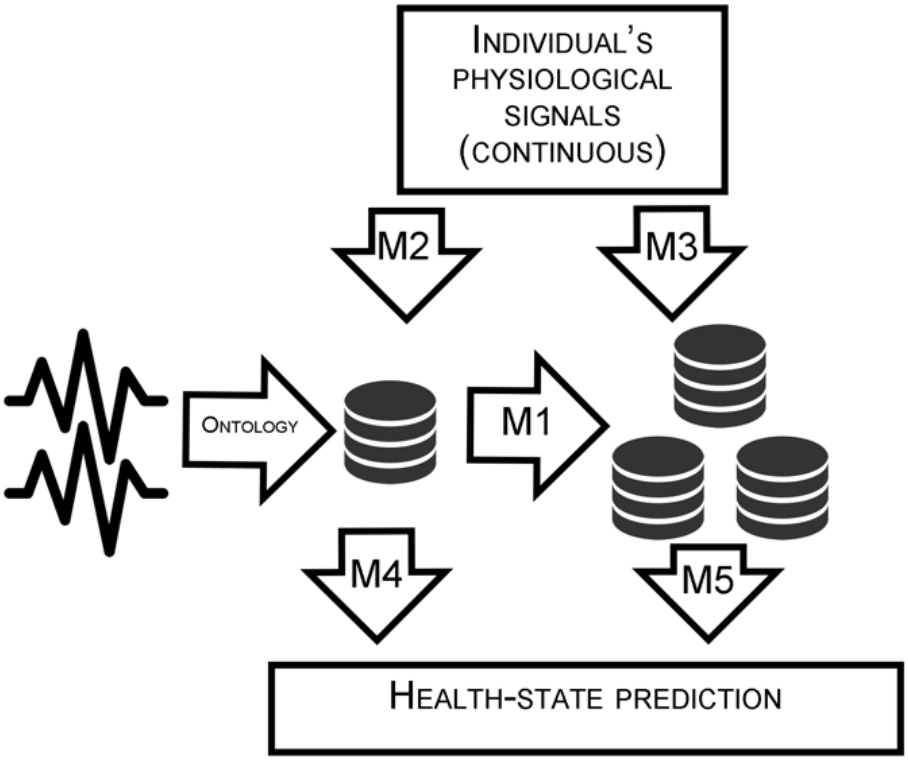

Figure 12: Models for mining physiological data

Ontology is a knowledge framework with a controlled vocabulary and defined relationship between them to be used in a subject or a domain for identification of themes and patterns in a given data set. At present, several ontologies are developed and applied to physiological data and can be extended to the storage and analyses of the data collected from different wearable sensors. Some of the developed ontologies for the standardization of physiological data are listed in Table 17. More ontologies are still needed for the diversity of physiological data from smart wearable sensors, including the basic and high-level physiological information like the pulse, the blood pressure, and the dynamic patterns of the personalized signals. The ontologies will not be only useful for the data sharing as they could be very powerful tools for the annotation and explanation of the data and the ontological functional analysis, then enabling and accelerating the researches.

Ontologies	Description and availability	References
Ion Channel ElectroPhysiology Ontology (ICEPO)	Ontological representation for extracting quantitative information from text http://openbionlp.org/mutd/supplementarydata/ICEPO/ICEPO.owl	Elayavilli RK, Liu H (2016) Ion Channel Electro Physiology Ontology (ICEPO) – a case study of text mining assisted ontology development. AMIA Joint Summits Transl Sci Proc AMIA - Joint Summits Transl Sci 2016:42–51

Ontologies	Description and availability	References
OntoVIP	The annotation of the models used in medical image simulation http://bioportal.bioontology.org/ontologies/OntoVIP	Gibaud B, Forestier G, Benoit-Cattin H, Cervenansky F, Clarysse P, Friboulet D, Gaignard A, Hugonnard P, Lartizien C, Liebgott H et al (2014) OntoVIP: an ontology for the annotation of object models used for medical image simulation. J Biomed Inform 52:279–292 Cook DL, Neal ML, Bookstein FL, Gennari JH (2013) Ontology of physics for biology: representing physical dependencies as a basis for biological processes. J Biomed Semant 4 (1):41
Ontology of Physics for Biology (OPB)	The representations of the thermodynamics and dynamics of physiological processes http://bioportal.bioontology.org/ontologies/OPB	Cook DL, Neal ML, Bookstein FL, Gennari JH (2013) Ontology of physics for biology: representing physical dependencies as a basis for biological processes. J Biomed Semant 4 (1):41
Epilepsy and Seizure Ontology (EpSO)	A suite of informatics tools for representation and study of epilepsy http://prism.case.edu/prism/index.php/EpilepsyOntology	Sahoo SS, Lhatoo SD, Gupta DK, Cui L, Zhao M, Jayapandian C, Bozorgi A, Zhang GQ (2014) Epilepsy and seizure ontology: towards an epilepsy informatics infrastructure for clinical research and patient care. J Am Med Inform Assoc AMIA 21(1):82–89 Gundel M, Younesi E, Malhotra A, Wang J, Li H, Zhang B, de Bono B, Mevissen HT, Hofmann-Apitius M (2013) HuPSON: the human physiology simulation ontology. J Biomed Semant 4(1):35
Human Physiology Simulation Ontology (HuPSON)	A framework for biomedical physiological simulation http://bishop.scai.fraunhofer.de/scaiview/	Gundel M, Younesi E, Malhotra A, Wang J, Li H, Zhang B, de Bono B, Mevissen HT, Hofmann-Apitius M (2013) HuPSON: the human physiology simulation ontology. J Biomed Semant 4(1):35
Cellular Phenotype Ontology (CPO)	Ontology for characterization of cell morphology and physiological phenotypes http://cell-phenotype.googlecode.com	Hoehndorf R, Harris MA, Herre H, Rustici G, Gkoutos GV (2012) Semantic integration of physiology phenotypes with an application to the cellular phenotype ontology. Bioinforma (Oxford, England) 28(13):1783–1789 Tinnakornsrisuphap T, Billo RE (2015) An interoperable system for automated diagnosis of cardiac abnormalities from electrocardiogram data. IEEE J Biomed Health Inform 19 (2):493–500
ECG Ontology	Ontology based on the HL7 standard	Tinnakornsrisuphap T, Billo RE (2015) An interoperable system for automated diagnosis of cardiac abnormalities from electrocardiogram data. IEEE J Biomed Health Inform 19 (2):493–500
Hierarchical Event Descriptors (HED)	Semi-structured tagging for EEG http://sccn.ucsd.edu/eeglab	Bigdely-Shamlo N, Cockfield J, Makeig S, Rognon T, La Valle C, Miyakoshi M, Robbins KA (2016) Hierarchical Event Descriptors (HED): semi-structured tagging for real-world events in large-scale EEG. Front Neuroinform 10:42

Table 17: Ontologies developed and applied in physiological data

For the data sharing, the privacy of the personalized data is another important issue needed to be resolved before the data distributed to public. Several concepts and frameworks are proposed for the privacy preserving of data from wearable sensors. The stringent CIA (confidentiality, integrity, and availability) and Health Insurance Portability and Accountability Act (HIPAA) principles are suggested to follow for the information security. [48]

Databases for the Mining of Physiological Signals

After the data standardization, different databases specific to various physiological data are then needed. In the past, some physiological databases have been built for public accessing. Comparing to the databases at gene level, physiological phenotype databases are still demanded. One of the most comprehensive databases is the PhysioBank database from PhysioNet resource, which includes physiological signals like ECG, interbeat interval, gait and balance, neuroelectric and myoelectric, image, etc. In the PhysioNet webpage, you can also download software tools for viewing and analysing of physiologic signals. Many associated physiological databases are also collected there, including MIT-BIH Arrhythmia, European ST-T, Long-Term ST, MIT-BIH Noise Stress Test, Creighton University Ventricular Tachyarrhythmia, MIT-BIH Atrial Fibrillation, and MIT-BIH Supraventricular Arrhythmia and Normal Sinus Rhythm.

As indicated in Figure 12, one of the big challenges to understand the complex physiological signals for healthcare or disease management is the building of specific data analysis models, such as (1) clustering or classifying individuals' physiological data to distinct groups based on their profile similarities (M1 in Figure 12), (2) comparing an individual's physiological feature to the population samples to identify similar health/disease profiles (M2), (3) classifying the individual's physiological signals from known groups (M3), and (4) optimizing a score function or model to classify a given physiological profile to predict the health state (M4 and M5). [48]

4.3 Maritime information sharing

This case study analyses the information sharing models applied in maritime domain. The main research question is "how can cyber information sharing models be understood in maritime domain?" The complete case study report is in Annex 3.

The EU's Integrated Maritime Policy (IMP) focuses on cross-sector and/or cross-border issues. EU Commission's communication COM(2007) 575 gives outlines for an IMP for enhanced and sharing of information. European Commission's publication "A Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain" gives principles for the EU's Maritime Authorities' cooperation on surveillance and information sharing cross-border and cross-sector [52].

There are seven user communities (or sectors) at EU level, as shown in the following figure.

Figure 13: Seven maritime user communities at the European Union level. (Adopted from [53])

Namely, these user communities (sectors) are: Border Control, Fisheries, Defence, Maritime Safety and security, Marine Environment, Customs and General Law Enforcement (LEA). Integrated Maritime Surveillance (IMS) interlinks user communities and builds a technical framework for integration and the interoperability [54]. The main shareholders of sensitive cyber information sharing in maritime domain and their User Communities' EU wide organisations and their used IT systems are introduced more specifically in Annex 3.

The need and importance for information sharing has been comprehended in maritime domain. With the EU funded projects the common information sharing has been developed from the fundamental idea to the pre operational sharing system within a decade. The latest maritime environment project EUCISE2020 developed an information-sharing environment (CISE) jointly by the European Commission and EU/EEA member states with the support of relevant agencies such as the EFCA. The CISE integrates existing maritime surveillance systems and networks and gives all those authorities concerned access to the information they need for their missions at sea. The CISE makes different systems interoperable so that information can be exchanged easily through the use of modern technologies without any changes to the national legacy systems. Today CISE is a situational awareness information sharing channel for EU maritime authorities in its way to operational use by 2021 but it could be developed to other purposes also. The key word is data model. For ECHO, CISE could be seen as an option for cyber information sharing platform. Technically CISE is information sharing system for maritime information and therefore not a Plug and Play system for ECHO but could be enlarged for cyber information sharing including the critical E-EWS information. The description of CISE testbed is presented in Annex 3.

In the course of BluemassMed, MARSUNO, CoopP and EUCISE2020 projects *the Responsibility to Share* principle has been formulated as the cornerstone vision of maritime information sharing. The rules for the distribution of information in EUCISE2020 is illustrated with the following words: “This principle means that an individual in possession of a piece of information is responsible for disseminating it to anyone that may have a legitimate use for it, and would be accountable if any harm happens as a consequence of the non-distribution” [55].

The maritime domain could not escape the cyber-attack either. The maritime environment could be classified in several different ways pending on in which forum it is discussed. Normally, people assume that navigational systems are the most vulnerable systems in which cyber-attack could cause most serious harm. On the other hand, the information in CISE environment would be useful for cyber criminals while the information is formulated by cross sectorial and cross border authorities. From that perspective, the CISE consortium has to take the cyber threat seriously, and the CISE could be a valuable or potential partner for the ECHO project.

4.4 Situational awareness and cyber information sharing between critical infrastructure organizations

This case study analyses inter-sector cyber information sharing models in critical infrastructure protection in Finland. It studies how the cyber situational awareness of an organization can be developed; how do the organizations exchange their cyber security related information; and how an organization’s cybersecurity capability can be utilised more extensively? The complete case study report is in Annex 4.

4.5 HAVARO: Cyber threat prevention mechanisms in Finland

The aim of this case study is to find out crucial national elements for a common Early-Warning System to EU level. In this context the elements mean functionalities and procedures but also technical solutions concerning cyber information sharing.

Case evidences are based on scientific literatures, interviews of IT specialists, research articles and official documents. This case study will find out the pros and cons of the HAVARO system and what are those factors (requirements), which effect for implementing national EWS system to common early warning ecosystem in EU level. Every EU member country has its own system for monitoring and protecting cyber domain among vital functions. It must be understood that national systems must find common procedural models in the name of the common good. Workable common system requires also common direction to develop a common systemThe research question is: *What are the main features of the cybersecurity information sharing model called HAVARO and how the early warning solution HAVARO and GovHAVARO (for public organizations) can be integrated and implement to the ECHO Early warning system solution?* Also, following sub-questions are

discussed: *How to create connection between existing procedures and new generation system with preventive or (predictive) cyber functions concerning preventive cyber-information sharing? How to combine and share relevant data between stakeholders in national level and in international level? It is important to take into account that private-public, private-private, public-private and public-public features must be included in multidirectional information sharing functions?*

The end result of this case study is only one suggestion for connecting the national HAVARO and a European level EWS system.

4.5.1 HAVARO 1.0

NCSC-FI's HAVARO service has been built for use of organisations as the help of the observation of serious information security threats. From the HAVARO system, the NCSC-FI has visibility to practically all the upcoming and outgoing traffic (metadata and content data). Many critical companies for security of supply and the state administration operators have put to use the HAVARO service, which indicates the trust in the NCSC-FI. That way, the information security breaches targeted at the organisation can be reported automatically to the authority without a chance for censoring the incidents before-hand. The system has been implemented in collaboration with the National Emergency Supply Agency (NESA).

The companies and public administration operators participate in the HAVARO operation voluntarily. The operation of the system is based on the information security threat identifiers coming from different sources. With the help of the identifiers, harmful or anomalous traffic can be detected from the organisation's network traffic. The NCSC-FI receives the information about the anomalies and analyses them. In case of an information security threat, the organisation is warned about it. Based on the information got from the HAVARO, also the other operators can be warned about the detected threat. That way, the system helps not only individual organisations but also in forming a general view about the information security threats against Finnish information networks.

The observation ability of information security threats is an important part of a comprehensive risk management. For its own part, HAVARO secures the organisation's business continuity against the threats of the operational environment. However, HAVARO is not meant to be an organisation's only information security solution, but it is designed to complete the other information security solutions of an information security investing organisation.

In addition, Traficom provides the GovHAVARO service for the state administration operators. It completes the information and cyber security threat detection of the state administration's Internet traffic. The service providers are Traficom, Valtori – Government ICT Centre and Telia. The GovCERT services, in turn, support the state's round-the-clock information security operation by producing the support services for preventing, detecting and investigating information security breaches, as part of the GovSOC operation. They are provided by Traficom and Valtori. [56]

The incident management of the state administration and other public administration organisations, so called VIRT operation, is cross-administrative operational level collaboration, which prepares for severe and extensive information security incidents. It consists of operational planning and rehearsing for different information security incidents. [56]

The industry-specific cyber information sharing groups (ISAC, Information Sharing and Analysis Centre) are established as collaboration organs between the organisations of different industries. Their operation enables

1. Confidential handling of information security matters between the participants.
2. Augmentation of the organisations' information security know-how.
3. Development of the NCSC-FI's overall situation awareness.

The ISAC operation is based on regular meetings and specified operational models and participants. The ISAC information sharing groups have been established for the following industries: state administration (VIRT),

Internet service providers, chemistry and lumber industry, banks, media, energy industry, food production and distribution, social and health care, and software manufacturers.

The main problem about the HAVARO 1.0 concerns the monitoring ability. It mainly monitors information security incidents only in internet traffic as Figure 14 illustrates, and it is incapable of monitoring the communication of the individual user behaviour. In the near future, it is not enough to monitor only internet traffic of companies. There should be wider right to access into the organisations information systems and communication, because Internet of Things is changing our way of understanding artificial intelligence atmosphere. When the combined electrical and telecommunication cable is placed on the same place possibilities for the vulnerabilities increases.

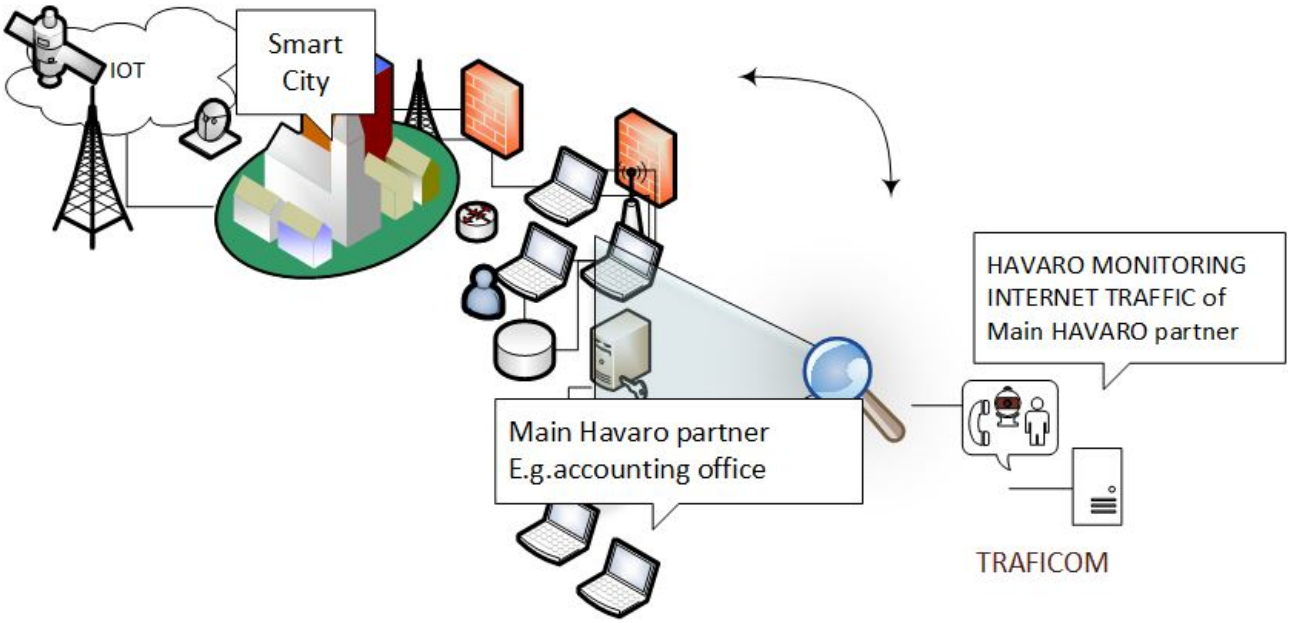

Figure 14: HAVARO 1.0 in enterprise level.

4.5.2 HAVARO 2.0

Now the HAVARO service is at the phase of development. The foundation of the operation will be the Havaro 2.0 system on the development work of which an agreement with Reaktor Oy was made in September 2018. 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 centers (SOC). The objective of the HAVARO 2.0 project is to create the trust network in which the members can change information better than before among themselves. The quick and reliable information exchange can be used to maintain the HAVARO service and however, the corresponding of the quantitative and qualitative development of information security threats to develop an early warning dimension, with the moderate resources. In the future, the service will be financed by market-based terms.

HAVARO 2.0 consists also GovHAVARO feature. That means a connection between public organisations and HAVARO early warning features. This information is classified more confidential, but sector-based sharing requires sharing of this information to all public safety organisations and central government. In EU level this information is important to be shared in real time to the stakeholders if threat-information regarding cybersecurity relate to other countries or threat information generate a common risk to vital functions. Therefor description of the HAVARO 2.0 software development has changed.

HAVARO 2.0 software development work is divided as follows:

1. Development of a network monitoring device; the sensor system needs more specialised detection features. Increasing cyber-threat atmosphere forcing to develop better and more efficient system. Gathering logs, gathering information, reverse engineering and analysing risks are not enough in the future.
2. A portal providing an interface for service centres and users;
3. An interface serving as a service bus between sensors, central system and external systems;
4. A repository where HAVARO 2.0 information is stored.

Developers are required to have knowledge of Python programming language, open source security software (including Snort, Suricata, and NFDump) and programming languages and technologies used in portals and user interfaces. System development requires experience in service design and usability design, as well as testing and automated software distribution technologies and management (e.g. Puppet or similar). Those who are working on the development of the new system require proactivity in following new cyber security and cyber security trends and solutions.

4.5.3 Shared digital library

HAVARO 2.0 will exploit identifiers to detecting threats. As MITRE Corporation mentioned [57], Common Vulnerabilities and Exposures (CVE) or (CVE-ID and CVEs) comprise a list of common identifiers for publicly known cybersecurity vulnerabilities. Each CVE Identifier consists of the following information:

- CVE identifier number
- Indication of candidate status or/and entry
- Summary description of the security vulnerability or exposure
- All essential references (i.e., vulnerability reports or OVAL-ID CVE)

CVE Numbering Authorities (CNAs) are authorised organisations which assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope for inclusion in public notifications of new vulnerabilities [57]. Information security product or service vendors and researchers use CVE Identifiers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE Identifiers [58].

The National Vulnerability Database (NVD) is the US government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP) [56]. This data enables e.g., automation of vulnerability management. The NVD consists databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics [59]. – The NVD is synchronised with the CVE List so that any updates to CVE appear directly in NVD. 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 [60].

4.5.4 Information sharing possibilities between HAVARO and E-EWS

NCSC-FI and NESA have made industry-specific classification for sharing cyber information. The classification is demonstrated as follow: VIRT (cross-administrative operational level collaboration), public organizations, defence industry, energy sector, Finance, industry automation, chemical and process industry, logistic 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 working under the Ministry of economic affairs and employment is responsible for functions vital for society in Finland. This classification follows mainly European level model, but also sector-based classification in the US.

The cyber information sharing model used in the US (Figure 5 in Chapter 3) is possible to replicate in EU level. Automated information sharing (AIS) mainly based on centralised ISACs which consists all actors of specific sector. Almost similar national level structure of information sharing is used in Finland, based on the classification of critical infrastructure sectors. The US has 16 critical infrastructure sectors; the same sector-specific frame is in use almost everywhere in western countries. AIS participants' connection to a EWS-managed system in NCSC allows bidirectional sharing of cyber threat indicators. A EWS server housed at each stakeholder´s (community) location allows them to exchange indicators with the NCSC, and participants receive and can share EWS-developed indicators they have observed in their own network defence efforts, which national cyber situation centre will then share back out to all AIS participants.

This is one kind of hybrid model, but the model consists also secure part of architecture, which allows to share trust level information. It is more important that e.g. national bureau of investigation have capability to gather trust level information concerning vital functions of society and have possibility to be connected in the system. It is relevant that the early warning data is shared from the central server to the affected sectors. International researches support controlled information sharing model where national public safety actor share relevant data to the international stakeholders via centralised centre (EWS centre) as Figure 5 illustrates. Two-way model allows also public safety organisations to use gathered information for the prevention against hybrid threats before separate phenomena illustrates as a domino effect. It is important that cross-border cooperation works directly and instantly.

4.5.5 An example concept

The future HAVARO 2.0 reflects a tendency to develop early warning functions at national level. However, this is not enough. Cross-border cyber-threats force to share critical information between EU member countries. HAVARO 2.0 will improve early detection and preventive functions. Operative public safety functions require quick response or even prediction. HAVARO 2.0 should utilise artificial intelligence (AI) to detect threats.

Figure 15 illustrates a formation of cyber information sharing between countries in which HAVARO 2.0 may join. This example consists separate national sub-hubs and one centralised hub. Information sharing participants does not exchange information with each other. All threat-informed data is shared via hub. Figure 16 demonstrates information sharing relationships and organisational structure concerning information sharing within a centralised hub system. Assume that HAVARO EWS in Country 1 (Finland) detects a weak signal of cyber-threat concerning internet traffic in multinational enterprise, but NCSA of Country 2 has not noticed signal of cyber-threat. Automated Information Sharing functionalities produce crucial data for the central EWS hub which share 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 organisations and/or to the governments which are associated with the cyber-threat.

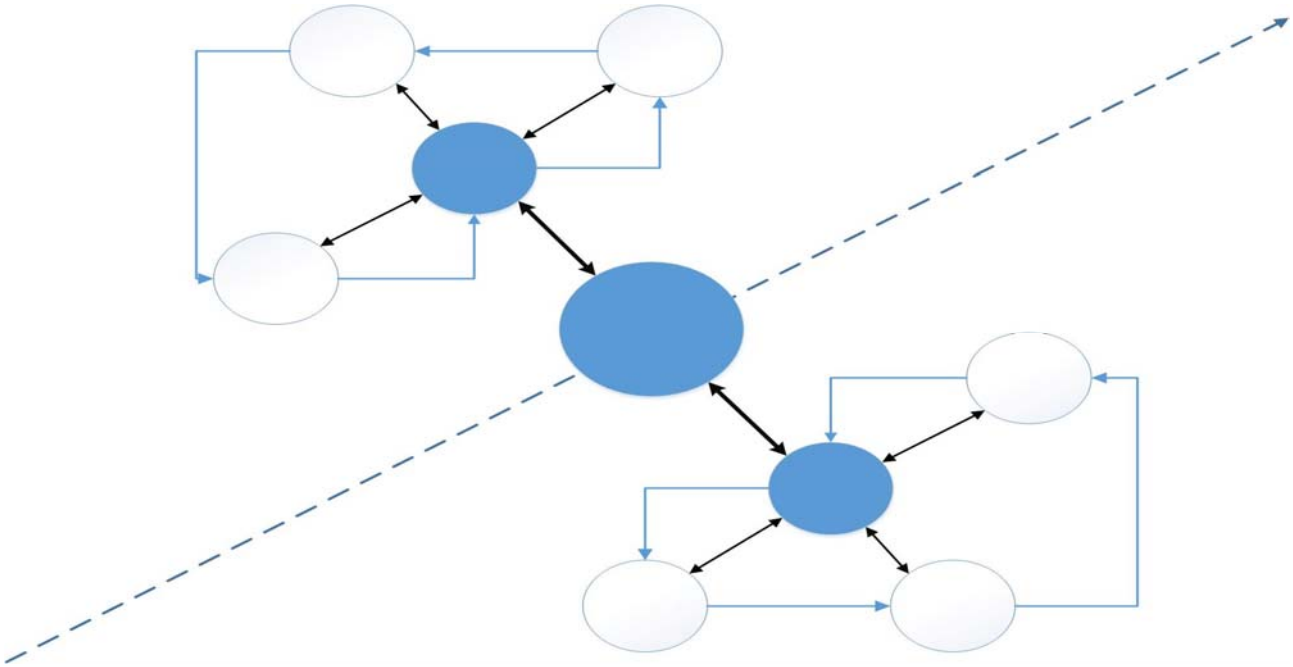

Figure 15: Centralised EWS hub and sub-hubs

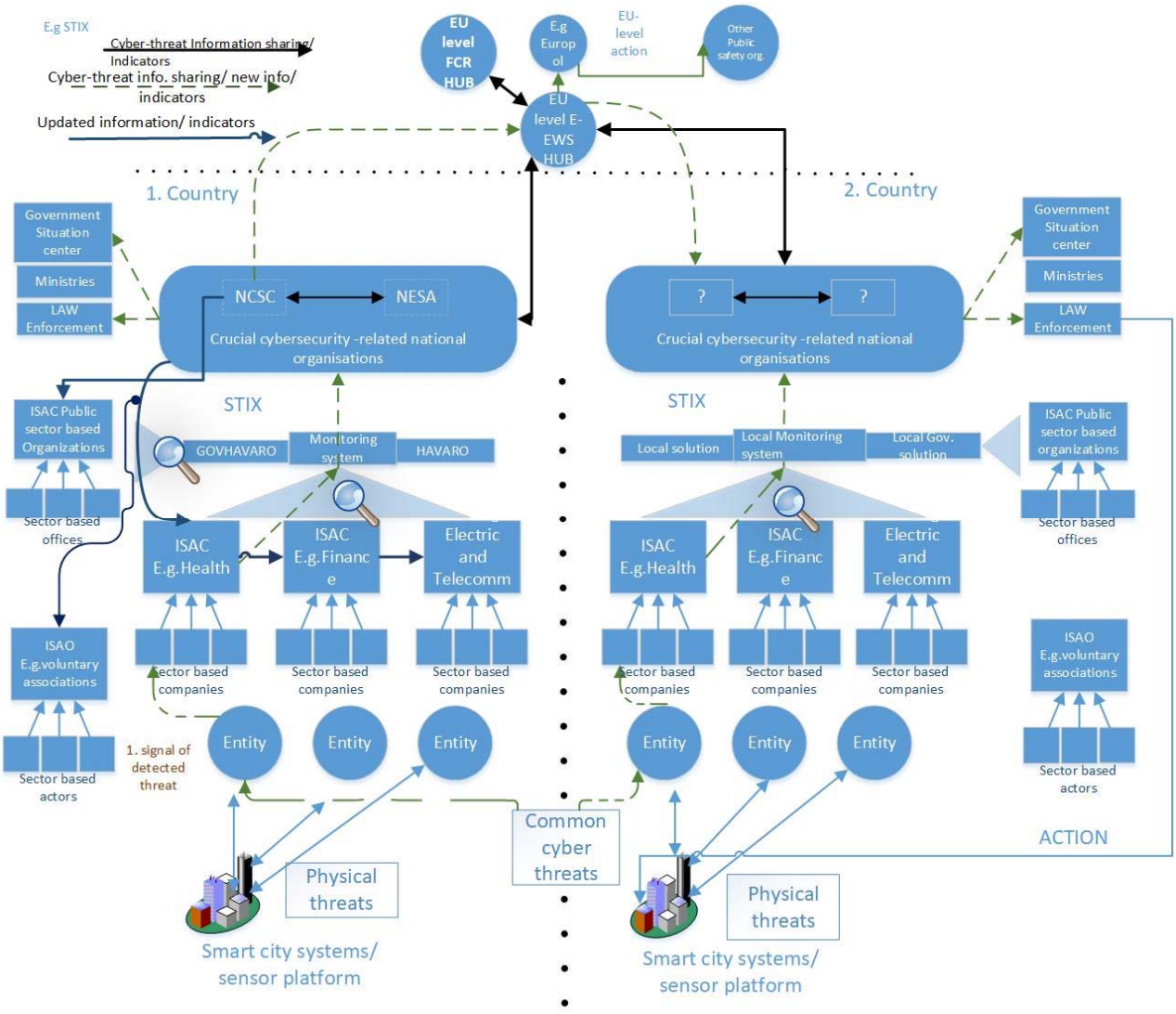

Figure 16: Example of the E-EWS information sharing

There could be own subsystem for the public organisations. NCSC of Finland use a parallel subsystem for them; HAVARO consist separate early warning solutions “GovHavaro” for all public organisations. Participants don’t need to share information directly with each other, but there is need to establish communities called e.g. ISAC and ISAO that collect crucial information concerning targeted sector of CI. This cyber security information is monitored and handled by national CERT or CIRT and cyber security centers 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.

From national systems’ point of view, such as Finnish HAVARO system, centralised EWS hub and sub-hubs is the simplest option. On the other hand, a big challenge will be who maintains the central hub, and what its governance model would be.

4.6 Comparison of information sharing models between U.S. and EU

One of the eight case studies carried out during Task 3.2 compares cyber information/intelligence sharing in and between the US and the EU emphasising cyber information sharing models in US. In addition, it handles

legislative factors, organisational factors and features of the analysed models. The complete case study report is in Annex 5.

4.7 Towards the trust-based model of the decision support mechanism

This case study aims to understand those fundamental risks that expose society to hybrid threats and to be a step towards building a trust-based model for the decision support mechanism. These threats affect to protection of critical infrastructure and prevent detection of threats. There are separate local situation centres for emerging situations, emergency response systems, separate cyber threat functions in national and EU level. All works mainly without synergy. Separate functionalities concerning artificial intelligence solutions produce more potential vulnerabilities for vital functions. Therefor it is important to develop common functionalities in cyber-ecosystem and gather relevant data for the next generation's early warning solutions.

EU needs cooperation between MSs and their smart cities, because without smart cities smart societies cannot be created. Financial competition between MSs create the need for intelligent technology development. Thus, smart information systems are being developed, it is important that there is already infrastructure where to connect the system. Every smart city should be construct from a long-term view. Every smart city needs urban built environment where different kind of intelligent systems communicate with each other.

According to Horizon 2020 work program, disruption in the operation of EU MSs within critical infrastructure may result from hazards and physical or cyber-physical events. Several public safety organisations have noticed that modern critical infrastructures and vital functions need 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. Therefore, it is important to create system which gather cyber-threat-related information to all participant.

In EU level, several ongoing projects such as MARISA and RANGER are producing better common situational awareness among MSs. Also, almost implemented EU-funded systems and mechanisms like RAPID exist. The main limitation to exploit the RAPID system is related to lack of real-time features of the mechanism. In addition, lack of leadership causes problems in collaboration.

Technical solutions need wider understanding of user needs, which means that infrastructure of smart city environment, cannot be developed separately. There is also wider need to develop common emergency response ecosystem for European public safety actors. This means that communication solutions that are used within public safety authorities must suite well in urban and rural area.

Public safety actors like European law enforcement agencies need common shared situational picture for the cross-boarding tasks in a way that operational co-operation is based on a reliable platform. Formal integration in European Union and between member countries has developed rapidly. This does not mean that co-operation between organisations has developed in the same proportion. Digitalisation cannot evolve in isolation from the society. There are fundamental needs within European public safety organisations that should be in a same level in every country.

The structure of central and local government in Finland challenges utilisation and implementation of new technology. Technological development, development of infrastructure, architecture of constructions and changes in legislation are inner-country challenges but also European common needs concerning safety development agenda. State level factors should be added in European safety framework. There are many strategy plans in the European level concerning safety functions, but national implementation realises in different order.

Political decision makers are elected in election, but highest authorities are chosen based on political selection criteria. Hybrid influencing can made unstable the society in many ways. One of the main key aims is to influence political decision-making. In practice, this means that there is a need to integrate organisational,

administrative and operative functions. Flow of reliable information between decision-makers, intelligence authorities and data protection authorities must be ensured by using artificial intelligence systems. In an ideal model, national protection of vital functions would be ensured automatically as a part of functionalities of cyber platform where human based decisions are also analysed.

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 is under the process. Time will show how prepare our politicians are to develop the legislative base for new cyber-ecosystem. It has been said that Finland need to update whole intelligence atmosphere to the same level as the other European countries has been done.

4.7.1 Development of Emergency response system solutions for PPDR authorities

Emergency Response Centre uses 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, to optimise response activities and to act as a mechanism for queuing ongoing incidents [43].

In Finland, traditional emergency response functions has been copied from the other countries, but still we have fundamental problems concerning the possibilities on how to transfer emergency data correctly and in time to the Emergency response centre. There was separate emergency response unit in the Police organisations until the 1999. For example, regional Radio Police consisted of their own dispatch personnel who answered to citizens'' emergency calls and managed the use of emergency units to the site of an accident; also, municipal rescue services handled their own emergency calls. In the 21st century, separate emergency call centre units and functions were united into one regional emergency response centre. Very soon after the organisation changes, PPDR authorities found the need to manage their emergency resources. PPDR organisations established own situation centres to allocate emergency resources concerning the field workers cooperation. It is impossible to develop technological solutions without understanding the culture of the organisation. Public safety organisations have common working culture, but also separate inner-organisational subcultures. That same issue concerning the meaning of the working culture relation to organisational reform occur also in different atmosphere and in different field.

In practice, this means that smart city infrastructure is the fundamental framework, which govern minor factors inside on it. Technological solutions cannot create its own separate entity regardless of the organisations culture.

4.7.2 Smart nations and cities

Political power relations effect to the national future of digitalisation. Urbanisation changes our style of living and the modern environment create new safety culture. Citizens meet other people in public places e.g., they go to the shopping mall for shopping goods. The time has changed, because of many terror attacks. There are many historical similarities between countries in northern Europe. That helps to understand the safety needs of other neighbouring country. While separate European societies are evolving, societies are developing their cooperation on digitalisation. It´s necessary to see the development of digitalisation of northern countries from the same perspective. There are different political aspects between countries concerning energy policy and security policy. EU as the commercial operator brings its own needs into discussion. Russia-China cooperation challenges our culture and western way of thinking. We need cooperation, but cybersecurity threats appear too often [61]. Nord Stream2 and different kind of 5g and cable projects may expose national security under to cross-boarding hybrid risks [62]. It is impossible to create entirety of smart society without understanding continuity management of society.

If departments of the central government design separate digitalisation projects without common understanding of the future needs, society's expenses and management of digitalisation becomes more

difficult. The governance of digitalisation 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.

4.7.3 Risk management and preparedness

The NIST risk management framework consist three elements of critical infrastructure (physical, cyber, and human) which are explicitly identified and should be integrated throughout the tiers of the framework [32]. The critical infrastructure risk management framework as Figure 17 illustrates supports a decision-making process that CI actors or partners together promise to inform the selection of risk management actions. It has planned to provide flexibility for use in all sectors, across geographic regions, and by different partners. It can be tailored to different operating environments and applies to all kind of threats [32].

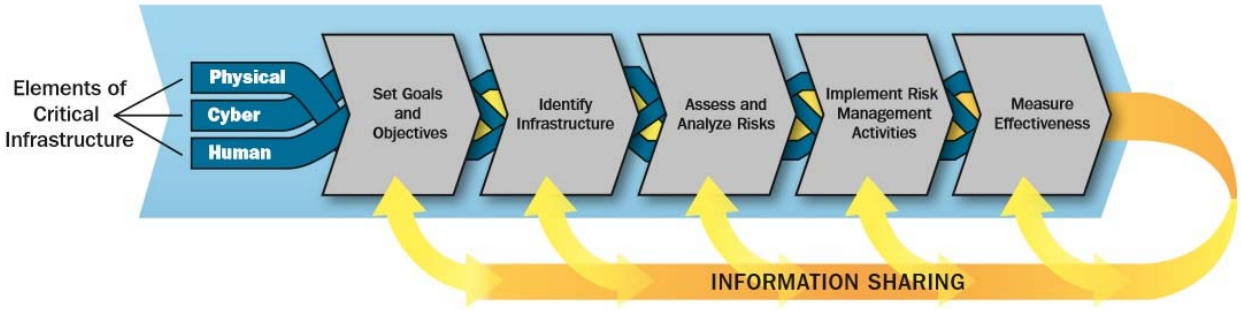

Figure 17: Elements of critical infrastructure [32]

Risk management concept enables the CI 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 hazards or incidents. It strengthens resilience by identifying and prioritising actions to secure continuity of vital functions and services [32].

The first point recommends to "*set infrastructure Goals and Objectives"* which are supported by objectives and priorities developed at the sector level. The second point recommends to "*manage CI risk effectively"*, which means that stakeholders need identify the assets, systems, and networks that are crucial to their continuity management, considering associated dependencies and interdependencies. This dimension of the risk management process should identify information and communications technologies that facilitate the provision of essential services [32].

Third point recommend to "*assessing and analysing risks"*. Those risks may comprise threats, vulnerabilities and consequences. Threat can be 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 happen as physical feature or operational attribute. It may render an entity open to exploitation. [32]. Consequence can be effect of an event, incident, or occurrence. "*Implementing risk management*" activities and functions means that decision makers prioritise activities to manage critical infrastructure risk based on the criticality, the costs of the affected infrastructure and the potential for risk reduction [32]. The last element "*measuring effectiveness"* means that the actors and stakeholders of the critical infrastructure evaluate the effectiveness of risk management efforts from national, to local levels by developing metrics for direct and indirect indicator measurements [32].

In this case study, we have applied a modified combination of NIST [17] and Octave Allegro Risk Assessment Frameworks. According to [63] Octave allegro is a strategy for prioritising and sharing information about the security risks to an information technology.

According to [64] NASA risk informed risk is the potential for performance shortfalls, which may be realised in the future. Risk Management by NASA integrates Risk-Informed Decision Making (RIDM) process and Continuous Risk Management (CRM) process into a single framework. The RIDM process focuses the risk-informed choice of decision alternatives to assure efficient approaches to achieving objectives. The CRM process addresses implementation of the selected alternative to ensure that requirements are fulfilled. RIDM and CRM generate effective risk management as NASA programs [63, 65].

4.7.4 Research process

There have been many state level discussions concerning digitalisation and robotics between decision makers in media. At present public safety authorities (PPDR) or state level decision makers do not use cyber dimension in their daily routine at all. The problem is that public safety authorities have separate Cyber security organisations with own administrations. Organisations, which have responsibilities for cyber security operations, are separated from PPDR services. As a part of TRAFICOM, 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 centres or situation centres. Separate organisational cyber security functions, methods and procedures prevent effective response for cyber physical threats. That is not only problem. New kind of emergency response systems are all useless if our politicians and other decision makers are not faithful or decisions are made for the benefit for a foreign country. It´s important to understand the source and degree of threat. Infrastructure of smart cities and all smart information systems may can be built on an unstable ground level, which may consist e.g. energy supply solutions and dicey communication equipment. Combining Open Source Intelligence data and traditional intelligence sources, overall situational awareness arises. Hybrid threats need coordinated hybrid responses, therefore also a cyber-situational picture is needed.

It is easier to detect fundamental level risk factors when basic threats and risks are categorised and classified. These threats affect to protection of vital functions and prevent detection of threats. We have used combination of different methodologies to find out those factors, which affect to the decision-making in society. As Table 18 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.

Main risk classification and subcategories				
A Administrative risks	**B Conflict risks**	**C PPDR services and functions related risks**	**D Socioeconomic risks**	**E 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 decision makers (B,C,D,E)	Human made disasters or pandemic €	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 €	Cross-border radiation (C,D,E)	Lack of resources in PPDR services/ (A,D,E)	Cultural change (A,B)	Recovery problems (A,B,C,D)
Organisational 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)

Main risk classification and subcategories				
	Unidentified people (A,C,E)			

Table 18: Risk classification

Separate risks are categorised and ranked on a three risks level process.

The first measure is valued “frequency of the phenomenon” (1 = phenomenon not occurs every year, 2 = phenomenon occurs yearly and 3 = a phenomenon is permanently). 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 = impact 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.

The one goal of the research is to create decision support sub-system for the proposed Hybrid Emergency Response system that could assist politicians and public sector actors. This 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 the designing of the subsystem of Hybrid emergency response systems. 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, which emphasises the proper use of risk analysis in its broadest sense to make risk-informed decisions that affect all mission execution domains, including safety, technical, cost, and schedule. RIDM helps to 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 [66] .

The main goal of the study is to find out fundamental societal factors, which affect to effective protection of critical infrastructure. This research divides the types of risks into four sections. Ground Level indicate fundamental risks with scenarios, which includes factors, events and actions of society. The fundamental factors of scenarios put all other societal factors, events or actions into secondary threats level. Fundamental factors also make it possible to realise lower-level threats.

This causes that the effective protection of critical infrastructure depends on external factors. Operator who controls external factors also dominates critical infrastructure. Therefor fundamental ground level risk factors should be recognised and minimise.

4.7.5 Findings

Table 19 shows that different elements of society between risks levels exist. Higher risk levels are in the right. These elements set the greatest threats to the vital functions. If ground level threats realised, protection of critical infrastructure loses its meaning. Finland as a member of the EU it is possible that we gave away part of the sovereignty of parliament concerning national regulation. This kind of problems may happen when supranational legislation gives away power of decision-making from government to the commercial operators.

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 urban area	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 PPDR services	XX	Unidentified people	XXX
		Organisational 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		

Table 19: Impacts of risks

Findings indicate that lower level risks of critical infrastructure do not cause problems to the ground level risks. Higher level risks indicate also structural governance problems in society. Effectiveness level indicate threats impacts to the vital functions. Three x means that basic independent level risk becomes more dangerous due to connection fundamental ground level scenario.

As Table 20 illustrates, if higher (4) level risk support 4 or more scenarios and consequences, impact level is occasional for the all vital functions. This change of situation is caused by the domino effect. E.g., a separate cyberattack is not so dangerous, but if it is due to a political decision, the danger of the event will change essentially.

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; foreign state may use cables and pipelines for hybrid influencing

Ground level - Scenario	Consequences
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.

Table 20: Scenarios and Consequences

Threats like serious disruptions to power supply, serious disruptions to telecommunications and information systems risks are noticed in Finland security strategy for society report, but the same fundamental risk types occur as the causes which has not taken to account in decision-making

4.7.6 Remarks

In our research, the need for the technology development was expressed as an overload of work environment and shortening of the life cycles of information systems. At present e.g. in Finland designed solutions of public operators based on old-fashioned technology. In the near future the victim of an accident may have to wait longer for the respond of emergency response centre, because call centre personnel have the learn how to use the new system. In Finland the main problem concerning interaction between artificial intelligence features of the new emergency response system and human being. Time to handle calls will initially be extended despite of new AI tools of the system. However, there are no more officers than before, but the need of dispatch workers will increase. Everything starts with cultural understanding and process management. The subcultures of different PPDR authorities should be coordinated through systems. Currently everyone actors have their own separate operating model.

For example, 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 a holiday weekend does not at least reflect the understanding of the situation in the operating environment. Fully automated call centre can be a reality within a decade. Fully automated decision support system for the highest decision makers can be in use in the near future, because vital functions require proof political decisions. When human weaknesses are left out of decision-making procedure, for example 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, because credibility and reliability of decision-making process can be calculated. At present emergency response functions and procedures are dependent on human ability. Early detection of a threat and rapid response often help to save human lives and properties during disasters.

We cannot hide our history and culture, but if we are developing cybersecurity smart ecosystem, we need to make changes to the decision-making processes. The research has been shown that different kind of structural fundamental threats may occur before any classified threat has been illustrated. Engineers, architects and designers cannot develop nothing new concerning smart solutions if fundamental base is unstable. An unsecured platform causes fundamental problems to develop solutions for the vital functions of the smart society. European Union level 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 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 fiber optical and power supply are transmitted through the same hybrid-cable. So called unexpected happenings effects to all elements of ecosystem. This kind of threats come true and happens out of public safety control. In the future its occasional issue to found right balance between national security and good bilateral relations

The case study shows that the most troublesome and most significant threats to national security and vital functions are related to human factors which based on politician´s decisions 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. The study suggests that the use of artificial intelligence should be enhanced to support decision-making. Subsystem could also operate as a part of the next generation emergency response model as Figure 18 illustrates. At present state level political decision-making dimension may prevent the utilisation and usefulness of the proposed smart hybrid emergency model. Politicians and other decision makers of Finland need to take into consideration that cyber preparedness, operational preparedness and reliability of decision making are not a separate part in the continuity management. If fundamental risk factors are not recognised technical early warning solutions become useless.

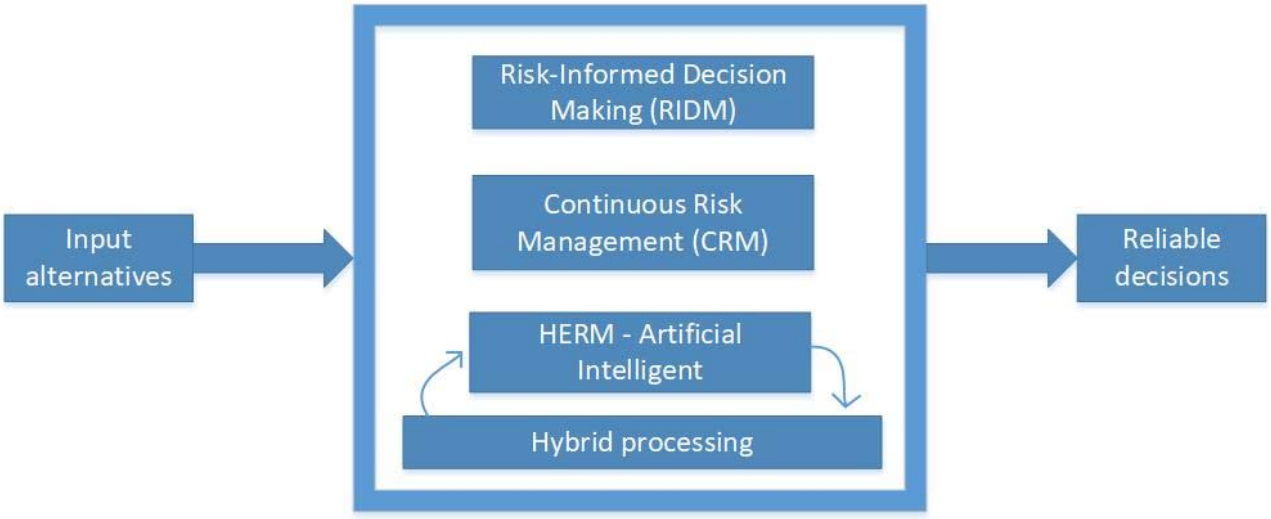

Figure 18: Hybrid Risk Management system

4.8 Synergies of information sharing needs with E-EWS and E-FCR

The role of the ECHO Federated Cyber Range (E-FCR) is to interconnect existing cyber-range capabilities through a convenient portal operating as a broker between user requirements and a pool of available cyber range capabilities.

The E-EWS and E-FCR are two of the four vital technologies developed within the ECHO project. Both can exploit each other in order to maximise their capabilities and offerings to the users. The following are the three most relevant use cases where data exchange is required:

1) The Early Warning System can be a part of an exercise or a training that runs on one of the cyber ranges which is also connected to the E-FCR. The data and incident reports that are produced from the exercise/training can be fed into the EWS which will then make an analysis of this. This analysis can be used to by the organisers of the exercise or training to maximise the impact of the exercise/training on the participants.
2) The EWS can collect threat intelligence data from the realistic simulation environment running on E-FCR. This in turn can be used as input by the EWS for alarms or any further analysis done on the EWS. Potentially a digital twin can be set up for the E-FCR where various simulations and scenarios can be run and tested. The EWS in turn can use this input for analysis.
3) EWS can share quarterly data and analysis with the E-FCR's Content Providers in order to allow them to design training and exercise scenarios based on real world needs.

5. Cross-case conclusions & System requirement

This section presents the recommendations for the E-EWS following a document analysis exercise of the preceding sections and a selection of literature sources.

5.1 Context

At the kernel of information sharing lies the intelligence data item (IDI). In the context of ECHO, an intelligence data item is defined as any piece of data that potentially contains actionable information relating to cyber security. Appreciating the enormous value of information and its potential, an information sharing framework is required in order to appropriately manage the lifecycle of the corresponding data items, from their generation, processing, dissemination all the way to their destruction. ECHO envisages the creation of a community of a large pool of stakeholders who will engage in joint intelligence activities and reliably share information and collaborate in handling security incidents in an effective and timely manner. As such, establishing and ensuring trust is a key factor for the successful adoption of the EWS.

ECHO's information sharing and its instantiation as the E-EWS will adopt the joint intelligence process comprising of the 6 operations (planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; evaluation and feedback) and adapt and extend - if necessary - the MISP taxonomies.

5.1.1 Characteristics of intelligence data items

At a first level of discrimination, IDIs can be structured, semi-structured or unstructured. Typically unstructured data refer to primary sources of information that are normally processed by automated or human means for extracting the necessary information. This process would generate structured IDIs that would allow automated processing. It should be noted though that there can be primary sources ingested into the EWS that are structured (e.g. log files).

IDIs can also be distinguished as reference information or operational information. Reference information refers to the IDIs that contribute in achieving situational awareness, allowing the beneficiary to make informed judgements on the cyber risks of the organisation. Operational information relates to those IDIs that support the actual decision making, handling incidents and so forth.

The IDIs should be accompanied by metadata that will contextualise the contained information but also enable the EWS to implement and enforce authorisation and access control mechanisms. Common identifiers and enumerations should be used whenever possible.

Figure 19 shows the key components and benefits and goals of the ECHO intelligence information sharing approach.

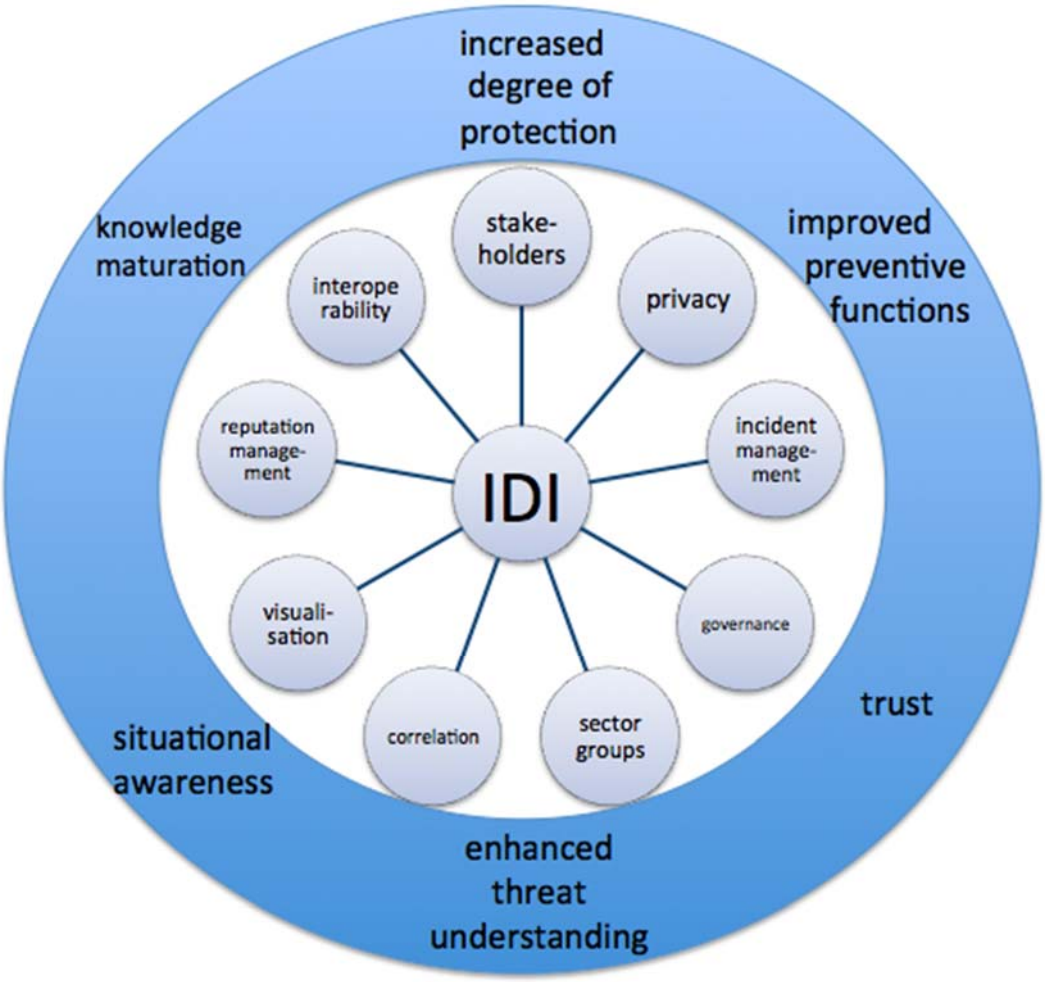

Figure 19: ECHO's information sharing at a glance

Table 21 presents an initial list of the categories of information and their expressions as IDIs. IDIs that potentially contain Personal Information will need to also meet the privacy requirements (see subsection below). The categories will be further expanded and refined following the requirements elicitation and specification of the E-EWS (WP5).

Information category	IDI	structured/ unstructured	reference/ operational	Personal Information
Technical threat indicator	IOC (email, IP address, file hash, mutex, domain)	S	R	
Intrusion attempt	Threat Actor IOC (atomic, composite, behavioural)	S S	O O	X
Security alert	Ticket Readiness level	Semi S	O R/O	
Vulnerability information	CVE CVSS Threat identification Geopolitical Exploitability	S S Semi U S	R/O R/O O R R	
Vulnerability report	Vulnerability scanning report	S	R	

Information category	IDI	structured/ unstructured	reference/ operational	Personal Information
Incident report	Report	U	O	?
TTP	ATT&CK STIX object	S S	R/O R/O	
Remediation actions	Operating procedure Playbook	U U	O O	
Asset	CPE to describe system platforms CCE (common configuration enumeration)	S S	R/O R/O	
Discussion	Discussion item	U	R/O	?
Blog post	Reference	U	R/O	
Poll	Poll item	U	R/O	
Raw data	Log-file Netflow Packet capture RAM image dump Malware sample VM Image File Email	S S Semi Semi Semi U U U	O O O O O O R/O R/O	X X ? X X

Table 21: Intelligence items

5.1.2 Information sharing model assumptions

Against all the above, the proposed ECHO information sharing model is based on the following assumptions or premises:

- There will be a clear and concise governance model for the intelligence data items, where each item will be described by a comprehensive list of contextual information (metadata) to allow fine-grained decision making on the management and handling of the data.
- There will be a clear process for on-boarding and off-boarding of participating organisations.
- It is expected that it would be easier for organisations being in the same sector or having similar goals and purpose to form easier clusters for sharing threat intelligence information, as they are more likely to have established and mature exchange arrangements; therefore they are more likely to reach consensus. On the contrary, organisations that operate in orthogonal industries (i.e. where their respective industries have virtually nothing in common) is expected that would be less forthcoming in sharing information.
- Stakeholders and participants are expected to join pre-defined and ad hoc groups.
- Trust will be delivered through technical, organisational and human means.
- Due to the nature and diversity of sectors, in order for information sharing to provide a meaningful and accurate services, the scope of the data items should be extended to encompass Cyber Physical Systems; indicatively, this can consider the practices found in the Maritime Sector where there is a clear distinction between cyber (e.g. IT networks) and Physical (e.g. Operational Technology networks) highlighting the existence and interdependencies between the physical and cyber plane.
- Translation and normalisation services will allow the standardisation of intelligence data items. The underlying taxonomies and schemas should cater for the verticals by including optional fields.
- Existing standards for information processing and sharing will be adopted wherever possible.

5.2 Information sharing architecture

Information sharing is highly dependent upon and influenced by the regulatory frameworks as well as the cultural norms both within a sector and the organisation itself. In academia for example, barriers to sharing are expected to be lower than the other sectors, due to the culture of freedom of academic expression and an academic citizen mentality of peer review and dissemination of research output. On the other hand, in critical infrastructure type of sectors such as Energy, or in banking, information sharing is more intensely regulated, and this also is reflected in the respective organisational cultures. This creates a tessellation of regulatory frameworks and cultural antecedents on the following levels:

1. Intra-Organisational, influenced by specific internal policies and procedures.
2. Intra-Sector, imposed by the respective sector.
3. National-governmental, governed by the respective strategic decisions on a national level.
4. Transnational, through the international agreements, treaties and EU legislation and directives, in the case of the organisation operating within the EU. This may include frameworks for information sharing with Law Enforcement entities.

The above are also complemented by horizontal legislation such as the GDPR that cuts across all sectors.

Provided that:

- The ECHO pilot is part of the EU initiative on establishing a network of competency centres, and
- ECHO aims to support information sharing among and between a multitude of sectors with Healthcare, Energy and Maritime being initially considered.

A modified hybrid model architecture is recommended as this appears to best fit the requirements following the cross-case analysis. In essence, the hybrid approach will allow to maintain a basic form of hierarchy, and at the same time it will allow the connection of different hubs, forming a higher level peer to peer. This is also in accordance to how CERTs operate and share information, which is done on a peer to peer basis but also within their level of operation (e.g. national, organisational, etc.). Allowing some degree of centralisation will also enable centralised decision making and support the emergence of Coordination Centres. A hub could represent a variety of communities, such as a specific sector, an interest group or a national point. It is recommended that each hub will refer to organisations of common characteristics, goals or sector, simplifying its management, internal governance and deployment complexity. This would be in line with the E-EWS architecture supporting tenants allowing also seamless integration through the sharing API capability that will connect EWS instances.

From a governance perspective, the immediate consequence of this would be to have trust realms, two tiers of cross organisational boundaries, as shown in Figure 20.

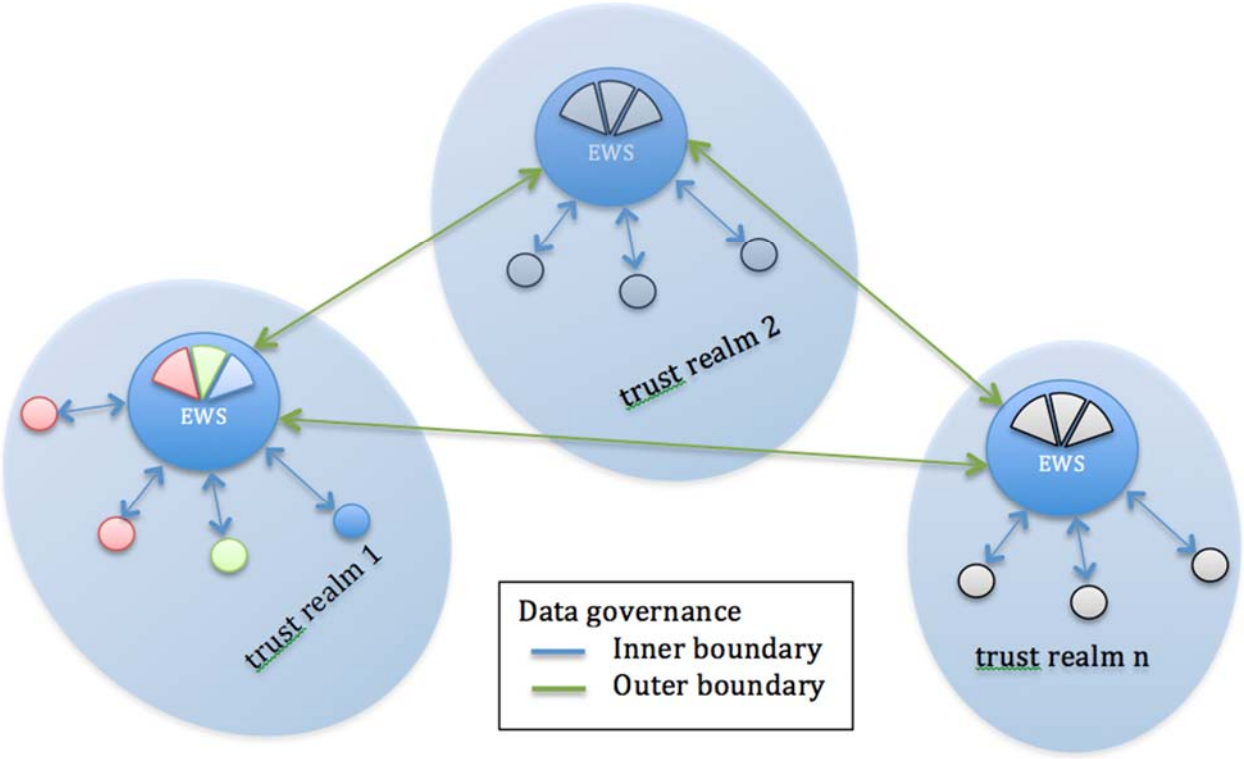

Figure 20: Information sharing architecture

In the figure above, three trust realms are presented. Each realm can correspond to any type of organisational cluster, e.g. realm 1 could be academic CERTs, realm 2 national cyber security competency centres and realms 3 maritime sector. Every trust realm can have more than one EWS instances, for scalability and resilience purposes. The governance model could refer to policies and security certification requirements for deploying an E-EWS instance.

The first step for an organisation or individual joining the E-EWS ecosystem is to complete the on-boarding process. Upon successful application, the organisation is allocated a tenant slice. This will host all information provided by the participating organisation. Organisation boundaries can be crossed within a given trust realm and these are specified through the inner boundary data governance. It is expected that these will be the first to be formed, upon the emergence of the E-EWS.

Inter-realm information sharing is controlled by the outer boundary data governance models. These are expected to be more complex and diverse and will require a longer maturity period. It should be noted that not all trust realms will necessarily connect to each other; such configurations imply that some realms will emerge to be more authoritative and trustworthy than others, but should also indicate that transitive trust should not be guaranteed or offered.

IDIs containing personal information will be go through anonymization and redaction layers prior to leaving a tenant's area. For structured IDIs, automated processes would seamlessly and efficiently implement the underlying privacy policy. Information classification schemes will be enforced at the organisational boundaries (coarse grained access control) as well as internally (fine grained).

As the organisation participation and connectivity between the hubs increases, the value of the network is expected also to increase, in accordance to Metcalfe's Law. However, as this increase is very likely to result to generation of large volumes of data, the perceived usefulness is expected to decrease. In order to compensate for this, information sharing should not only be limited by access control criteria, but additional contextual features to enable effective filtering of non-relevant information (noise). A representative feature for

this task is asset information. For example, by using the Common Platform Enumeration (CPE) convention, an organisation can describe their assets in a standardised way. By doing this it would be possible to quickly filter out attacks and vulnerabilities that are not applicable to a particular organisation's attack surface.

5.3 Stakeholders

These operate at different levels, having potentially diverse agendas and priorities:

CERTS/CSIRTS:

- National/EU CERTS – protect national and critical infrastructure
- ISP CERTS – protect Internet related services and backbone
- Organisational CERTS – protect organisation
- ICT Vendor CERTS – protect products
- Academic CERTS – protect academic infrastructure, facilitate research and innovation

Public safety organisations:

- Law enforcement Agencies. These are secondary users that may be involved when handling incidents. As such, the E-EWS will allow the collection and preservation of evidence in a forensically sound manner.

Information sharing entities:

- Individuals
- Researchers
- Organisations
- National
- Private
- Critical infrastructure
- Research

5.4 Features of the information sharing system

A modular approach for the E-EWS is considered. The core EWS should comprised of a ticketing system supporting distributed workflow among a number of different partners and organisations. The EWS should allow the enrichment and contextualisation of the introduced and ingress information. As such, a standard description and an expandable information taxonomy should be considered.

An initial list of features of the perspective E-EWS is presented below:

- **A suitable confidentiality model, such as the traffic light protocol.**
  All intelligence items will need to be assigned with a designation to ensure that the sensitive information is shared with the appropriate audience. TLP is recommended because it is less formal, does not really require NDAs, etc., it is more of a "gentlemen's agreement" and allows a faster communication of incident data. TLP will of course run in conjunction with the standard system's access control mechanisms, such as RBAC. For the E-EWS system in particular and upon a joint decision, FIRST's TLP definition is adopted to support future interoperability and standardisation with all pilots. Moreover, the confidentiality model – due to the nature of the EWS – should include introduction of information by protecting source attribution (Chatham House rule), in order to facilitate the submission of any information that can be vital when handling security incidents. A direct consequence of this is the consideration of the reliability of the data, defined further below.

- **An access control scheme, capable of making fine-grained access control decisions.**
  The audience accessing intelligence items shall be controlled through access classifiers such as organisations, groups, and roles.
- **Support of multiple taxonomies and standards for intelligence sharing**.
  This will allow the hosting of organisations belonging in different sectors.
- **Capabilities for a structured sharing of intelligence data**
  e.g. use of Structured Threat Information eXpression (STIX)
- **The system should facilitate the exchange of intelligence between CERTS/CSIRTS and LEAs**.
  Terminologies used in the two communities are sometimes different. ENISA recommends using the 'Common Taxonomy for Law Enforcement and The National Network of CSIRTs'.
- **Common data and document formats support**.
  Use of common formats e.g. Word, PDF, and CSV facilitate intelligence sharing where the use of specialised formats is not an option.
- **Capability to evaluate the reliability of the source of an intelligence data item**.
  All information sources should be assessed for reliability based on a technical assessment of their capability, or in the case of human intelligence source, their history.
- **Assessment of the credibility of an intelligence data item based on likelihood and levels of corroboration by other sources.**
  An EWS allowing a quick turnaround and fast decision making requires that the ingress information is trusted. The system should have mechanisms to assess the credibility of the information and include fake news protection mechanisms.
- **A shared workflow management system for incident handling**.
  This is one of the main purposes and core functionalities of the E-EWS, allowing also to monitor the effectiveness and efficiency of the system.
- **Trust-boosting security technologies**.
  Supporting the creation of closed communities and encrypted peer to peer communication.
- **Data redaction capabilities, for privacy compliance**.
  The system will need to redact personal information for data items marked to contain PI when exporting them to other EWS instances based on a privacy protection policy. For structured data, this can be done automatically. For unstructured data, this can be done semi-automatically, but may require human inspection and approval.
- **Attribution capabilities, identification of the origins of the source of information**.
  For traceability, disseminated information shall contain appropriate origin describing meta-data.
- **Anonymous sharing of information**.
  Despite the attribution requirements, it is advised that the system would still allow anonymous information, however, these items will need to be clearly marked as anonymous and is expected to have an impact on the reliability of the information.
- **Customisable exchange of intelligence data**.
  Customisation may be in accordance with internal (originating organisation) or external requirements.
- **Predefined criteria for data dissemination**.
  This relates to both the originator of the information (e.g. the criteria a set in accordance with audience, trust realms etc.) and the consumer of the information (e.g. data versions and revisions, severity, etc.)
- **Data normalisation**.
  The system shall normalise all ingress data under a common format, or data model. This will enable compatibility, interoperability and other functions (correlation)
- **A flexible data model**.
  Expansion of the data model is a prerequisite to allow E-EWS to grow across different domains and verticals. The system can allow custom creation of tags and the enrichment of existing IDIs. This could be automatic or manual. For example an IDI may be enriched by external information from OSINT activities.

- **Correlation capabilities**.
  At a minimum level, the system should automatically link newly imported IDIs with existing IDIs.
- **Data items curation**.
  The system shall curate and de-duplicate IDIs imported from different sources and datasets. This is for ensuring that the integrity and accuracy of analytics is offered.
- **Advanced data analytics**.
  Situational awareness will be considerably supported from data analytics techniques (e.g. clustering and classification). This could include production of trends over time related data to support predictive analytics.
- **Visual analytics**.
  The system should provide visual analytics through a dynamic, interactive UI.
- **Pivoting capabilities**.
  In order to support the analytics processes and allow complex correlations and analytics, the system should offer pivoting capabilities over data.
- **Data exporting formats**.
  The system shall support exporting of data in different formats e.g. STIX, OpenIOC, CSV, Yara, sigma, etc.
- **Filtering capabilities**.
  The system should support filtering of information across a number of parameters and features. This also includes both whitelisting, blacklisting, to filter out benign activity and to pin down suspicious/malicious events.
- **Triaging**.
  The system should provide a high level overview of the data so that the analyst can quickly get a "gist" of what they contain. For example, for numerical data, the basic statistical information should be presented.
- **Alerting and communication**.
  This feature is required to improve the response times to incidents. This involves capabilities to match asset configuration with vulnerability information (for example describing assets as CPE and pairing with CVE and CVSS items) and sending a message to a designated contact point if a criticality level of an event exceeds some threshold. For example, this can be done if an asset described through a configuration is detected to be vulnerable to an exploit with a CVSS score.
- **Intelligence report generation**.
  The information shared should be available to the stakeholders in an appropriate format and level of detail.

5.5 Privacy requirements

In order to identify the personal information to be managed and processed by ECHO, the consortium carried out a detailed analysis of the different categories of personal information to be processed and its lifecycle. This analysis is described in the Data Protection Impact Analysis Report [67].

ECHO is underpinned by a series of privacy statements. These comply with the General Data Protection Regulation (GDPR) and are managed and overseen by the Data Controller and Data Protection Officer (DPO) for the project, RHEA System SA (RHEA).

In addition to these statements, each consortium member will liaise with the DPO to establish a Data Protection Impact Assessment (DPIA) must be conducted prior to any data collection or processing taking place. This decision will be reviewed whenever the data category, type or the nature and/or scope of the processing changes.

Data Processing refers to any handling of data whether this is capturing, creating, modifying, adding, deleting, sharing or otherwise handling of data. Therefore, any and all data captured/to be captured and processed,

whether manually or by automation as part of this project will be processed in some way and potentially fall within the remit of the General Data Protection (GDPR).

Collecting of IDIs having personal information such as a threat actor, log-file, RAM image dump, etc. (see Table 21) will be processed and stored in accordance with the following privacy requirements:

P1. Lawful basis for processing:

a. the lawful basis for processing data will be specified, recorded and justified;
b. the data will be classified in accordance with sensitivity as either:
    I. Personally Identifying (PI)
    II. Non-personal (N)
    III. Other (O) (meaning the classification is to be confirmed pending discussion with project lead, privacy officer or DPO)

P2. Purpose Limitation: personal data should only be processed for needed and specified purpose; no personal data should be reused without informed consent first being obtained. Informed consent templates are provided within the ECHO project documentation (Reference Materials, documents folder);

P3. Data Minimisation: only necessary data for the specified purpose will be processed;

P4. Accuracy: the data will be accurate and kept up to date;

P5. Storage Limitation: data will be pseudonymised or anonymised as soon as practicable and kept for no longer than absolutely necessary ('the data life'). At the end of the data life, data will be securely deleted and/or destroyed.

P6. Integrity and Confidentiality:

a. Confidentiality: Ensuring data is only accessible to authorised stakeholders
b. Integrity: Ensuring non-repudiation and reliability for each piece of data, i.e. processing correct, authentic, and unmodified data.
c. Availability: Ensuring data is usable on demand and accessible to authorised stakeholders
d. Unlinkability: Ensuring data cannot be sufficiently distinguished to linked across platforms or domains with similar context or purposes
e. Unobservability/ Undetectability: Ensuring data is anonymised so that the anonymity and undectability of the individual is preserved
f. Anonymity: Obfuscating links between data and identity i.e. the ability to distinguish any one individual from the data
g. Pseudonymity: Replacing identifying data with pseudonyms ensuring any links to original data cannot be made by unauthorised parties

P7. Intervenability: Enabling data subject access and/or supervisory authority access to affect action on the records (e.g. request modification and/or deletion). In that way it can be seen as a safeguarding measure that must be included within any process or system involving personal data

a. Transparency: Openness - Providing assurance, accountability and traceability for internal and external stakeholders.

P8. Proportionality: Proportionality requires that any limitation on the rights of the individual have to be justified. For example, making sure that the measure(s) taken in processing the data do not disproportionally limit the rights of the individual whose data is being processed. A pre-condition is that the measure(s) taken in processing or safeguarding are sufficient to achieve the objective while only relevant personal data for the purposes of the processing is collected and processed.

These privacy goals comply with the GDPR and are based on the privacy principles of GDPR (P1-7) and those in the Privacy Lifecycle PLAN (i-ix), that forms part of the Privacy and Compliance framework (PACT) [68].

6. Conclusions

- ECHO envisages the creation of a community of a large pool of stakeholders who will engage in joint intelligence activities and reliably share information and collaborate in handling security incidents in an effective and timely manner. The main goals of ECHO intelligence information sharing are: 1) trust, 2) enhanced threat understanding, 3) situational awareness, 4) knowledge maturation, 5) increased degree of protection, and 6) improved preventive functions.
- ECHO's information sharing and its instantiation as the E-EWS will adopt the joint intelligence process comprising of the 6 operations (planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; evaluation and feedback) and adapt and extend - if necessary - the MISP taxonomies.
- In ECHO, Intelligence Data Item (IDI), the kernel of information sharing, is any piece of data that potentially contains actionable information relating to cyber security. An information sharing framework is required to manage IDIs' lifecycle; generation, processing, dissemination all the way to destruction.
- The main IDI categories in ECHO: Technical threat indicator, Intrusion attempt, Security alert, Vulnerability information, Vulnerability report, Incident report, TTP, Remediation actions, Asset, Discussion, Blog post, Poll, Raw data.
- ECHO information sharing model will be based on the following assumptions or premises:
    - IDIs have a clear and concise governance model, where each item is described by metadata to allow fine-grained decision making on the management and handling of the data
    - A clear process for on-boarding and off-boarding of participating organisations exists.
    - Organisations from the same sector have similar goals; form easier clusters for sharing threat intelligence information, and are more likely to reach consensus.
    - Stakeholders and participants are expected to join pre-defined and ad hoc groups.
    - Trust will be delivered through technical, organisational and human means.
    - The scope of IDIs should be extended to encompass Cyber Physical Systems; indicatively, this can consider the practices found in the Maritime Sector where there is a clear distinction between cyber (e.g. IT networks) and Physical (e.g. Operational Technology networks) highlighting the existence and interdependencies between the physical and cyber plane.
    - Translation and normalisation services allow the standardisation of IDIs. Taxonomies and schemas should cater for the verticals by including optional fields.
    - Existing standards for information processing and sharing are adopted wherever possible.
- The ECHO pilot is part of the EU initiative on establishing a network of competency centres, and aims to support information sharing among and between a multitude of sectors with Healthcare, Energy and Maritime being initially considered in this deliverable.
- A hybrid model architecture best fit the requirements following the cross-case analysis. In essence, the hybrid approach will allow to maintain a basic form of hierarchy, and at the same time it will allow the connection of different hubs, forming a higher level peer to peer. This is also in accordance to how CERTs operate and share information, which is done on a peer to peer basis but also within their level of operation (e.g. national, organisational, etc.). Allowing some degree of centralisation will also enable centralised decision making and support the emergence of Coordination Centres. A hub could represent a variety of communities, such as a specific sector, an interest group or a national point. It is recommended that each hub will refer to organisations of common characteristics, goals or sector, simplifying its management, internal governance and deployment complexity. This would be inline with the EWS architecture supporting tenants allowing also seamless integration through the sharing API capability that will connect EWS instances.
- From a governance perspective, the immediate consequence of this would be to have trust realms, two tiers of cross organisational boundaries.
- Information sharing stakeholders:
    - CERTS/CSIRTS

        - National/EU CERTS – protect national and critical infrastructure
        - ISP CERTS – protect Internet related services and backbone
        - Organisational CERTS – protect organisation
        - ICT Vendor CERTS – protect products
        - Academic CERTS – protect academic infrastructure, facilitate research and innovation
    - Public safety organisations: Law enforcement Agencies. These are secondary users that may be involved when handling incidents. As such, the E-EWS will allow the collection and preservation of evidence in a forensically sound manner.
    - Information sharing entities: Individuals, Researchers, Organisations, National, Private, Critical infrastructure, Research
- ECHO is underpinned by a series of privacy statements. These comply with the General Data Protection Regulation (GDPR) and are managed and overseen by the Data Controller and Data Protection Officer (DPO) for the project, RHEA System SA (RHEA).

Annexes

Annex 1 – Systematic literature review sources

This annex consists relevant sources and analysed documents concerning this deliverable.

Main research were made by using words and sentences; cybersecurity Information sharing, features of cyber exchange models, cybersecurity information sharing governance and sharing technologies for cybersecurity. After that in each case, the search queries like “cybersecurity information sharing” was entered with no temporal limitation. A query without quotation marks returns some variations, where the search engine allows for permutations and inflections.

Initial search in Springerlink returned 1612 results for “cybersecurity information sharing” within content computer science and it returns 31 researches with quotations as table TableA1 illustrates. There were few main tasks in the research: Identifying existing early warning systems and frameworks within public safety organisations, Identifying information sharing models and governance models in private and public safety organisations, Identifying features of cyber exchange models e.g. best practices and defensive measures and Different classification concerning phenomena like events, incidents, vulnerabilities threats and others.

Sharing technologies without word “cybersecurity” returned 517 results. Features of cyber information sharing models without quotations returned 279 results.

Item Title	Publication Title	Authors	Year
Network Externalities in Cybersecurity Information Sharing Ecosystems	Economics of Grids, Clouds, Systems, and Services	Zahid RashidUmara NoorJörn Altmann	2019
Risk Management Using Cyber-Threat Information Sharing and Cyber-Insurance	Game Theory for Networks	Deepak K. ToshSachin ShettyShamik SenguptaJay P. KesanCharles A. Kamhoua	2017
Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection	Critical Information Infrastructures Security	Alain MermoudMarcus Matthias KeuppSolange GhernaoutiDimitri Percia David	2017
Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance	Decision and Game Theory for Security	Deepak K. ToshIman VakiliniaSachin ShettyShamik SenguptaCharles A. KamhouaLaurent NjillaKevin Kwiat	2017
Distributed, Collaborative and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems	Cloud-Based Design and Manufacturing (CBDM)	J. Lane Thames	2014
Toward a Safer Tomorrow: Cybersecurity and Critical Infrastructure	The Palgrave Handbook of Managing Continuous Business Transformation	Solomon KarchefskyH. Raghav Rao	2017
IoT: Privacy, Security, and Your Civil Rights	Women Securing the Future with TIPPSS for IoT	Cynthia D. Mares	2019
Part 2: Legal and Regulatory Framework	Transatlantic Data Protection in Practice	Rolf H. WeberDominic Staiger	2017
Cybersecurity in the US: Major Trends and Challenges	The New US Security Agenda	Brian FonsecaJonathan D. Rosen	2017

Item Title	Publication Title	Authors	Year
Cyber Attacks, Prevention, and Countermeasures	Counterterrorism and Cybersecurity	Newton Lee	2015
Regulation of Cyberspace and Human Rights	Public International Law of Cyberspace	Kriangsak Kittichaisaree	2017
Toward a Holistic Approach of Cybersecurity Capacity Building Through an Innovative Transversal Sandwich Training	Industry Integrated Engineering and Computing Education	Jessica El MelhemAbdelaziz BourasYacine Ouzrout	2019
Frameworks and Best Practices	Cyber Resilience of Systems and Networks	Brianna KeysStuart Shapiro	2019
Economic valuation for information security investment: a systematic literature review	Information Systems Frontiers	Daniel SchatzRabih Bashroush	2017
Main Initiatives to Safeguard Cyberspace Sovereignty	Cyberspace Sovereignty	Binxing Fang	2018
Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?	Cybersecurity in the European Union	George Christou	2016
Learning quasi-identifiers for privacy-preserving exchanges: a rough set theory approach	Granular Computing	C. Wafo SohL. L. NjillaK. K. KwiatC. A. Kamhoua	2018
IT-Security in Critical Infrastructures Experiences, Results and Research Directions	Distributed Computing and Internet Technology	Ulrike Lechner	2019
Proposed Model for a Cybersecurity Centre of Innovation for South Africa	ICT and Society	Joey Jansen van VuurenMarthie GroblerLouise LeenenJackie Phahlamohlaka	2014
Trends in Cyber Operations: An Introduction	Current and Emerging Trends in Cyber Operations	Frederic Lemieux	2015
Cybersecurity in the U.S.	The Quest to Cyber Superiority	Nir Kshetri	2016
Sharing Cyber Threat Intelligence Under the General Data Protection Regulation	Privacy Technologies and Policy	Adham AlbakriEerke BoitenRogério De Lemos	2019
Vanishing Boundaries of Control: Implications for Security and Sovereignty of the Changing Nature and Global Expansion of Neoliberal Criminal Justice Provision	The Private Sector and Criminal Justice	Robert P. Weiss	2018
International Cyberspace Governance	World Internet Development Report 2017		2019
The Role of Blockchain in Underpinning Mission Critical Infrastructure	Industry 4.0 and Engineering for a Sustainable Future	Hamid JahankhaniStefan Kendzierskyj	2019
Cyber Attacks, Prevention, and Countermeasures	Counterterrorism and Cybersecurity	Newton Lee	2013
Interpretation of the Concept of "Cyberspace Sovereignty"	Cyberspace Sovereignty	Binxing Fang	2018
Dark Web: Deterring Cybercrimes and Cyber-Attacks	Technology-Enhanced Methods of Money Laundering	Fausto Martin De Sanctis	2019
Towards a Systematic View on Cybersecurity Ecology	Combatting Cybercrime and Cyberterrorism	Wojciech MazurczykSzymon DrobniakSean Moore	2016
More Than Humans	Digital Urban Acupuncture	Salvatore IaconesiOriana Persico	2017

Item Title	Publication Title	Authors	Year
Digital Security – Wie Unternehmen den Sicherheitsrisiken des digitalen Wandels trotzen	Digitalisierung in Industrie-, Handels- und Dienstleistungsunternehmen	Alexander Weise	2018

Table A1*:* Relevant Springelink research publications

IEEE Xplore returned 147 results by using words: *cybersecurity, information* and *sharing* together. We got access to 129 files data: Conferences (82), Journals (28), Magazines (16), Courses (15), Early Access Articles (3), Books (2). *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 same, as Table A2 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; D. K. Tosh; S. Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017
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; D. K. Tosh; S. Sengupta	MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)	2017
Attribute based sharing in cybersecurity information exchange framework	I. Vakilinia; D. K. Tosh; S. Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017
Privacy-preserving cybersecurity information exchange mechanism	I. Vakilinia; D. K. 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 A2: Specified IEEE returns

JYKDOC returned 9 results by using words: cybersecurity, information and sharing together. “We got access to 9 files data. Separate words cyber exchange models returned 22 results. ”information sharing technologies” returned 268 results.

AI tool “iris” requires title of research question and problem statement. We have used follow words to describe our 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. Identifying information sharing models. Identifying features of cyber exchange models. Early warning solution will deliver a secure sharing support tool for personnel to coordinate and share information in near real time. It will support information sharing across organisational boundaries and provide sharing of both general cyber information as a reference library. It will also ensure secure connection management from clients accessing the early-warning system.”* AI tool “IRIS” returned 270 results by using following words in title: cybersecurity, information and sharing together as Figure A1 illustrates. Almost all were relevant material. The system calculates the relevance percentage for the results. All relevant results were between 78% and 95%.

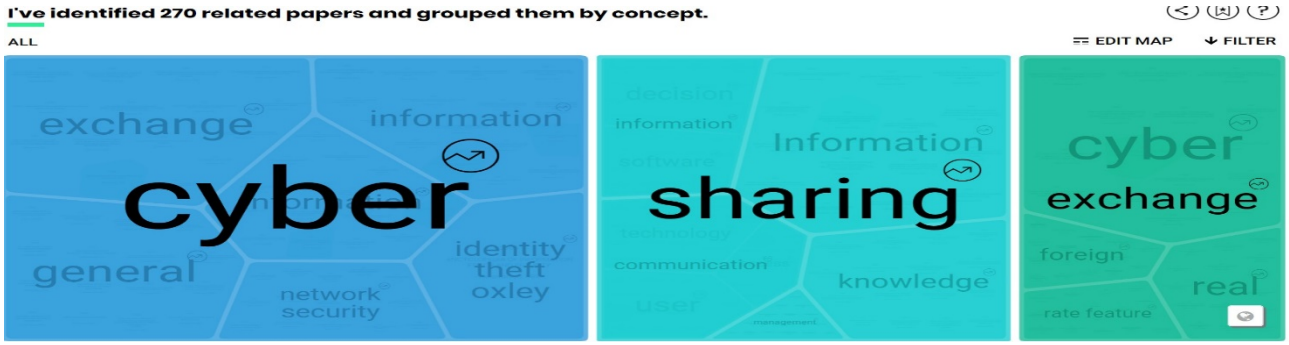

Figure A1*:* Identified papers by AI tool IRIS

Several studies were based on fundamental level public-related sources, which formed the main frame of the research. Most relevant public-related documents in this research are follows:

- Department of Homeland Security, "NIPP 2013 - partnering for critical infrastructure security and resilience," DHS, U.S., 2013.
- MITRE, "Trusted Automated eXchange of Indicator Information — TAXII™ Enabling Cyber Threat Information Exchange," 2018.
- NIST, "Guide to cyber threat information sharing," National Institute of Standards and Technology, Gaithersburg, Tech. Rep. NIST Special Publication 800-150, 2016.
- Johnson et al, "Guide to cyber threat information sharing. NIST special publication (NIST SP) 800–150." NIST, 2016.
- OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C), "TAXII™ version 2.0. committee specification 01," OASIS Open, Tech. Rep. taxii-v2.0-cs01, 2017.
- OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C), "STIX™ version 2.0. part 2: STIX objects," OASIS open, Tech. Rep. stix-v2.0-wd03-part2-stix-objects, 2017.

Annex 2 – Analysed information sharing and trust models: technologies and frameworks

The systematic review of scientific articles included studies and evaluations of hundreds of information sharing and trust models. During the case studies, the following technologies, structures, models and frameworks were analysed in more detail:

- Structured Threat Information eXpression (STIX™)
  STIX 1.1.1: https://stixproject.github.io/about/
  STIX 2.0: https://oasis-open.github.io/cti-documentation/
- Malware Attribute Enumeration and Characterization (MAEC™)
  MAEC 5.0: https://maecproject.github.io/
- Incident Categories
  FIRST CASE Classification: www.first.org
- Traffic Light Protocol (TLP)
  TLP 1.0: https://www.first.org/tlp/
- NATO Cyber Rapid Reaction Team (RRT) that protect its critical infrastructure.
- NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)
- European Public-Private Partnership for Resilience (EP3R)
- Schengen Information Systems (SIS)
- European Information Exchange Model (EIXM)
- Europol's Secure Information Exchange Network Application (SIENA); enables authorities to exchange information with each other, with Europol, and with a number of third parties.
- U.S. Information Sharing and Analysis Center (ISAC) for telecommunications
- Communications Information Sharing and Analysis Center (Comm-ISAC)
- EU-U.S. Privacy Shield
- ENISA: ISAC member driven organisation model. (Country-Focused ISAC, sector-specific ISAC and International ISAC) - Sharing knowledge about incidents.
- ENISA PPP – cooperative model incident handling and crisis management.
- NIST Cybersecurity Framework
- MITRE: CORA (Cyber Operations Rapid Assessment)
- MITRE: TISCO Threat-informed model
- UN-NATO information sharing International organisation as UN (United Nations) and NATO are the connecting factors concerning harmonization of information sharing procedures in the EU and USA and between them
- UN-NATO-EU-USA information sharing
- NIST: RAF (Risk Assessment Framework)
- NIST: RMF (Risk Management Framework)
- CYBersecurity information EXchange with Privacy (CYBEX-P) ; a structured information sharing platform with integrating privacy-preserving mechanisms.
- Cyberx industrial cybersecurity platform
- CybOX - The Cyber Observable eXpression. Standadised language
- TAXII Trusted Automated eXchange of Indicator Information
- OpenIOC an open framework for sharing threat intelligence information
- VERIS The Vocabulary for Event Recording and Incident Sharing
- MAEC Malware Attribute Enumeration and Characterization
- SCAP Methods and components e.g. for using automated vulnerability management
- IODEF Incident Object Description Exchange Format
- MARISA Maritime Information sharing model and toolkit developed by MARISA project

- RANGER Surveillance platform that will offer features for the information sharing
- Health Information Exchange (HIE)
- Laboratory information system (LIS)
- EUCISE Information Sharing between the maritime authorities
- Trust models in national level
- Trust models in cross boarding situations
- Cyber information sharing between situation centers
- Cyber information sharing within emergency response procedures
- National cyber-threat prevention mechanism HAVARO 1.0
- National cyber-threat prevention mechanism HAVARO 2.0
- The EaP Rapid Response Mechanism for civil society organisations
- Information Against Hate Crimes Toolkit (INFAHCT)
- The Camden Asset Recovery Inter-Agency Network (CARIN)
- The Egmont Group of Financial Intelligence Units - a network of financial intelligence units from all States
- The Global Focal Points Initiative (GFPI) – INTERPOL
- The Stolen Asset Recovery Initiative (StAR)
- Mutual legal assistance (MLA) for the G7 and G20 countries
- Cyber Information Sharing and Collaboration Program (CISCP)
- The Critical Infrastructure Key Resources (CIKR)
- CRAMM - CCTA Risk Analysis and Management Method is a risk management methodology
- OCTAVE - Method for the define and share threat information between the teams within the organisation
- SOMAP - The Security Officers Management & Analysis Project
- OGRCM3 - Open Governance, Risk and Compliance Maturity Management Methodology

Annex 3 – CISE as a tool for sharing sensitive cyber information in maritime domain

by J. Rajamäki, I. Tikanmäki & J. Räsänen

In vol. 43 of Information & Security: An International Journal, https://doi.org/10.11610/isij.v43

Information & Security

J. Rajamäki, I. Tikanmäki & J. Räsänen,
vol. 43, no. 2 (2019): 215-235
https://doi.org/10.11610/isij.4317

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain

Jyri Rajamäki (✉), Ilkka Tikanmäki, Jari Räsänen

Laurea University of Applied Sciences, https://www.laurea.fi/en/

ABSTRACT:

The ECHO project aims at organizing and coordinating an approach to strengthen proactive cyber security in the European Union through effective and efficient multi-sector collaboration. One important tool for this aim is the ECHO Early Warning System (E-EWS). The development of the E-EWS will be rooted in a comprehensive review of information sharing and trust models from within the cyber domain, as well as models from other domains. In 2009, the Commission adopted a Communication Towards the integration of maritime surveillance in the EU: "A common information sharing environment for the EU maritime domain (CISE)," setting out guiding principles towards its establishment. The aim of the COM(2010)584 final was to generate a situational awareness of activities at sea and impact overall maritime safety and security. As a outcome of COM(2010)584 final, the EUCISE2020 project has developed a test-bed for maritime information sharing. This case study analyses information sharing models in the maritime domain, the EUCISE2020 test bed and the CISE itself as an alternative for cyber information sharing system. The maritime sector represents a suitable research case because it is already digitized in many aspects.

ARTICLE INFO:

RECEIVED: 08 MAY 2019
REVISED: 28 AUG 2019
ONLINE: 22 SEP 2019

KEYWORDS:

information sharing, maritime surveillance, early warning, cybersecurity, ECHO project

Introduction

Cybersecurity is critical to both our prosperity and our security, because our daily lives and economies become increasingly dependent on digital technologies.[11] The main prerequisite towards cybersecurity is situational awareness (SA). Without

✉ E-mail: jyri.rajamaki@laurea.fi

cyber SA, it is impossible to systematically prevent, identify, and protect the system from the cyber incidents and if, for example, a cyber-attack happens, to recover from the attack. SA involves being aware of what is happening around your system to understand how information, events, and how your own actions affect the goals and objectives, both now and in the near future. It also enables to select effective and efficient countermeasures, and thus, to protect the system from varying threats and attacks. From research point of view, some aspects of the cyber SA area are more mature than others: there is plenty of work dedicated to cyber SA in industrial control systems, but less research has been devoted to areas such as information exchange and sharing for cyber SA.[12]

On the other hand, sharing of proper cyber SA information is the key element of cybersecurity,[5] and it has been noticed recently by public administrations. In the U.S., two laws about sharing the information on cyber SA were recently signed: The Cybersecurity Information Sharing Act requires the parties to develop procedures for sharing threat information of cyber security between different stakeholders, whereas the Cyber Intelligence Sharing and Protection Act obliges the parties to provide sharing of situational information of cyber threats in real-time between nominated stakeholders. The European Commission notes that "cooperation and information sharing between the public and private sectors faces a number of obstacles. Governments and public authorities are reluctant to share cybersecurity-relevant information for fear of compromising national security or competitiveness. Private undertakings are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules. Trust needs to be strengthened for public-private partnerships to underpin wider cooperation and sharing of information across a greater number of sectors. The role of Information Sharing and Analysis Centres is particularly important in creating the necessary trust for sharing information between private and public sector. Some first steps have been taken in respect of specific critical sectors such as aviation, through the creation of the European Centre for Cybersecurity in Aviation, and energy, by developing Information Sharing and Analysis Centres. The Commission will contribute in full to this approach with support from ENISA, with an acceleration needed in particular with regard to sectors providing essential services as identified in the NIS Directive."[11]

The ECHO (European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations) project started in 2019. It aims at organizing and coordinating an approach to strengthen proactive cyber security in the European Union, through effective and efficient multi-sector collaboration. One important tool for this aim is the ECHO Early Warning System (E-EWS). The development of the E-EWS will be rooted in a comprehensive review of information sharing and trust models from within the cyber domain, as well as models from other domains. This paper analyses information sharing models in maritime sector that is already digitized on many aspects, and it continues its digital transformation, at the same pace as the rest of the world. This sector includes various activities such as:

- Shipping (bulk, liquid, gas, containers, RO-RO);

- Passengers transportation and cruises (over 20 million passengers in 2013);
- Ports and Shipyard;
- Fishing and related activities, Offshore platforms, Renewables Maritime Energies and Submarine cables.

The sum of these activities makes up a major economic sector and, in some cases, belongs to the domain of strategic activities for the survival of the nation. Marine Transportation System (MTS) is a major component of the world's overall transportation and energy system. It is a dominant factor in the global supply chain that connects businesses and individuals all over the world. U.S. economic prosperity is highly dependent upon maritime trade and the ships, boats, terminals, and related maritime critical infrastructure that support their many tributaries. According to the U.S. Maritime Administration, waterborne cargo and associated activities contribute more than $ 649 billion to the U.S. Gross Domestic Product (GDP) sustaining more than 13 million jobs. Many thousands of vessels, from tugs and barges to ocean going ships complete this system. By volume, over 90 % of U.S. overseas trade travels by water.[24] At the international level, the maritime domain is in full growth and sustains a worldwide economy of 1.5 trillion euros. The stakes are huge and the increasing digitization of this domain will increase the cyber risk. As early as 2011, ENISA, in a report on maritime cybersecurity, rung the alarm bell on the massive under protection of maritime systems.[8] The US Coast Guard and other authorities have document-ed cyber-related impacts on technologies ranging from container terminal operations ashore to offshore platform stability and dynamic positioning systems for offshore supply vessels.[24]

This paper unfolds as follows. Section 2 includes a quick summarization of the field's knowledge about this research topic. Section 3 outlines the case study method used in this study. Section 4 contains the main contribution: analysis of information sharing models as may be applied to the ECHO Network including related trust models and needs for granular control of information sharing and information distribution in maritime sector. The findings are discussed and concluded in Section 5.

Related Work

Information Sharing in Maritime Domain

Maritime surveillance is essential for creating maritime awareness, in other words "knowing what is happening at sea." Integrated maritime surveillance is about providing authorities interested or active in maritime surveillance with ways to exchange information and data. Support is provided by responding to the needs of a wide range of maritime policies – irregular migration/border control, maritime security, fisheries control, anti-piracy, oil pollution, smuggling etc. Also, the global dimension of these policies is addressed, e.g. to help detect unlawful activities in international waters. Sharing data will make surveillance cheaper and more effective. Currently, EU and national authorities responsible for different aspects of surveillance, e.g. border control, safety and security, fisheries control, customs, environment or defence, collect data separately and often do not share them. As a

result, the same data may be collected more than once. A common information-sharing environment (CISE) is currently being developed jointly by the European Commission and EU/EEA member states with the support of relevant agencies such as the EFCA. It will integrate existing surveillance systems and networks and give all those authorities concerned access to the information they need for their missions at sea. The CISE will make different systems interoperable so that data and other information can be exchanged easily through the use of modern technologies.

Cybersecurity Information Sharing Governance Structures

Almost all the business areas are using networked systems or services and the services provided by globally interconnected, decentralized IT systems and networks, the cyberspace, play a prominent role in our world. Cyberspace reaches all corners of human access and encompasses all interconnected devices into one large virtual entity. To understand the complexity and issues associated with cybersecurity, one must be knowledgeable about the evolution and growth of cyberspace, and the fact that cyberspace is mostly unregulated and uncontrolled.[19] Cyber threats, cyberattacks, or more commonly intrusions, might affect to the continuity of business in all sectors. The dilemma of digitalisation poses the requirement for comprehensive situational awareness in cyber security as a backbone for decision making. The dependence on these services requires the high-level security of cyberspace that can be ensured by a broad cooperation of different organisations. Information sharing is a vital component of cyber risk management, and has benefits in both preventing incidents, and managing them when they do occur. The actors sharing or exchanging information related to cyber intrusions would use it as an early warning information for immediate intrusion mitigation and threat response activities. Of course information sharing can also be useful after an incident. “Zero Day Attacks” are attacks that exploit previously unknown vulnerabilities. Reporting these incidents can help spread the word to others and enable them to prepare. Reporting incidents to trade associations, regulators, and others may also provide access to mitigation measures.[24] The systematic review of the literature with regard to cyber SA by Franke and Brynielsson found that one way of gaining increased cyber SA is to exchange information with others.[12] Table 1 summarises their findings in that area. Successful and efficient cooperation cannot be achieved without a similar level of information exchange between the actors, and their IT systems that requires interoperability of these systems.[20] Information exchange receives much attention in the national strategies. Information related to cyber threat is often sensitive and might be classified, so when that information is shared with other organisations, there is a risk of being compromised.[18]

Information sharing among industry peers, and with government agencies, can allow a company to identify possible vulnerabilities in their systems, anticipate attacks, and provide access to software patches and other mitigation tools. Some reports indicate that as much as 8 % of successful cyber breaches are in part preventable in that they exploit known vulnerabilities for which software patches

Table 1. Articles with regard to cyber SA information exchange.

Article	Content
Klump and Kwiatkowski [16]	An architecture for information exchange about incidents in the power system.
Hennin [14]	Sharing of information about suspicious IP addresses.
Brunner, et al.[3]	Principled problems as they ponder the trade-off between the increased awareness gained by sharing data and the loss of privacy entailed. Combining peer-to-peer networking and traceable anonymous certificates, they propose a collaborative and decentralized concept for an exchange platform.
National Coordinator for Security and Counterterrorism [21]	The Netherlands find "information-exchange between the various players" to be "of the utmost importance" for fighting cybercrime.
Australian Government, Attorney-General's Department [1]	The Australian government strives to foster "more intensive trusted information exchanges with high risk sectors to share information on sophisticated threats", aiming primarily at telecommunications, banking and finance, and owners of industrial control systems.
Cyber Security Strategy Committee, Ministry of Defence [4]	Estonia highlights the importance of exchanging expert information within the frameworks of the international network of national CERTs, the network of government CERTs, Interpol, Europol and organizations dealing with critical information infrastructure protection.

have been available for at least a year.[24] There are different types of cybersecurity-related information that could be shared to improve cybersecurity defences and incident response. Munk divides this information into four major groups: information related to events, to vulnerabilities, to threats, and other information.[20] The classification proposed by Sedenberg and Dempsey [23] includes incidents (including attack methods), best practices, tactical indicators, vulnerabilities, and defensive measures. According to them, organizations are engaged in sharing tactical indicators ("indictors of compromise", IOCs). IOCs are artefacts that relate to a particular security incident or attack, such as filenames, hashes, IP addresses, hostnames, or a wide range of other information. Cybersecurity defenders may use IOCs forensically to identify the compromise or defensively to prevent it.[23]

Sedenberg and Dempsey [23] identified seven different cyber information sharing models in the U.S. that are summarised in Table 2. Their taxonomy of cybersecurity information sharing structures may help illustrate how different design and policy choices result in different information sharing outcomes. Based on the governance models described, they identified a set of factors or determinants of effectiveness that appear in different cybersecurity information sharing regimes.[23]

Table 2. Taxonomy of Information Sharing Models.[23]

Classification	Organizational Units	Example Organizations	Governance types
Government-centric	Government operated; private sector members can be corporations, private sector associations (e.g., ISACs), non-profits (e.g., universities), or individuals	DHS AIS; US-CERT; ECTF; FBI's e-guardian; ECS	Federal laws and policies; voluntary participation; Rules range from open sharing subject to traffic light protocol or FOUO (for official use only) to classified information restrictions (ECS)
Government-prompted, industry-centric	Sector or problem specific	ISACs; ISAOs	Sector or problem specific; voluntary participation; generally organized as non-profits, use terms of service or other contractual methods to enforce limits on re-disclosure of information
Corporate-initiated, peer-based (organizational level)	Specific private companies	Facebook ThreatExchange; Cyber Threat Alliance	Reciprocal sharing; closed membership; information controlled by contract (e.g., ThreatExchange Terms and Conditions)
Small, highly vetted, individual-based groups	Individuals join, take membership with them through different jobs	OpSec Trust; secretive, adhoc groups	Trust based upon personal relationships and vetting of members; membership and conduct rules
Open-source sharing platforms		Spamhaus Project	Information published and open to all; no membership but may be formed around community of active contributors and information users; one organization may manage platform infrastructure
Proprietary products	Organization or individuals participate by purchasing the product	AV and firewall vendors	Information via paid interface; responsibility and security management still in house
Commercialized services	Organizations purchase service	Managed Security Service Providers	Outsourcing of security

Always, when dealing with information exchange and sharing, the main question is "trust."[22] The lack of trust in information propagation is the key to a lack of robust security.[19] Lack of trust is the primary reason cyber vulnerability and threat data is not shared within and between the public and private sectors.[13] Sedenberg and Dempsey [23] identify that trust within cybersecurity information sharing must

be bidirectional, meaning that 1) the sharing entity needs to trust that the information will not be used against it for regulatory or liability purposes, obtained by adversaries and exploited against it as a vulnerability, or disclosed publicly to hurt the reputation of the sharer; and 2) the recipient of information needs to trust the integrity of the information shared. Also, reciprocity is important; parties need to trust that other participants will contribute roughly equivalent information.[23]

Reporting to law enforcement and government agencies is required in some industries, and can help public servants "connect the dots" if there is a pattern to attacks that suggests further attacks (including physical attacks) are likely, or can help authorities identify the perpetrators.[24] In the U.S., the Cybersecurity Information Sharing Act (CISA) attempts to alleviate trust burdens that accompany sharing private sector information with the government, by limiting public disclosure through Freedom of Information Act (FOIA) and by offering protections against liability and regulation. Sedenberg and Dempsey [23] found no evidence to indicate that CISA has succeeded in encouraging increased cybersecurity information sharing, and their research highlights some of the limitations of the statute's approach: "By focusing on concerns over liability exposure, especially related to privacy laws, CISA failed to take into account other issues relevant to the sharing of private sector data with the federal government in a post-Snowden reality—particularly issues of public perception. Aside from the negative implications of sharing with the government, CISA did not account—and perhaps no law could account—for companies' fears about the reputational harm they might incur should their vulnerability become publicly known, or their fears about future attacks if vulnerabilities fall into the wrong hands. If indeed CISA has failed to induce more cybersecurity information sharing, it may be because it did not take into account these foundational elements of trust." Sedenberg and Dempsey [23] research points toward a clear trade-off between membership size and the amount and sensitivity of information shared: "Governance and policy structures can generate trust by limiting membership with some level of vetting and by requiring active participation. These dimensions of trust should be taken as governance design choices that can be worked into any organizational structure."

Sharing Technologies for Cyber Security Information

Kokkonen et al. implement and evaluate a model for creating the information sharing communities for the cyber security situational awareness information.[18] Table 3 presents the most popular technical standards for sharing the information of cyber security required in cyber situational awareness.

The U.S Department of Homeland Security uses a system called Automated Indicator Sharing for providing the bidirectional sharing of the cyber security threat indicator information utilizing TAXII™ capability and STIX™profile.[18] Figure 2 demonstrates STIX™ use cases where also cyber security information sharing between organisations is implemented.[2]

Table 3. Technical standards for sharing cyber information.

Standard	Description
Structured Cyber Observable eX-pression (CybOX™) https://cybox.mitre.org/about/	A language for standardized structured information of cyber observables. It is not targeted at a single cyber security use case but to be flexible for offering a common solution for all cyber security use cases requiring the ability to deal with cyber observables. By specifying a common structured schematic mechanism for cyber observables, the intent is to enable the potential for detailed automatable sharing, mapping, detection and analysis heuristics.
Threat Information eXpression (STIX™), https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf	A language for standardized structured communication of cyber threat information for improving interoperability and cyber security situational awareness. It consists of eight constructs, which are utilized to the XML schema: Observable, Indicator, Incident, TTP (tactics, techniques, and procedures), ExploitTarget, CourseOfAction, Campaign and Threat-Actor (see Fig. 1).
Trusted Automated eXchange of Indicator Information (TAXII™), https://www.mitre.org/sites/default/files/publications/taxii.pdf	A framework for exchanging cyber threat information that determines the set of messages, protocols, and services. It supports following information sharing models: hub-and-spoke, peer-to-peer and source-subscriber.

Kokkonen and co-authors have developed a model for constructing the topology of the information sharing community.[18] Their model is based on the assumption: a predefined risk level exists for sharing the information between organisations. They use TAXII™ peer-to-peer information sharing model with STIX™ architecture; risk level values are required to have the same scale and organisations are sharing information only to trusted partners. Figure 3 presents a real-life scenario applying this model: Three different national CERTs act as the highest national authority, the national and international Internet Service Providers (ISPs) act as the next level and the lowest level of information sharing organisations are various national and international enterprises. Every peer-to-peer TAXII™ link has risk level value of [1, 20], where the risk values are defined as 1 = min-risk and 20 = max-risk. Fig. 4 shows the information sharing topology with a minimum risk level implementation applying Dikstra's shortest path algorithm. Even if there are no direct connections between all the organisations, the data flow still goes to every organisation in that community.[18]

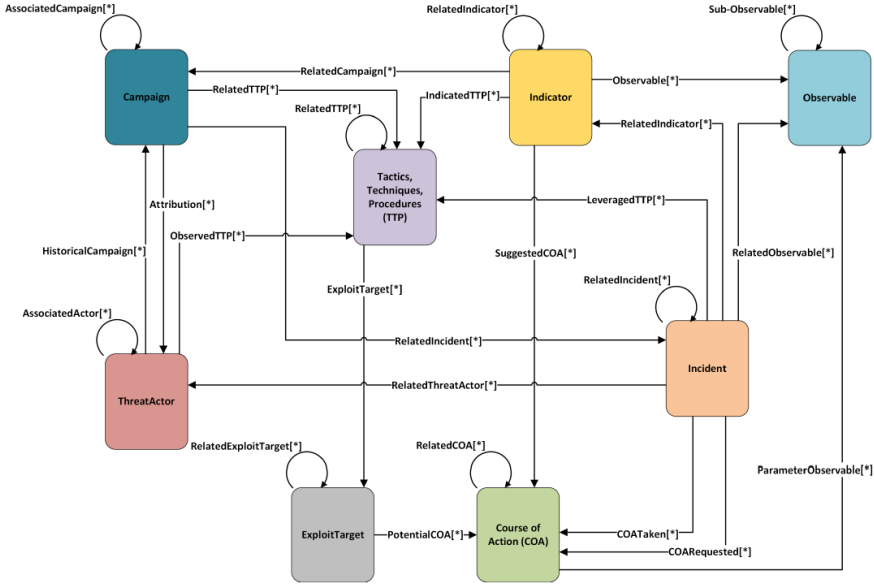

Figure 1: Architecture of STIX™.[18]

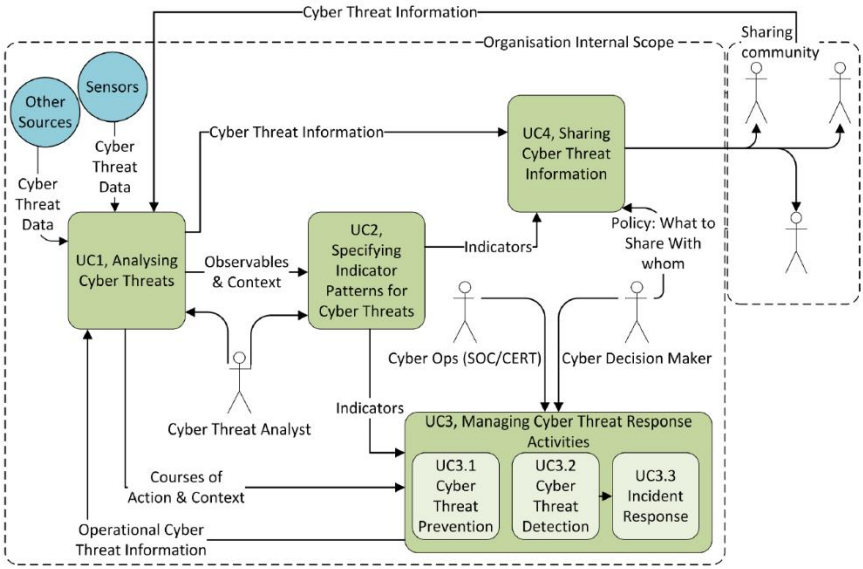

Figure 2: Example of STIX™ use case.[18]

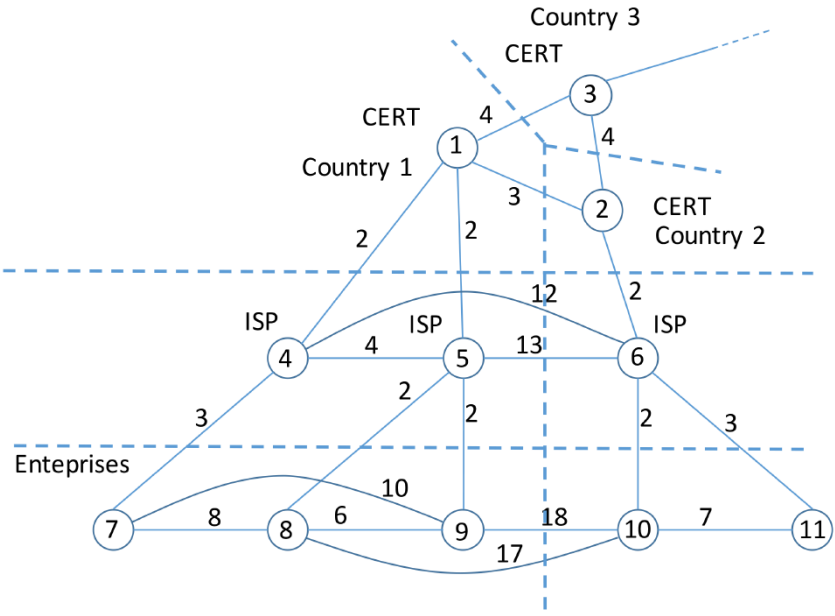

Figure 3: Cyber security information sharing community.[18]

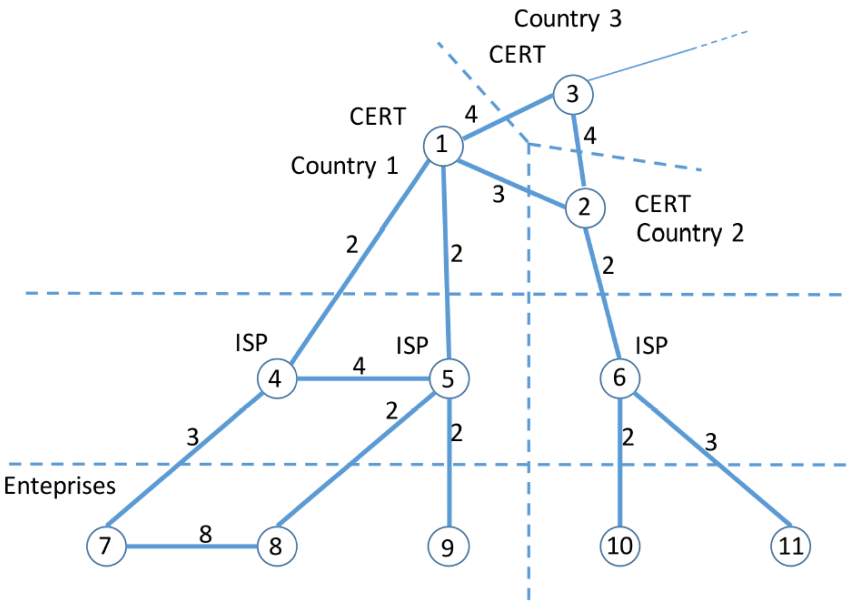

Figure 4: Cyber security information sharing topology with a minimum risk level implementation.[18]

The Forum of Incident Response and Security Teams (FIRST) has released Traffic Light Protocol (TLP) that facilitates a four-colour category for information sharing (red, amber, green, white). Red means "not for disclosure, restricted to participants only" and the meaning of white is "disclosure is not limited." The TLP categories can be applied as a part of information sharing rules and topology construction for filtering data between organisations.[17]

Cyber Information Sharing in Maritime Domain

Cyberspace in the maritime domain comprises ports and harbours, shipping, offshore facilities, and autonomous ships, and the satellites that keep these systems connected to the deepest depths of the ocean where autonomous underwater vehicles navigate.[19] The global maritime system—including all civilian, commercial, and military ship traffic—is a system of systems, in which each system can be described as a set of components and the communication pathways between those components.[15] The maritime transportation system is increasingly a target of cyberattacks.[15] The ECHO project's maritime sector use case focuses on the commercial ship that is itself a complex cyber-physical system (CPS) with a large variety of communication systems for crew, passengers, external sources, and internal operations. According to Kessler et al.,[15] the ship's CPS includes:

- Bridge Navigation Systems (e.g., GPS, Electronic Chart Display and Information System /ECDIS/, AIS, LRIT)
- External Communication Systems (e.g., satellite communications, FleetBroadband, Internet)
- Mechanical Systems (e.g., main engine, auxiliary engine, steering control, ballast management)
- Ship Monitoring and Security Systems (e.g., closed-circuit television, Ship Security Alert System /SSAS/, access control systems, sensors)
- Cargo Handling Systems (e.g., valve remote control systems, level/pressure monitoring systems)
- Other specialized networks (e.g., Combat Command & Control Systems on warships, Entertainment Systems and Point-Of-Sale terminals on passenger vessels; Vessel Management Systems on commercial fishing vessels).

The maritime industry has a long history of success in risk management. While physical and personnel risks are relatively easy to identify, cyber risks pose a unique challenge.[24] In modern ships, IT technology and operational technology (OT) on board are networked and highly integrated, so in order to maintain the naval survivability main aspects (susceptibility, vulnerability, recoverability), the underlying IT Infrastructure must be designed to assure the cyber security triad (availability, confidentiality and integrity) of any information and IT service, application, industrial control. The starting point is *a cyber-risk assessment* of the IT infrastructure, of the organization and of the available operators' skill, in order to evaluate the risk posed by the cyber threats or change on the services in all the

possible operational conditions and finds, in each case, the most appropriate strategy of prevention, control and reaction. The scope of the risk management must encompasses all digital systems on vessels. These systems can be divided in two main categories: 1) the IT networks, the hardware and software dedicated to manage and to exchange information; and 2) the Operational Technology (OT) networks, the hardware and software dedicated to detecting or causing changes in physical processes through Industrial Control Systems which direct monitor and control the physical devices such as engines, rudder, valves, conveyors, pumps, etc.[6]

When the cyber risks are recognized, the organization can select mitigation strategies to reduce that risk. Policy enforcement controls required for risk mitigation that include Technical Cyber Security Controls and Procedural controls. The Cyber Security policy adopted should be defined and distributed over five different levels: Secure by Design, Access Control Management, Proactive Protection, Continuous Threat Monitoring and Disaster Recovery Procedure.[6]

Study Methods

This case study analyses the information sharing models applied in maritime domain. The purpose of the paper is to be a background study for the development of a secure sharing support tool enabling personnel to coordinate and share cyber-sensitive information in near real time. The applied research methods are case study research in general,[25] and in the cyber security domain.[7] The main research question is "how can cyber information sharing models be understood in maritime domain?"

Research data was collected during the EUCISE2020 project in which all the authors participated in different roles, as well as the following documents:1) reports of CooP, MARSUNO and BlueMassMed projects, 2) EUCISE DOW, 3) EUCISE2020 D8.3 Dissemination plan with Policy recommends and governance model, 4) EUCISE2020 Technical documents stored in EUCISE2020 intranet, 5) Discussions with The Finnish Transport Infrastructure Agency and Finnish Boarder Guard (FBG) representatives (April 17, 2019; April 25, 2019).

In addressing the research question presented above, the qualitative data analysis was continuously involved in organising, accounting for, and explaining the collected data, and making sense of the data in terms of situation, themes, categories, entities, relations, and regularities.

Study Results

Who are the Main Shareholders of Sensitive Cyber Information Sharing in the Maritime Domain?

On 15 October 2009 the European Commission adopted a "Communication Towards the integration of maritime surveillance in the EU: A common information sharing environment for the EU maritime domain (CISE),"[9] setting out guiding principles towards its establishment. The aim of COM(2010) 584 final was to "*generate a situational awareness of activities at sea*" and impact overall maritime safety

and security. The aim of the integrated maritime surveillance is to increase sectoral maritime awareness pictures of the EU's and European Economic Area (EEA) States' sectorial user communities cross-sectoral and cross-border. COM(2010) 584 final identified members of the Common Information Sharing Environment (CISE) and named CISE members as User Communities. Following functions were performed: 1) Maritime Safety including Search and Rescue (SAR) and prevention of pollution caused by ships; 2) Fisheries control; 3) Marine pollution preparedness and response in Marine environment: 4) Customs; 5) Border control; 6) General law enforcement; and 7) Defence. These User Communities are the shareholders of sensitive cyber information sharing in maritime domain.[9]

Function 1 Maritime safety is covered by the European Vessel Traffic Monitoring Directive and the system is operational. Function 2 Fisheries control's main initiatives are Fisheries Information System and Vessel monitoring System. Function 3 Marine environment use, among other systems, European Marine Observation and Data Network (EMODNet) and European platform for maritime data exchange named CleanSeaNet. Function 4 Customs have European Customs Information System (CIS), Customs Risk Management system and DG TAXUD managed Common Communication Network and Common Systems Interface (CCN/CSI). Function 5 Border control is covered by European Border Surveillance System (EUROSUR) and Visa Information System (VIS). Function 6 General Law enforcement is covered by internal security responsibilities dealt with European Law Enforcement Agency (EUROPOL) and other agencies. Systems used for General Law enforcement are Secure Information Exchange Network Application (SIENA), Europol Information System (EIS), and Europol Platform for Experts (EPE) and the Schengen Information System (SIS). Function 7 Defence improve maritime picture by linking existing military networks and systems.[10]

Table 4 introduces User Communities' EU wide organisations and their used IT systems. It presents only European level organisations and their IT systems. However, there are many regional and national systems in use.

How Can the CISE Environment be Applied for Sharing Sensitive Cyber Information in the Maritime Domain?

Political consensus and common understanding of information sharing necessity has been build up among EU maritime authorities during several cooperation projects, e.g. BluemassMed, MARSUNO and CoopP. The CISE environment could be applied for sharing the sensitive cyber information by following the CoopP and EUCISE 2020 projects. CoopP support the first phase where the overall objective of the Cooperation Project was to support further cross-border and cross-sector operational cooperation between public authorities (including EU Agencies) in the execution of the defined maritime functionalities, with a focus on information sharing across sea-basins.

The information sharing cooperation was to be envisaged in the context of operational situations (use cases), and identify needs for improved information exchanges and the associated costs and benefits. In concrete terms the project was

Table 4. European wide User Communities' organisations and used IT systems.

User Community	EU organisation	System(s)
Maritime safety & security	European Maritime Safety Agency (EMSA)	EU Vessel traffic information (SafeSeaNet), Long-range identification and tracking (LRIT), Thetis, alert and notifications application (CECIS)
Fisheries control	European Fisheries Control Agency (EFCA)	EFCA Fisheries Information System (Fishnet collaboration tool, Vessel monitoring System (VMS), EFCA Electronic Recording and Reporting System, EFCA Electronic Inspection Report System)
Marine environment	European Environment Agency	The European Marine Observation and Data Network (EMODNet), European Pollutant Release and Transfer Register (E-PRTR), Shared Environmental Information System (SEIS), CleanSeaNet, European system for monitoring the Earth (Copernicus)
Customs	EU taxation and customs union DG TAXUD	European Customs Information System (CIS), Customs Risk Management system, Common Communication Network and Common Systems Interface (CCN/CSI)
Border Control	European Border and Coast Guard Agency (FRONTEX)	European Border Surveillance System (EUROSUR), the Visa Information System (VIS)
General law enforcement	European Union Agency for Law Enforcement Cooperation (EUROPOL)	Secure Information Exchange Network Application (SIENA), Europol Information System (EIS), Europol Platform for Experts (EPE), The Schengen Information System (SIS)
Defence	European Defence Agency (EDA)	Maritime Surveillance (MARSUR)

meant to define a number of information services and their data specifications (i.e. common data formats and common semantics) which may not be dependent upon existing systems.

Overall Objectives were to be accomplished by executing the Specific Objectives, namely defining and agreeing on a selection of use cases with related information services and attached access rights, defining common data formats and semantics, and contributing to the cost-benefit analysis of Integrated Maritime Surveillance.

The second phase of applying the CISE for sharing the sensitive cyber information could be to follow the EUCISE2020 project and utilized the solution build during the EUCISE2020 project. EUCISE 2020 is a Security Research project of the European Seventh Framework Program, which aims to achieve the pre-operational Information Sharing between the maritime authorities. EUCISE2020 is one important milestone for implementation of the European CISE – Common Information Sharing Environment.

EUCISE2020 project built and tested the Test-Bed for maritime information sharing. The test-bed includes both unclassified and classified network but only the unclassified network is online. The technical specification for the classified network exist and the system has been tested during the Factory Acceptance Test. The security level of the classified solution is EU-Restricted but after all the level is matter of crypto device and network solution. Both networks are equal, the only difference is the crypto device which encrypts the information before sending it in the EUCISE2020 Virtual Private Network (VPN).

In theory, EUCISE2020 test-bed could be applied for sharing cyber information while the main goal of the EUCISE2020 network is to allow data exchange among the Legacy Systems (LS). This section includes a short introduce to EUCISE2020 Test-Bed infrastructure and services for supporting the discussion how it could be applied to cyber information sharing.

The Legacy Systems participate in the exchange of information by providing and receiving data and services; they are the fundamental elements of the CISE environment, but are considered elements external to the EUCISE2020 network. The EUCISE2020 system configurations include the following components:

- CISE adaptor allows a LS to connect to a CISE Gateway (GW). It translates the LS data into the common CISE Data Model and adapts the internal protocol of the LS into the protocol of the GW.
- CISE Gateway implements the CISE messaging and network protocols to exchange data with the CISE adaptor and with the other CISE Gateways/ Nodes.
- CISE Node (NODE) is an enhanced gateway, capable of performing added values services such as data fusion and storing of information.

The services implemented by the EUCISE2020 are grouped into the following categories:

- Core Services are infrastructure services that provide common facilities. These services are devoted to enables the connection of the EUCISE2020 Participants through the EUCISE2020 Network. Transferring data among EUCISE2020 Participants and allowing the availability of pertinent data to EUCISE2020 services.
- Common Services are application services that provide the capability to exchange data in the EUCISE2020 Network. Consequently, these services manage EUCISE2020 data model entities.
- Advanced Services are application which compose and orchestrate services to implement added value functionalities.

The Member State has three different models to connect to the EUCISE2020 network. The three different configurations are:

- *Configuration A:* a single Public Authority belonging to a single Member State will connect to EUCISE2020 contributing with a single Legacy System. The Legacy System provides and consumes EUCISE2020 services available from other European Public Authorities through only one Adaptor

- *Configuration B:* each Public Authority of the same Member State taking part in the EUCISE2020 information exchange connects its own Legacy System to a dedicated Adaptor; several Adaptors connect to a EUCISE2020 Gateway type B that will access the EUCISE2020 Network
- *Configuration C*: the Public Authorities of the same Member State taking part in the EUCISE2020 information exchange connect to the EUCISE2020 Network through a single EUCISE2020 Node. The configuration C includes also a Light-Client which provides a human interface for graphical presentation of georeferenced data.

Figure 5 describes the logical architecture of EUCISE2020 configurations. Inside the redline components were developed through the joint European tender and outside the red line the interfaces with national legacy systems were developed through the national procurements.

The system uses EUCISE2020 data model for information exchange. The data model is based on the CISE data model version 1.0 that was defined in the CoopP Project and modified in partnership with Joint Research Centre (EUCISE2020 D4.3 Annex B). The CISE Data Model designed in CoopP Project identified seven core data entities (Agent, Object, Location, Document, Event, Risk and Period) and eleven auxiliary ones (Vessel, Cargo, Operational Asset, Person, Organization, Movement, Incident, Anomaly, Action, Unique Identifier and Metadata).

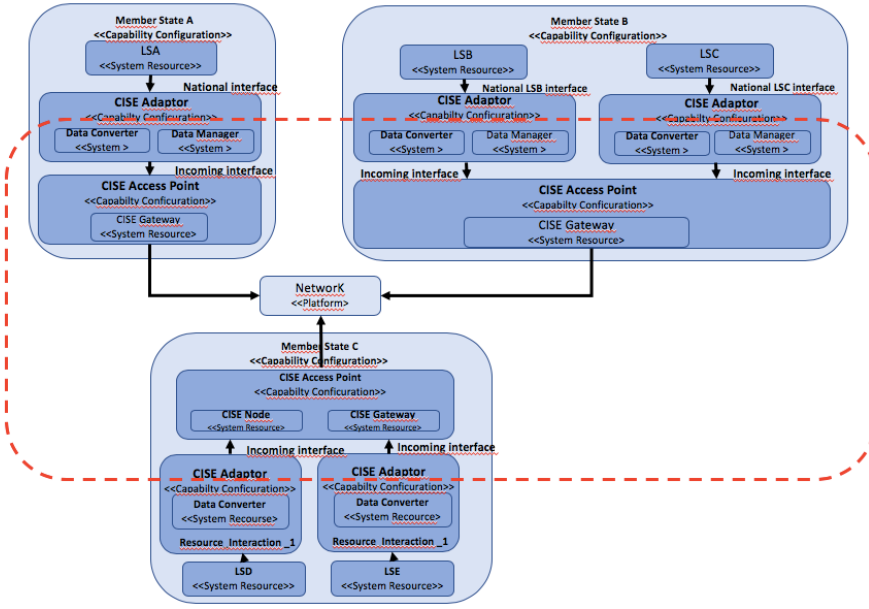

Figure 5: Logical Architecture of EUCISE2020 configurations A, B and C.

Figure 6 shows the EUCISE2020 data model. It is based on the same data entities (7+11), but in order to take into account additional data sources (meteo-oceanographic), EUCISE2020 defined additional attributes to some of the above mentioned data entities.

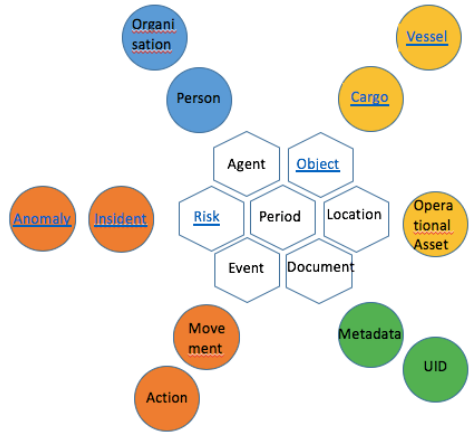

Figure 6: CISE data model (EUCISE2020 D4.3 Annex B).

The solution includes the elements, principals and technics for cyber information sharing but has to be updated or improved for cyber information exchange. The standardized language used for information exchange has to be decided as well as messages, protocols and services to use and systems software has to update to understand these. Earlier in chapter 2.3 mentioned STIX™ and TAXII™ are considerable alternatives. Depending on each partner's cyber information Legacy System (LS) data model the adaptor between LS and Node/GW has to update to "translate" LS data to chosen exchange data model and to understand the messages and services used in information sharing.

Lessons learned from the EUCISE2020 project were that special attention has to be paid on the information exchange network reliability and in cyber case also to security. The EUCISE2020 network is a peer-to-peer network where the amount of VPN connections per partner increase significantly and makes the network vulnerable.

Discussion

CISE is not only a technical solution of information sharing. The fundamental part of CISE and the principle of Responsibility to Share is even more mandatory to understand and adopt for information sharing. The information sharing policy "Responsibility to Share" is a cornerstone of CISE vision which clearly indicate the change in information exchange policy and constitutes the basis for reliable and trustworthy CISE information exchange. It also accounts for the fact that the party needing a certain piece of information might not know that the information exists

in the first place, much less where it is kept, and thus might be unable to actively search the missing information.

The EUCISE2020 project has faced the phase where the network controlling will be mandatory to all Member States. The maritime information is shared in Test-Bed network, which is controlled by MS according the national rules and methods. During the EUCISE2020 Transition Phase and before the operational phase the network will be certificated, rules for network controlling will be agreed which means that cyber information sharing in maritime domain will be under discussions and guidelines how the maritime consortium act to cyber threats will be decided (Discussions with Finnish Transport Infrastructure Agency, EUCISE2020 meeting on December 3, 2018.)

Information sharing limitations in maritime domain could be divided in at least in technical and organisational limitations. The actualized CISE network do not support classified information sharing as mentioned earlier. However, the EUCISE2020 Deliverable D8.3 "Dissemination plan with Policy recommendations and Governance model" states that CISE must allow the exchange of classified data, for instance in a parallel embedded secure network architecture, as significant amount of maritime reporting and surveillance data are treated confidentially.

The organisational limitation is based on observation in which the maritime authorities have outsourced the network controlling and therefore co-operation might be limited between the actors. On the other hand, CISE network itself and the traffic inside the network has to be controlled by the Members States and whenever a cyber-threat is found in one MS it should be informed to the other MSs. In other words, it is mandatory for CISE operational phase on 2020 to start building up the cyber information sharing network among the maritime authorities. A wide scale of open or undiscussed issues of cyber information exchange exists among maritime CISE consortium. The common understanding or agreement which data model should be used for sharing has not been determined so far as well as the information type which will be shared.

The next recommended steps for this are (not in order of importance):

- Identify the maritime cyber organisations and actors
- Follow network control related actions on EUCISE2020 transition phase
- Identify the cyber information sharing related projects outside CISE
- Identify maritime sensitive cyber information
- Identify the information to share
- Open the discussions about the information sharing importance, meaning, interests, what, how when etc.
- Identify and introduce the existing information sharing tools to cyber information organisations
- Investigate the technical updates needed for sharing the cyber information using existing information sharing systems.

CISE is a transmission channel between user communities and it's not a system or platform for data storing. Each user community gathers and stores its data by

its sectoral systems and security standards. Data classification levels are missing due to fact that same data may be classified differently by the different user communities. Common ontology for data classification levels on cross-sectoral information exchange should develop. CISE roadmap explained data classification levels and access profiles as "In order to facilitate cross-sectorial information exchange, User Communities should develop a common approach when attributing classification levels."[9]

Acknowledgements

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

References

1. Australian Government, Attorney-General's Department, "Cyber Security Strategy," 2009.
2. Sean Barnum, *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)*, white paper, 2014, available at http://stixproject.github.io/getting-started/whitepaper/.
3. Martin Brunner, Hans Hofinger, Christopher Roblee, Peter Schoo, and Sascha Todt, "Anonymity and Privacy in Distributed Early Warning Systems," *CRITIS 2010: Critical Information Infrastructures Security* (2010): 81-92.
4. Cyber Security Strategy Committee, Ministry of Defence, "Cyber Security Strategy," 2008.
5. Michael Davies and Menisha Patel, "Are We Managing the Risk of Sharing Cyber Situational Awareness? A UK Public Sector Case Study," *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, *CyberSA*, London, UK (2016).
6. ECHO Project, ECHO Proposal, 2018.
7. Thomas W. Edgar and David O. Manz, *Research Methods for Cyber Security* (Cambridge: Elsevier, 2017).
8. ENISA, "Critical Infrastructures and Services: Maritime," 2011, available at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/dependencies-of-maritime-transport-to-icts (accessed April 1, 2019).
9. European Commission, Communication from the Commission to the Council and the European Parliament on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain COM(2010), 584.
10. European Commission, "CISE Architecture Visions Document (Study supporting the Impact Assessment)," Brussels, European Commission, 2013.
11. European Commission, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU," Brussels, European Commission, 2017.

12. Ulrik Franke and Joel Brynielsson, "Cyber Situational Awareness: A Systematic Review of the Literature," *Computers & Security* 46 (2014): 18-31.
13. Matthew Harwood, "Lack of Trust Thwarts Cybersecurity Information Sharing," *Security Management* (2011).
14. Simon Hennin, "Control System Cyber Incident Reporting Protocol," *IEEE International Conference on Technologies for Homeland Security*, Waltham, MA (2008): 463-468.
15. Gary C. Kessler, J. Philip Craiger, and Jon C. Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," *The International Journal on Marine Navigation and Safety of Sea Transportation* 12, no 3 (2018): 429-437.
16. Ray Klump and Matthew Kwiatkowski, "Distributed IP Watchlist Generation for Intrusion Detection in the Electrical Smart Grid," in *Critical Infrastructure Protection* IV, edited by T. Moore and S. Shenoi, *IFIP Advances in Information and Communication Technology*, vol. 342 (Berlin: Springer, 2010), 113-126.
17. Tero Kokkonen, *Anomaly-Based Online Intrusion Detection System as a Sensor for Cyber Security Situational Awareness System* (Jyväskylä: University of Jyväskylä, Tietotekniikka, 2016).
18. Tero Kokkonen, Jari Hautamäki, Jarmo Siltanen, Timo Hämäläinen, "Model for Sharing the Information of Cyber Security Situation Awareness between Organizations," *23rd International Conference on Telecommunications*, Thessaloniki, Greece, 2016.
19. Paul Mario Koola, "Cybersecurity – A Systems Perspective," *Dynamic Positioning Conference*, Marine Technology Society (2018): 1-12.
20. Sándor Munk, "Interoperability Services Supporting Information Exchange Between Cybersecurity Organisations," *AARMS* 17, no. 3 (2018): 131-148.
21. National Coordinator for Security and Counterterrorism, Netherlands, "National Cyber Security Strategy," 2013.
22. Jyri Rajamäki, Juha Knuuttila, "Cyber Security and Trust Tools for Multi-agency Cooperation between Public Authorities," *Proceedings of the 7th International Conference on Knowledge Management and Information Sharing - KMIS* (2015), pp. 397-404.
23. Elaine M. Sedenberg and James X. Dempsey, "Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs," 2018, available at https://arxiv.org/abs/1805.12266 (accessed March 30, 2019).
24. Andrew E. Tucci, "Cyber Risks in the Marine Transportation System," in *Cyber-Physical Security. Protecting Critical Infrastructure*, edited by R. Clark and S. Hakim, vol. 3 (Cham: Springer, 2017), 113-131.
25. Robert K. Yin, *Case Study Research and Applications: Design and Methods*, Sixth ed. (Los Angeles: SAGE Publications, 2017).

About the Authors

Jyri **Rajamäki** is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology and a PhD in mathematical information technology from University of Jyväskylä.

Ilkka **Tikanmäki** is a researcher at Laurea University of Applied Sciences and a doctoral student of Operational art and tactics at the Finnish National Defence University. He holds a MBA degree in Information Systems and BSc degree in Information Technology.

Jari **Räsänen** (LtCDR ret.) currently conducts research on a project basis at Laurea University of Applied Sciences. He has specialized in air and maritime surveillance systems and information sharing environments, especially EUCISE2020 and preceding CISE projects during his thirty years' military service in Finnish Defence Forces.

Annex 4 – Cyber situational Awareness and information sharing in critical infrastructure organizations

by J. Pöyhönen, V. Nuojua, M. Lehto & J. Rajamäki

In vol. 43 of Information & Security: An International Journal, https://doi.org/10.11610/isij.v43

Information & Security

J. Pöyhönen, V. Nuojua, M. Lehto & J. Rajamäki, vol. 43, no. 2 (2019): 236-256
https://doi.org/10.11610/isij.4318

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations

Jouni Pöyhönen [a] (✉), ***Viivi Nuojua*** [a], ***Martti Lehto*** [a], ***Jyri Rajamäki*** [a,b]

[a] *University of Jyväskylä, https://www.jyu.fi/en*

[b] *Laurea University of Applied Sciences, https://www.laurea.fi/en/*

ABSTRACT:

Cybersecurity-related capabilities play an ever-growing role in national security, as well as securing the functions vital to society. The national cyber capability includes the resilience of companies running critical infrastructures, their cyber situational awareness (SA) and the sharing of cybersecurity information required for cyber SA. As critical infrastructures become more complex and interdependent, ramifications of incidents multiply. The EU Network and Information Security Directive calls for cybersecurity collaboration between EU member states regarding critical infrastructures and places the most crucial service providers and digital service providers under security-related obligations. Developing better SA requires information sharing between the different interest groups and enhances the preparation for and management of incidents. The arrangement is based on drawing correct situation-specific conclusions and, when needed, on sharing critical knowledge in the cyber networks. The target state is achieved with an efficient process that includes a three-level—strategic, operational and technical/tactical—operating model to support decision-making by utilizing national and international strengths. In the dynamic cyber environment strategic agility and speed are needed to prepare for incidents.

ARTICLE INFO:

RECEIVED: 12 JUN 2019
REVISED: 28 AUG 2019
ONLINE: 22 SEP 2019

KEYWORDS:

cybersecurity, situational awareness, information sharing, critical infrastructure, vital societal functions

✉ E-mail: jouni.a.poyhonen@jyu.fi

Introduction

The capability related to national cybersecurity plays an even more important role when it comes to the overall security and securing the crucial functions of society in the future. The national capability consists of most of the resilience of the critical infrastructure companies and the situational awareness of the cyber environment, they constantly maintain.

The critical infrastructures become more complex and their parts are even more strongly dependent on each other, and that way, the ramifications of the incidents can be multiple compared with the original impact. The operation of critical infrastructure and the threats having an impact on them are not limited to organizations or administrative borders.[18]

The EU Network and Information Security (NIS) Directive [4] increases the collaboration between the member states in the important field of cybersecurity. It puts the most crucial service providers (critical industries such as energy, transport, health, and financing) and digital service providers (online marketplaces, search engines, and cloud computing) of society under the security-related obligations. The application of the Directive results in imposing the security and information requirements concerning the aforementioned operators. The goal is to develop even better situational awareness and information sharing. The critical infrastructure consists especially of the crucial service providers defined by the NIS Directive. In Finland, the administrative sector coordinates the operations required by the Directive, when both monitoring and the duty to notify are decentralized. The National Cyber Security Centre Finland builds situational awareness.

Principally, the functional observation and analysing ability collected from the different trust circles gives a good basis for the development of Finland's national situational awareness, and information sharing.[9] Critical infrastructure can be described as a three-levelled system of systems (Fig. 1); efficient and appropriate operations can be targeted at its three levels, from bottom to the top: power grid, data transmission network, and services.[14]

The situational awareness of critical infrastructure is emphasized also in the Security Strategy for Society,[16] as part of maintaining vital national operations. Efficient incident management requires tight collaboration between the management, situation awareness and communication. Good management requires:

- unquestionable managerial responsibility, the casting of different operators and the decision-making ability of the ministerial authority

Figure 1: Plain structure of critical infrastructure.

- building of situation awareness (situational understanding, evaluation of situational development)
- crisis communication
- information sharing, and supporting technical solutions
- business continuity management
- co-operation.

Research Purpose, Research Questions, and Article Structure

The research questions deal with the situational awareness and understanding of an organization, as well as the data analysis and information sharing between the different interest groups. The aim is to develop the preparation for incidents and their management in the whole society. The arrangement is based on drawing correct situation-specific conclusions and, when needed, on sharing critical knowledge in the cyber networks of society.

The research questions are:

1. How the cyber situational awareness of an organization can be developed?
2. How do the organizations exchange their cybersecurity-related information?
3. Can an organization's cybersecurity capability be utilised more extensively?

This paper is a continuum of the research "Cyber strategic management in Finland,"[10] in which one task was to formulate management proposals for the management of nationally pervasive incidents concerning cyber environment. Good situational awareness and information sharing between the different interest groups have an essential impact on incident management. The research method was an open theme interview with material-based content analysis. All three levels of the critical infrastructure system of systems (see Figure 1) were represented. There were altogether 40 interviewees from 25 private or public organizations, which were leaders or persons responsible for the information/ cybersecurity of their organizations.

In Finland, the significance of the private businesses is emphasised in the operation of critical infrastructure, since approximately 80 % of the operations can be estimated to belong to their responsibility. Researchers interviewed six private businesses, as well as public authorities, such as the National Cyber Security Centre Finland and the National Emergency Supply Agency.

Section 2 deals with the need for situational awareness, and related decision-making levels and the theory of situational awareness. In Section 3, the information sharing needs of an organization are explored, ever since the national and European Union needs. Section 4 describes the formation of situational awareness into the different levels of an organization, and the information-sharing procedures at the national level. Finally, Section 5 concludes with the conclusion.

Situational Awareness

To function, every organization needs information about its environment and happenings, and also about its impact on its operation. An appropriate and fast situational awareness is based on correct information and evaluations, and it is emphasized in the case of incidents when very pervasive decisions must be made quickly. To make correct solutions, decision-makers have to know the base for their decisions, consequences how the others react to them and what risks the decisions include. For that reason, decision-makers must have sufficient situational awareness and understanding of all the operational levels, which enables timely decision-making and operation. Situational awareness and understanding require collaboration and expertise, which enables the comprehensive monitoring of the operational environment, data analysis, and aggregation, information sharing, recognition of the research needs and network management. The information systems must enable the systematic use of information sources and collaboration and the flexible sharing of situation information related to it.[11]

The organizations' and decision-makers' formation of situational awareness is supported by the situation awareness arrangements. In general, situation awareness means the description of the dominant circumstances and the operational preparedness of different operators aggregated by the specialists, the happenings caused by an incident, its background information and the evaluations concerning the development of a situation. In addition, data analysis based operational recommendations may be related to situation awareness. The general view is constituted by utilizing a networked operational model based on different sources. The process consists of data acquisition, information aggregation, classification and analysis, and of a timely and efficient sharing of the analysed information with those in need. The surrounding data space is organised such that the information is understood correctly, and that the operators have a chance to get the information important to their operation.[11]

The pervasive incidents targeting society are a challenging cyber environment when it comes to the critical reaction speed required by the situation management. Advanced Persistent Threats (APT) are unfamiliar attacks to the traditional protection ways and can proceed quickly when fast information sharing and good situational awareness play an important role in incident management. In a worst-case scenario, the delegation of responsibility should be able to make possible in a few minutes, the response evoked without delay, and the abilities and tools put to use.[12]

Decision-making levels

Organizations operate in very complex, interrelated cyber environments, in which the new and long used information technology system entities (e.g. a system of systems) are utilized. Organizations are depended on these systems and their apparatus to accomplish their missions. The management must recognize that clear, rational and risk-based decision are necessary for business continuity. The risk management at best combines the best collective risk assessments of the organization's individuals and different groups related to strategic planning, and also the

operative and daily business management. The understanding and dealing of risks are an organization's strategic capabilities and key tasks when organizing the operations. This requires, for example, the continuous recognition and understanding of the security risks on the different levels of the management. The security risks may be targeted not only at the organization's operation but also at individuals, other organizations and the whole society.[8]

Joint Task Force Transformation Initiative recommends implementing the organization's cyber risk management as a comprehensive operation, in which the risks are dealt with from the strategic to tactical level.[8] That way, risk-based decision-making is integrated into all parts of an organization. In Joint Task Force Transformation Initiative's research, the follow-up operations of the risks are emphasised in every decision-making level. For example, in the tactical level, the follow-up operations may include constant threat evaluations about how the changes in an area can affect the strategic and operational levels. The operational level's follow-up operations, in turn, may contain for example the analysis of the new or present technologies to recognize the risks to the business continuity. The follow-up operations of the strategic level can often concentrate on the organization's information system entities, the standardization of the operation and for example on the continuous monitoring of the security operation.[8]

From the necessity of the organization's risk, follow-up operations can be drawn the necessity of the whole organization's situational awareness. As mentioned, the formation of the organizations' and decision-makers' situational awareness is supported by the situation awareness arrangements. Thus, an appropriate situational awareness supports cyber risk management and more extensively the evaluation of the organization's whole cyber capability.

Theory of Situational Awareness

Mica Endsley has developed a situational awareness model when working on several different research assignments in the service of the United States Air Force.[3] Figure 2 describes the general structure of the model. The core of situational awareness consists of three basic elements: detection (Level 1), situational understanding (Level 2) and its impact assessment towards the future (Level 3). This situational awareness provides the foundation for conclusions and the following decision-making. Depending on the situation, the assignment- and system-specific features and the decision-maker's experience and evaluation ability bring their impacts on the table. Decision-making, in turn, guides the operation that reflects the observed operational environment.

Sid Faber regards the situational awareness development operations, concerning both public and private businesses, as one of the most significant near-future goals aiming to improve cybersecurity.[5] He recommends applying Endsley's model to the follow-up needs of a cyber-operational environment.

Figure 2: Situational awareness and dynamic decision-making (adapted from Endsley [3]).

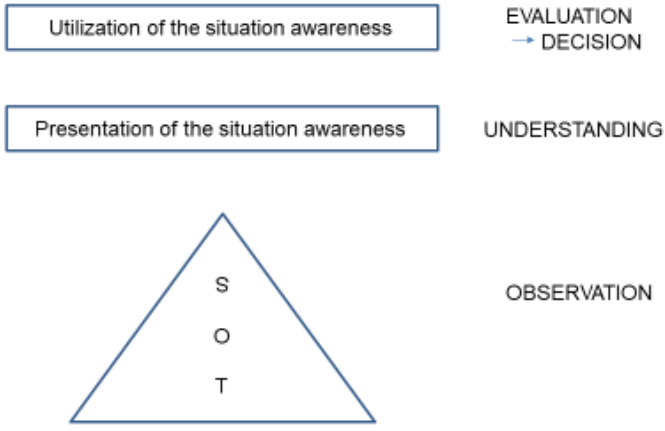

Figure 3: Framework for forming situational awareness.

The general structure of Endsley's situational awareness model is applied when solving our research questions.[3] The framework for forming the critical infrastructure situational awareness is introduced in Figure 3. The detection part (Level 1) of Endsley's structure is presented as the organization-specific detection needs of the strategic (S), operational (O) and technical/tactical (T) decision-making levels. The goal is to gain a perception that serves each decision-making level. The situation awareness that is formed of observations is a prerequisite for understanding the observations (Level 2). After that, the impact analysis and assessment of the observations are made possible by utilizing the understanding about situation awareness (Level 3). There, analysis capability plays an important role. The final goal is to make appropriate and situation-specific decisions on each decision-making level and conduct the operations followed by the decisions.

General Requirements for Situation Awareness

Horsmanheimo and co-workers set some requirements for the situation awareness in their research: [6]

- Situation awareness is a series of presentations whose shape does not matter. It is more essential than somebody manages it, makes analysis and decisions.
- Information is brought to the situation awareness system in collaboration. Every operator is independently responsible for the production and validity of the information related to their knowledge area.
- The information must be processed, analysed and understandable. It has to be meaningful for both oneself and other receivers.
- The information must be performed visually and clearly.
- The information must be performed without unnecessary technical details. The information must be understandable for people from other industries.
- Situation awareness system should be dynamic and tailored by users and industries. Information should be able to put on different views.
- Terminology and classifications should be uniform.
- Situation awareness system should be able to be included in the organization processes such that the maintenance of the situation awareness system would not become an extra task in grand incidents.
- Different operators should be able to define what kind of information they need and what kind of information they can input to the system.
- Situation awareness system should be able to be utilised for information exchange between different operators on different organization levels. Information should be able to be shared also with the supervisory organizations.
- The situational awareness system should be able to make predictions of what is happening by 3, 6 or 12 hours.
- The situational awareness system should be able to perform a temporal dimension to how the things have developed – whether the direction is worse or better.

Information Sharing Needs of an Organization

The EU Network and Information Security (NIS) Directive increases the collaboration between the member states in the important field of cybersecurity. It puts the most crucial service providers (critical industries such as energy, transport, health, and financing) and digital service providers (online marketplaces, search engines, and cloud computing) of society under the security-related obligations. The application of the Directive results in imposing the security and information requirements concerning the aforementioned operators. Also, the Directive supports in developing nationally better situational awareness.

The operations of the concerned Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 have been carried out nationally since 2018. The Directive states the subject matter and scopes the following: [4]

1. This Directive lays down measures to achieve a high common level of security of network and information systems within the Union to improve the functioning of the internal market.

2. To that end, this Directive: a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems; b) creates a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among the Member States and to develop trust and confidence amongst them; c) creates a computer security incident response teams network (‘CSIRTs network') to contribute to the development of trust and confidence between the Member States and to promote swift and effective operational cooperation; d) establishes security and notification requirements for operators of essential services and digital service providers; e) lays down obligations for the Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

Principally, a functioning observation and analysing ability composed from different trust circles provides a good starting point for the development of Finland's national situational awareness.[9] By the most crucial service providers' and digital service providers' duty to notify, the national situational awareness can be developed. The duty to notify expands the previous procedure considerably and therefore covers a significant part of the critical infrastructure by private businesses. Also, the operation involves information sharing between the authorities, and more than before between the authorities and private business operators. In Finland, the operations required by the Directive relate to sector-specific laws and, consequently, their monitoring as well as the duty to notify happen sector-specific. The laws include the definitions of the crucial service providers' duty to notify. The situational awareness is built by the National Cyber Security Centre Finland.

The National Cyber Security Centre Finland

The National Cyber Security Centre Finland (NCSC-FI) is part of the Finnish Transport and Communication Agency, Traficom. Traficom is an authority in a permit, license, registration, and monitoring of transport and communication. It promotes traffic safety and the smooth functioning of the transport system and speeds up the development of digital society. Also, the agency supports sustainable development and ensures that everyone in Finland has access to high-quality and secure communications connections and services.[17]

Nationally, the NCSC-FI plays the most crucial part in forming and analysing the cyber situational awareness, and in incident management. It has three main tasks:

1. The NCSC-FI acts as a national communications security authority (NCSA) and is responsible for the security matters related to the electrical data transmission and processing of the safety-classified material. The NCSA operation is part of Finland's security authority organization.
2. The CERT (Computer Emergency Response Team) operation of the NCSC-FI takes care of the prevention, investigation and announcement tasks in case of information security breaches. The main purpose of the CERT operation is to produce and maintain the cyber situation awareness together with domestic and foreign cooperation partners and counterparts. As an essential part of

the CERT operation, the NCSC-FI acts as a national point of contact for information security breaches and threats. It also investigates these cases and helps the concerned parties.

3. The NCSC-FI manages the information security regulation tasks of Traficom. It acts as a national regulatory authority (NRA), i.e. as a guiding and monitoring authority.

The NCSC-FI is an authority that aggregates and builds national situational awareness. It collaborates closely with other authorities and private business operators.

HAVARO is a service that detects and warns about information security breaches, serves the critical companies for security of supply and the state administration. From the HAVARO system, the NCSC-FI has visibility to practically all the upcoming and outgoing traffic (metadata and content data). Many critical companies for security of supply and the state administration operators have put to use the HAVARO service, which indicates the trust in the NCSC-FI. That way, the information security breaches targeted at the organization can be reported automatically to the authority without a chance for censoring the incidents beforehand. The system has been implemented in collaboration with the National Emergency Supply Agency.

The companies and public administration operators participate in the HAVARO operation voluntarily. The operation of the system is based on the information security threat identifiers coming from different sources. With the help of the identifiers, harmful or anomalous traffic can be detected from the organization's network traffic. The NCSC-FI receives information about the anomalies and analyses them. In case of an information security threat, the organization is warned about it. Based on the information got from the HAVARO, also the other operators can be warned about the detected threat. That way, the system helps not only individual organizations but also in forming a general view about the information security threats against Finnish information networks.

The observation ability of information security threats is an important part of comprehensive risk management. For its part, HAVARO secures the organization's business continuity against the threats of the operational environment. However, HAVARO is not meant to be an organization's only information security solution, but it is designed to complete the other information security solutions of information security investing organization.

Also, Traficom provides the *GovHAVARO* service for the state administration operators. It completes the information and cybersecurity threat detection of the state administration's Internet traffic. The service providers are Traficom, Valtori – Government ICT Centre and Telia. The *GovCERT* services, in turn, support the state's round-the-clock information security operation by producing the support services for preventing, detecting and investigating information security breaches, as part of the GovSOC operation. They are provided by Traficom and Valtori.[7]

The incident management of the state administration and other public administration organizations, so-called VIRT operation, is a cross-administrative opera-

tional level collaboration, which prepares for severe and extensive information security incidents. It consists of operational planning and rehearsing for different information security incidents.[7]

The industry-specific cyber information-sharing groups (ISAC, Information Sharing and Analysis Centre) are established as collaboration organs between the organizations of different industries. Their operation enables:

1. Confidential handling of information security matters between the participants.
2. Augmentation of the organizations' information security know-how.
3. Development of the NCSC-FI's overall situational awareness.

The ISAC operation is based on regular meetings and specified operational models and participants. The ISAC information sharing groups have been established for the following industries: state administration (VIRT), Internet service providers, chemistry and lumber industry, banks, media, energy industry, food production and distribution, social and health care, and software manufacturers.

The National Emergency Supply Agency

The National Emergency Supply Agency (NESA) is an institution working under the Ministry of Economic Affairs and Employment of Finland. It is tasked with planning and operations related to maintaining and developing the country’s security of supply. As part of the security of supply organization, the NESA’s mission is to support the operation of the pools and sectors and to take care of the other legislative tasks given to it. Security of supply means the ability to maintain such economical basic operations of society that are necessary for securing the populations' living prospects, society's functioning and safety, and the material prerequisite for national defence in severe incidents and extraordinary circumstances.[13]

The national cybersecurity management requires a close-knit collaboration between the critical infrastructure operators (Public-Private Partnership, PPP). The NESA's information society pools take care of the collaboration.

Formation of Situational Awareness

The analysed collection of data was created based on interview material, document analysis, and international comparison information. The observations, presentations, and models presented in this article, are based on this data.

Situational Awareness on a Tactical Level

Both technical, networked and management situation awareness are emphasized when building the situational awareness. During the last years, Finland has formed its cyber situation awareness through the information-sharing mechanisms of different operators. It is about national and international collaboration. The improvement of information sharing and perception is still a matter of development when it comes to Finland's cybersecurity.[9]

The critical infrastructure operators use such protection techniques in their ICT systems that extend from the interface of the Internet and the organization's internal network right up to the protection of a single workstation or apparatus. These technical solutions make it possible to verify different harmful or anomalous observations. The typical technologies are related to security products such as network traffic analysis and log management (Security Information and Event Management, SIEM), firewall protection, intrusion prevention and detection systems (IPS and IDS) and antivirus. The situation awareness builds up to centralized monitoring rooms (Security Operations Centre, SOC). These technical solutions can be under the organization's control, or the service can be outsourced to the information security operator. A crucial goal is the situational awareness and protection of the business processes.

Also, especially the critical companies for security of supply have the HAVARO system in the external interface of their network. The system follows the network traffic and detects harmful and anomalous traffic. Then, the warnings come from the NCSC-FI.

The observation ability relates also to a so-called advance warning that can be received from the organization's international or national operation networks. In the centre of operation, there is always the organization's capability to pay attention to the abnormal operation that possibly occurs in the system. The overall observation ability is developed for example by benchmarking and practicing.

The organizations implement the analysis of incidents and anomalies from their own starting points, at the hands of their own or carried out by the service provider. The analysing ability requires more and more the securing of the organization's business process operation. The intensification of protection operations or for example the introduction of alternative operational models are the most important goals of the operation. The analysing capability determines the choice of needed operations and, that way plays an important role in the organization's decision-making process. The analysing ability must enable a severity classification and so-called cyber-physical view.

The analysing usually happens in centralized monitoring rooms (Security Operations Centre, SOC) based on situational awareness. In the monitoring rooms, the information coming from different sensors is aggregated and a situation-specific analysis is formed. Based on the analysis the needed operations are launched. The organization's possibilities to utilize the information gotten from international or national operational networks relate to the analysing ability. The personnel's capability to interpret the available observations correctly has a significant meaning in composing situation-specific analyses.

A typical reaction to an incident or anomalous operation comes at first from an incident response manager based on the situation awareness and its analysing. The magnitude and severity of an incident have an impact on the operations. Besides fast-reacting, the organization's management can be congregated to decide on the extension of the operations, and the allocation of the needed resources. Depending on the magnitude of an incident, the whole organization's management to the supervising board can be informed. Regarding the publicly traded

companies, the organization's external informing is guided by the informing obligations based on the law.

In the case of a nationally extensive incident, the critical infrastructure organizations keep in touch with the NCSC-FI and utilize not only the authority network but also the industry's network and their business networks. In this communication, the organization's situation awareness and its situation-specific analysing are combined.

Part of the critical companies for security of supply have a communication demand for authorities, such as NCSC-FI, in case of an incident. Based on the NIS Directive, an authority can expand this demand to the critical infrastructure organizations whom the duty to notify does not yet apply.

Developing Competences for Situational Awareness of the Organization

The nationally significant critical infrastructure organizations have developed in forming the cyber situational awareness and observation ability concerning the technical and tactical preparedness. It is also improved by the industry-specific and even more large-scale networking of the organizations. Networking and information sharing are supported by a functional collaboration between the authorities and the private sector. The good situational awareness of different companies (situational awareness and its analysing) and the information sharing via their interest groups is, indeed, a crucial factor in the whole national cybersecurity. Figure 4 sums up the factors that have come up in this research and further the organization's tactical level cybersecurity. The starting point is always the capability of the organization's personnel in recognizing the possible anomalous activity in the used systems and in operating reliably and organized in different situations. In an ideal case, the operation is supported by the technical systems or the used services of the ICT or information security operators or by utilizing the operational network, participating in the authority collaboration, utilizing the consulting services or benchmarking or testing and exercising the operation.

Operational Level Situational Awareness

The operational level operations are used to advance strategic goals. Comprehensive security- and trust-adding operations require comprehensive cybersecurity management. Its starting point has to be the target's risk assessment, and the operation analyses carried out based on it. The operational level's concrete hands-on operations must be targeted at the confirmation of information security solutions and the composition of the organization's continuity and disaster recovery plans. The goal has to be the continuous monitoring of the operational processes' usability, and the decision-making support in case of incidents that require analysing and decisions.

The NCSC-FI and NESA are identified as state administrative point of contacts on the business level. The NESA and different pools, especially the digital pool, support companies in developing and maintaining the situation awareness of the cyber operational environment. Because of the operation goals, the NESA brings together a significant part of the authorities and IT businesses. The private sector

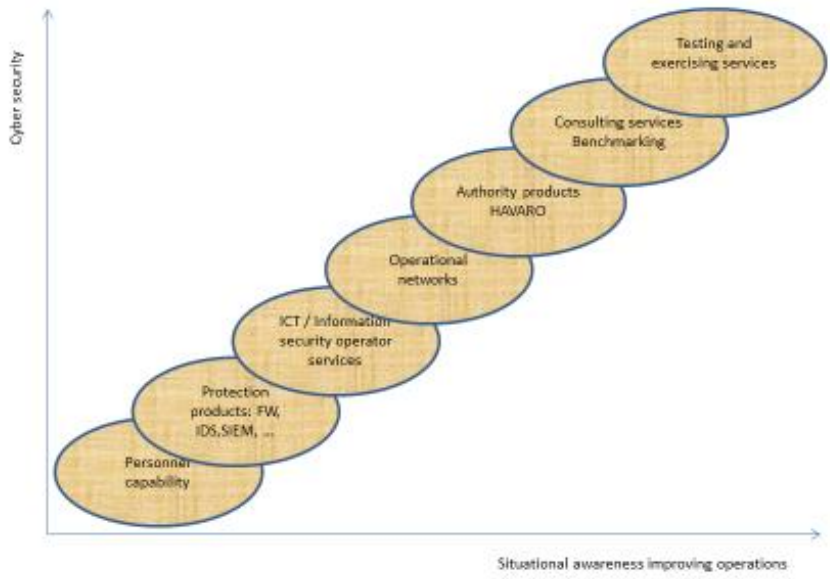

Figure 4: Development of an organization's cyber situational awareness as part of comprehensive cybersecurity.[10]

recognizes its tasks in advancing national cybersecurity. The collaboration models between the authorities and private businesses have been created, and they are internationally comparable.

With the support of the authorities, have been developed not only HAVARO for the security of supply critical operators but also KRIVAT service for critical infrastructure organizations such that the operators themselves form the network. The purpose is to strengthen the collaboration between organizations in grand incidents and speed up the recovery from them.

The technical protection ability of the most significant critical infrastructure organizations and the observation ability based on that are on a good level. Different collaboration networks are widely used. Organizations and the NCSC-FI keep in touch regularly. The analysing ability of anomalous operation and the incident management ability base on the capable personnel and functional collaboration networks.

Situational Awareness at Uppermost Management Level

One of the most fundamental cybersecurity tasks of the organization's uppermost management is the continuous development and maintaining of the trust in operation as part of the national critical infrastructure. The strategic choices relate to the reputation of an organization. The management is required to make concrete strategic choices and to support and guide the performance of the chosen operations through the whole organization. An important task of the management is to take care of the adequate resourcing of operations. About the chosen operations

must be communicated extensively with the organization's personnel and other interest groups.

It is important to create a cybersecurity assessment model for the needs of the uppermost management. With the help of that model, for example, other organizations can evaluate their cybersecurity level, become aware of their weaknesses and insufficient contingency planning, and take care of at least of the basics. The operations require strategic level decisions from the organization's uppermost management.

Finland's national cybersecurity execution program 2017–2020 aggregates the pervasive and significant information and cybersecurity improving projects and operations of the state administration, business, and associations, and their responsibilities. The progress of the execution program can be followed by following the development of the different organization's capabilities during the concerned inspection period. The execution program includes extensively effective operations that are developed by other administrative-specific operations, and by the work related to the development of cyber and information security and business continuity management. At the same time, the follow-up results in the formation of national cyber situational awareness.[10, 15]

The National Cyber Security Index (NCSI) is developed for the follow-up of the national cybersecurity-related capability. It is based on twelve sectors that are sorted into four groups as follows: [2]

- General cybersecurity indicators
- Cybersecurity basic indicators
- Event and crisis management indicators
- International event indicators

The NCSI index has four cybersecurity viewpoints per every twelve sections. These are the effective legislation, functioning individuals, collaboration arrangements and the results from different processes. The operation of the index is based on the evaluations of the specialist group.

Table 1 introduces a measure that is based on the NCSI index. It measures the cybersecurity capability of an organization and is developed for the use of businesses and other organizations. The evaluation is based on the requirements, business, interest group collaboration and results. In this organization measure, the twelve sectors of cybersecurity are arranged into four groups as follows:

1. General indicators
2. Basic level indicators
3. Event and incident management indicators
4. National impact indicators.

The commissioning of the measure can be seen to be targeted at the national cybersecurity execution program's goal "A national light cybersecurity evaluation, by which the organizations can take care of reaching the minimum level of security, has been composed." By the organization-specific commissioning of the

Table 1. Structure of an organization-specific measure.

	Requirements	Business	Interest group collaboration	Results
GENERAL INDICATORS				
Ability to develop the organization's cybersecurity culture				
Ability to analyse its cyber environment				
Magnitude of cybersecurity training				
BASIC LEVEL INDICATORS				
Confirmation of operational resources				
Risk assessments				
Quality requirements of the information systems' operation				
Operation follow-up and measures				
EVENT AND INCIDENT MANAGEMENT INDICATORS				
Quality of contingency planning for incidents				
Situational awareness 24/7				
Ability to manage incidents				
Ability to recover from incidents				
NATIONAL IMPACT INDICATORS				
Operation in cyber operational networks				
POINTS				

measure, the aforementioned goal can be seen as achieved. The widespread commissioning of the measure in critical infrastructure organizations would make it possible to follow the cybersecurity development of the whole area in the same way as it serves the strategic level needs of a single organization.

Information Sharing on National Level

The NIS Directive requires explicit, identifiable and concrete operations to develop the national situational information sharing. The identification of collaboration partners and information producing operators generates prerequisites for society's encompassing information sharing and, that way, for the development of situational awareness. Figure 5 introduces a national information-sharing structure that enables the NIS Directive-based operation.

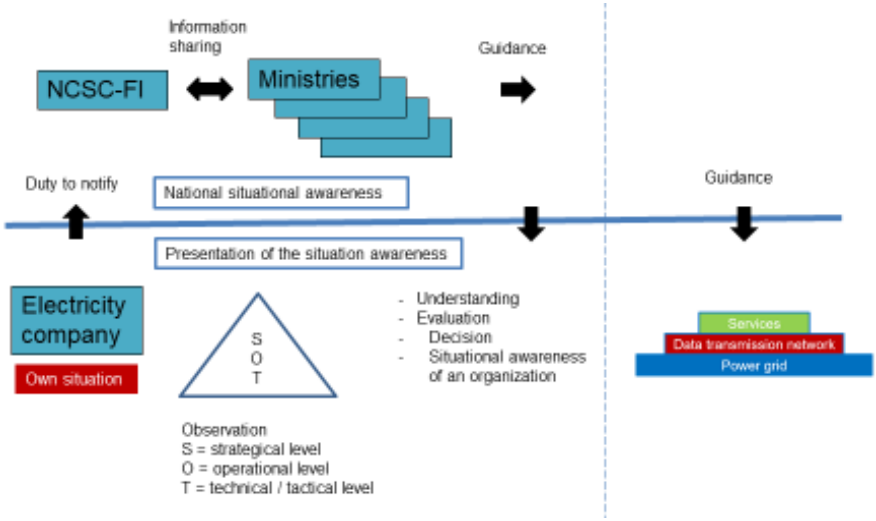

Figure 5: Information sharing on a national level.

The European EECSP report "Cyber Security in the Energy Sector" encourages to use the best practices of information sharing through some kind of analysing centre or analysing the process. Thus, the best practice sharing via interest groups and learning from that can be supported. The challenges related to the introduction of new technologies, the challenges caused by the mutual dependence of the market operators, or the challenges build-up by the links between the energy systems and networks are typical scenarios that can especially benefit from the sharing of best practices. Also, the procedure can be used for sharing delicate information that helps the operators in protecting their network proactively.[1]

In national information sharing, a critical infrastructure organization (electricity company in Figure 5) forms a cyber situation awareness from its starting points. In an ideal case, it bases on the observations from the different levels of the organization that is strategic, operational and technical/tactical level. Based on the information, the electricity company maintains its continuous situational awareness to support its decisions. In case of a cyber incident, the electricity company delivers information about its situation-specific analysis, based on the duty to notify, to the NCSC-FI and when need also to the responsible ministry. Based on their mutual information sharing, the NCSC-FI and responsible ministry form a national situational awareness about the matter. The responsible ministry takes care of the related and needed guidance operations to the other interest groups and the organizations of its area of responsibility. The NCSC-FI carries out continuous information sharing with the critical infrastructure organizations about the cybersecurity situation.

Finland's national strength in the organizations' possibilities in utilizing different networks when sharing the cybersecurity information has been emphasized in different researches.[9, 10] Here, three confidential information-sharing networks that

are utilized actively are introduced. These have been formed in connection with business operation, or a separate trust circle has been established between some industry's companies that can reach also into an international collaboration. Also, nationally operates a trust circle between the authorities and private sector (Public-Private Partnership, PPP). Figure 6 illustrates the aforementioned trust circles in the company field.

The critical infrastructure organizations have functioning situation awareness arrangements and analysing capability, and they exchange information by utilizing their networks and are capable of incident management based on their starting points. The risk assessments and the procedure option analyses based on the evaluations are a significant part of the continuity management of the organization's business processes. The concrete hands-on operations of the operational level must be targeted at securing the information security solutions and composing the organization's operational continuity and disaster recovery plans. The goal must be in the continuous follow-up of the operational processes' usability, and the contingency planning for incidents.

The cyber operational environment is dynamic, which means that especially the strategic agility is required when preparing for incidents. On the other hand, the organization's strategic decision-making level must also have tools for evaluating the development of the whole organization's cybersecurity. In this paper, the commissioning of the measure that follows the organization-specific capability is recommended. There, the evaluation is carried out via the requirements set for the

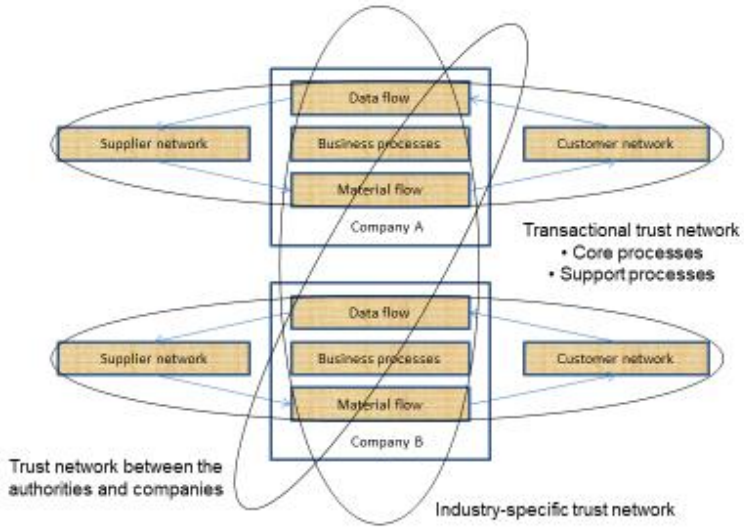

Figure 6: Trust networks related to an organization's cyber situational awareness development.

operation, business, interest group collaboration and results by utilizing four indicators. The four indicators have been derived from this cybersecurity measure from the international index, and they are the organization's general indicators, basic level indicators, event and incident management indicators, and national impact indicators.

Summary

The main novelty value of this study is the promotion of their practical measures which the NIS Directive required. In the big picture, the different parties related to the development of situational awareness must yet be able to improve their operation by even more efficient technical procedures, strengthen the network-like operation, and increase the utilization of public sector services. There will be good preconditions to the above-mentioned matter when cybersecurity capabilities of the organization are widely promoted as a part of the national critical infrastructure and the common objectives determined by the EU.

For the first research question, it is stated that as the target state of the organization's cyber situational awareness and its interest groups' information sharing can be set the operation where the recognition of threatening incidents and reacting to them happens in an efficient process. It must include all the organization's decision-making levels (strategic, operational and technical/ tactical) and utilize the national and international strengths of information sharing.

Based on the research the following basic requirements apply to the development of the organization's incident management:

- Strategic goals: a) Cybersecurity management in all circumstances; b) Strategic choices for operational continuity management
- Critical success factors: a) Good situational awareness on all the organizational levels; b) Fast reaction ability and executive guidance; c) Clear operational models and their sufficient resourcing; d) Good information sharing between the different interest groups; e) Crisis communication
- Evaluation criteria and target levels: a) Effectivity of the operation; b) Optimal resourcing.

For the second research question, the techniques used by organizations, procedures developed for incident reacting and different trust circles form a nationally useful observation ability. This scattered organization-specific observation ability and the analysing information and data reserve it contains can be utilised nationally in the analysing phase for the management of wide-scale incidents. The arrangement requires the creation of mutual operational models for information sharing. Because it is very presumable that there are not enough centralized resources to be used for analysing a wide-scale and quickly evolving cybersecurity incident, as a solution should be outlined a network-like operation consisting of the experts from different organizations (virtual analysing). Then, the data reserve should be jointly used, and the experts would use their trust circles that reach to the international information sharing relations. The usability of data reserve forms

the key for analysing. When building it must take into account not only confidentiality but also the data integrity and amount questions. In the referenced research, the evaluations of i.e. the formation of excessive data amount were presented, and then the analysing becomes more difficult too. Thus, the different technical solutions of data processing should be examined.

For the third research question, the main conclusion is that the organization-specific measures, which promote cybersecurity and situational awareness, make the filling of the obligations of the NIS directive (Part D) possible. Part D requires that the providers of central and/or digital service should take into use the security and notification requirements. In every member state, national and EU -level situational awareness is based on the ability to maintain situation consciousness. Thus, the measures presented in this study also will promote other objectives appointed by the NIS directive.

Acknowledgements

The part of the work performed by Laurea University of Applied Sciences was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

References

1 EECSP Expert Group, "Cyber Security in the Energy Sector," Europe: Energy Expert Cyber Security Platform (EECSP), 2017.

2 e-Governance Academy, "National Cyber Security Index (NCSI)," 2017, https://ncsi.ega.ee/, accessed August 6, 2019.

3 Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors and Ergonomics Society* 37, no. 1 (1995): 32-64.

4 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, *Official Journal* L 194, July 19, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

5 Sid Faber, "Flow Analysis for Cyber Situational Awareness," Software Engineering Institute, Carnegie Mellon University, December 7, 2015, https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html, accessed August 6, 2019.

6 Seppo Horsmanheimo, Heli Kokkoniemi-Tarkkanen, and Jouko Vankka, "Kriittisen infrastruktuurin tilannetietoisuus (Situational Awareness of Critical Infrastructure)" (Helsinki: Prime Minister's Office, 2017).

7 Kirsi Janhunen, "Valtionhallinnon häiriötilanteiden hallinta - miten VIRT-toimintaa kehitetään?" (Helsinki: Ministry of Finance, 2015).

[8] Joint Task Force Transformation Initiative, "Managing Information Security Risk – Organization, Mission, and Information System View," NIST Special Publication 800-39 (Gaithersburg, MD: National Institute of Standards and Technology, 2011).

[9] Martti Lehto and Jarno Limnéll, "Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi (Finland's Cyber Security: The Present State, Vision and the Actions Needed to Achieve the Vision)" (Helsinki: Prime Minister's Office, 2017).

[10] Martti Lehto, et al., "Kyberturvallisuuden strateginen johtaminen Suomessa (Strategic Management of Cyber Security in Finland)" (Helsinki: Prime Minister's Office, 2018).

[11] Ministry of Defence of Finland, "Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society)" (Helsinki, Ministry of Defence, 2010).

[12] National Audit Office of Finland, "Kybersuojauksen järjestäminen" (Helsinki, National Audit Office of Finland, 2017).

[13] National Emergency Supply Agency – Organisation, www.nesa.fi/organisation/, accessed August 6, 2019.

[14] Jouni Pöyhönen and Martti Lehto, "Cyber Security Creation as Part of the Management of an Energy Company," *16th European Conference on Cyber Warfare and Security*, Dublin, 2017, pp. 332-340.

[15] The Security Committee, "Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020 (Implementation Programme for Finland's Cyber Security Strategy for 2017-2020)" (Helsinki: The Security Committee, 2017).

[16] The Security Committee, "Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society)" (Helsinki, The Security Committee, 2017).

[17] Traficom – About us, https://www.traficom.fi/en/traficom/about-us, accessed August 6, 2019.

[18] Kirsi Virrantaus and Hannes Seppänen, "Yhteiskunnan Kriittisen Infran Dynaaminen Haavoittuvuusmalli," Helsinki, Matine, Apr 10, 2014.

About the Authors

Jouni **Pöyhönen** holds an MSc. Degree in Industrial Development and Management. Retired Colonel, he is currently PhD student in cybersecurity in the Faculty of Information Technology at the University of Jyväskylä. He has over 30 years' experience as developer and leader of C4ISR Systems in the Finnish Air Forces. He conducts project-based research in the cybersecurity programs, and has already published several related research reports and articles.

Viivi **Nuojua** holds an MSc degree in statistics and works as information security specialist in the Jyväskylä Energy Group. She works in the group's development function, in a close collaboration with the IT management. She is part of the information security steering group and technical information security group, involved in the group's comprehensive cyber security development. She is also PhD student in Cybersecurity in the Faculty of Information Technology at the University of Jyväskylä.

Martti **Lehto** is retired Colonel holding PhD in Military Sciences, with over 40 years' experience in C4ISR Systems in the Finnish Defence Forces. Currently he is Professor (cyber security and defence) in the University of Jyväskylä, conducting research, teaching and managing the M.Sc. Security and Strategic programme. He is also Adjunct professor in National Defence University in air and cyber warfare, with over 140 publications on the areas of C4ISR systems, cyber security and defence, information warfare, artificial intelligence, air power and defence policy.

Jyri **Rajamäki** is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology and a PhD in mathematical information technology from University of Jyväskylä.

Annex 5 – Comparative research of cybersecurity information sharing models

by J. Simola

In vol. 43 of Information & Security: An International Journal, https://doi.org/10.11610/isij.v43

Information & Security

J. Simola, vol. 43, no. 2 (2019): 175-195
https://doi.org/10.11610/isij.4315

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Comparative Research of Cybersecurity Information Sharing Models

Jussi Simola

Laurea University of Applied Sciences R&D, Espoo Finland, https://www.laurea.fi/en/

ABSTRACT:

Cyber threats are on the increase. Authorities need to respond to growing challenges by increasing cooperation. Information sharing or information exchange in the EU level and between the countries is a main facility when the objective is to prevent hybrid threats. Intensifying relationships with private sector companies has become very important function and operating model to authorities to provide cyber-safe atmosphere. The main purpose of this study is to find out separating and combining factors concerning cyber information sharing models. The aim is also to find out nation level factors, which affect the utilization of a common Early Warning system by the ECHO stakeholders.

Summary of findings: unclear allocation of responsibilities in national government departments prevents authorities from fighting together against cyber and physical threats. Cybersecurity responsibilities have been spread too widely. Operational work concerning cyber threat prevention between European public safety authorities should be more standardized, with more centralized management. When the purpose is to protect vital functions of society, public safety organizations in EU member states need proactive features in their information systems. An essential factor in information exchange is the place of registration of organizations or companies. Unclear standardization concerning cyber emergency procedures between authorities and organizations and lack of co-operation between cyber situation centres and cyber emergency response centres prevent common situational awareness.

ARTICLE INFO:

RECEIVED: 20 JUN 2019
REVISED: 03 SEP 2019
ONLINE: 21 SEP 2019

KEYWORDS:

information sharing, Early Warnings, situational awareness, cooperation, ECHO project, indicators

E-mail: juhemisi@student.jyu.fi

Introduction

The purpose of this paper is to assist ECHO and E-EWS developers, European decision-makers 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. With the E-EWS ECHO stakeholders can retain their fully independent management of cyber-sensitive information and related data management. 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 transfer US- and NATO-related cyber information sharing models to Europe. The United States of America and European Union has a lot of similarities, but many differences. It is important to notice how global markets divide and integrate our entities where we live. There are territorial and cultural differences between the countries, but technological solutions create new kind of opportunities within EU member countries to reach the same situation as USA have concerning quality and quantity of threat-informed data. Comparative 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 sharing in the western world. Therefor 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. Agencies of The United States of America have enough resources to act proactively and use predictive functions in cyber space. This research belongs to European network of Cybersecurity centres and competence Hub for innovation and Operations, which is part of 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 Method and Process. Section 5 presents information sharing models and frameworks. Section 6 presents findings. Section 7 presents conclusion about the research.

Alert and Detection System

An alert and detection system produces information, which makes it 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. The information on situation awareness provided by the system increases understanding about the organization’s own and general state of information security.

CSIRT (Computer Security Incident Response Team) or 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.[1] 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) and Critical Information Infrastructure Protection (CIIP)

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.[2, 3] According to the Secretariat of the Security Committee of Finland, Critical infrastructure refers to the structures and functions which are necessary for the vital functions of society.[4] They comprise fundamental physical facilities and structures as well as electronic functions and services.

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.[5]

Cyber Threats in Critical Infrastructure

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 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 the US National Institute of Standards and Technology,[6, 7] Cyber-Physical attacks can be classified into three broad sections:

Physical attacks informed by cyber

The use of information gathered by cyber means that allows an attacker 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.

Cyber-attacks 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 adversary uses a cyber-system that controls physical equipment in such a manner to cause physical harm/damage. An example of this is the burner management system for a natural gas generator. In this case, an adversary 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 adversary could turn on the ignition source, potentially causing an explosion.

Good cyber, physical and operational security planning and implementations can minimize these impacts of cyber physical attacks. Defensive measures that can be used to minimize the likelihood of successful cyber-attacks and physical attacks will also work to minimize the impacts of a cyber-physical attack.

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. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA provides recommendations on cybersecurity, supports policy development and its implementation, and collaborates with operational teams throughout Europe.[8]

National Regulatory Authority (NRA)

NRAs can play different roles in relation to cybersecurity. In Finland, for example, the tasks are: Steering and supervision of telecoms operators' operations, information security and preparedness, for example, monitoring compliance with the

information security regulation, steering and supervision of strong electronic identification and the provision of qualified certificates, for example, monitoring compliance and carrying out annual audits of certification authorities providing qualified certificates.[9]

The European Cyber Security Organization (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 Sharing and Analysis Centres (ISACs)

ISAC is collaboration community created for sector-specific national or international information sharing. Information Sharing and Analysis Centres 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,[10] or support economic interests.[11]

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.[12]

Industrial Internet of Things (IIOT)

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. The major area where IOT deals with energy management systems is the smart grid. IOT extends the benefits of smart grid beyond the automation, distribution and monitoring being done by the utilities.[13]

Risk Assessment Framework (RAF)

According to the National Institute of Standards and Technology,[14] the purpose of risk assessments is to inform decision makers and support risk responses by:

- Identifying relevant threats to organizations or threats directed through organizations against other organizations;
- Identifying vulnerabilities both internal and external to organizations;
- Impact to organizations that may occur given the potential for threats exploiting vulnerabilities and

- 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.

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."[15]

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.[16]

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.[17]

Organizational Bases of Cybersecurity 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, analysing 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 (CPTs) creates security for all states in USA. NATO does not have an inherent cyber offensive capability, as the U.S Cyber CPT has.

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.[18] NATO does not have own cyber weapons against

cyber-attacks. The U.S.-led alliance established an operations centre on August 31, 2018 at its military hub in Belgium and the USA, Britain, Estonia and other allies have since offered their cyber capabilities.[19]

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 USA.[20]

Background of Information Exchange among USA and EU

Are there differences between information sharing, transferring information and information exchange? In 2009 ENISA, the European Network and Information Security Agency, defined the difference as follows: An *information exchange* is a form of strategic partnership among key public and private stakeholders. The common goal of the 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.[21]

The European Commission presented the cybersecurity strategy of the European Union in 2013. 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 – the national Network and Information Sharing competent authorities should collaborate and exchange relevant information with other regulatory bodies.[22]

The European Public-Private Partnership for Resilience (EP3R) was established in 2009 and was the very first attempt at 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.[23, 24]

Development of Information Exchange in Law Enforcement

How to prevent criminal activities has been one of the main questions 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.[25]

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.[26]

The Schengen Information Systems (SIS) is widely used information sharing tool today. Law enforcement authorities can use it to consult alerts on wanted persons etc. both inside the EU and at the EU external border. The SIS improve 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). The Swedish decision sets out how information should be exchange between EU Member States.[28]

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.[29]

Legislation and regulation concerning information exchange in USA and Europe

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.

The communications Information Sharing and Analysis Center (Comm-ISAC) incorporating dozens of organizations. 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.[30]

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. The Ombudsperson mechanism means that an independent senior official within the U.S. Department of state will ensure that complaints are properly investigated and addressed in a timely manner.[31]

Regulation in European Union

The list of the most relevant regulation taken into consideration in EU level.

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.

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, or the *NIS Directive* 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.[32] 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.[33]

The NIS Directive consist of 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),

ex-post supervision for critical digital service providers (internet exchange points, domain name systems, etc).

General Data Protection Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council 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, or the General Data Protection Regulation (GDPR) replaced 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.[34] The Regulation introduces stronger citizens' rights as new transparency requirements. It strengthens the rights of information, access and the right to be forgotten. 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 is organized in accordance with pre-defined criteria.[35] 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. Personal data consists 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.

Other Relevant Regulations

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
- European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cybersecurity (2011/2284(INI)) (CIIP)
- COM(2017) 477 final 2017/0225 (COD) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency," and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")
- COM(2016) 705 final Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Space Strategy for Europe"
- JOIN(2014) 9 final - Joint Communication to the European Parliament and the Council "For an open and secure global maritime domain: elements for a European Union maritime security strategy"

- JOIN(2016) 18 final Joint Communication to the European Parliament and the Council "Joint Framework on countering hybrid threats a European Union response"
- EU Cyber Defence Policy Framework [Concilium 15585/14] and Joint Communication on "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," February 2013 [JOIN(2013)1].[36]

Method and Process

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, collected articles and literary material. The research is focused on how it is possible iterate USA-related research concerning cyber information sharing models in Europe. Yin identifies five components of research design for case studies:[37] (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 following the guidance by Yin.

There are country-specific differences, institutional differences, etc. legislative differences in legislation, etc. The purpose is to categorize things into their own groups. Some models 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 and features of information sharing systems in the EU, USA and NATO. The results of the research will be utilized in developing the echo early warning system.

Definition of information sharing

According to NIST,[38] 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.

Define information sharing goals

According to Skopik and co-authors,[39] the primary dimensions of security information sharing can be divided as follows: a) Cooperation and coordination economic need for coordinated cyber defence. 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 centres 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.

Identify Internal Sources of Cyber Threat Information

The 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 defences. CORA identifies five major areas of cyber security where the proper introduction of threat information can have tremendous impact on the efficacy of defences: 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.[40] Examples of PIRs include:

- Threats and threat actors that have attacked your specific organization previously
- Vulnerabilities and exploits that pertain to technology specific to your organization or industry
- Threats and attacks against industry/sector peers or business partners.[41]

A first step in any information sharing effort is to identify sources of threat information within an organization. By conducting an inventory of internal threat information sources, an organization is better able to identify knowledge gaps. The process of identifying threat information sources includes the following sections: [42]

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 analysed as part of an organization's continuous monitoring strategy;

c) Locate threat information that is collected and stored, but not necessarily analysed 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.

Table 1 provides illustration through modified examples of selected internal cybersecurity-related information sources with human factors from NIST.

Table 1. Examples of cyber threat sources (modified from NIST).[43]

Human Factors & Network Data Sources		Human Factors & Host data Sources	
Sources	*Examples*	*Sources*	*Examples*
Router, firewall, equipment, Wi-Fi, remote services (such as remote login or remote command execution), and Dynamic Host Configuration Protocol (DHCP) server logs	Timestamp Source and destination IP address Domain name TCP/UDP port number Media Access Control (MAC) address Hostname Action (deny/allow) Status code Other protocol information	Operating system and application configuration settings states and logs	Bound and established network connection and port Process and thread Registry setting, Configuration file entry, Software version and patch level information Hardware information, User and group File attribute (e.g., name, hash value, permissions, timestamp, size) File access System event (e.g., startup, shutdown, failures), Command history
Diagnostic and monitoring tools (network intrusion detection and prevention system), packet capture & protocol analysis	IP address, port, and other protocol information Network flow data Packet payload Application-specific information Type of attack (e.g., SQL injection, buffer overflow) Targeted vulnerability Attack status (success/fail/blocked)	Antivirus products	Hostname, IP and MAC address, Malware name and type (e.g., virus, hacking tool, spyware, remote access) File name and location (i.e., path) File hash Action taken (e.g., quarantine, clean, rename, delete)
Human Factors & Other Data Sources		Web browsers	Browser history and cache including: Site visited; Forms, Social media platforms, Object downloaded; Object uploaded; Browser extension installed or enabled; Cookies; Transactions
Security Information and Event Management (SIEM)	Summary reports synthesized from a variety of data sources (e.g., operating system, application, and network logs)		
Email systems	Email messages: Email header content - Sender/recipient email address - Subject line - Routing information Attachments, URLs, Embedded graphic		
Help desk ticketing systems, incident management/tracking system and human activity within the organization	Analysis reports and observations regarding: TTPs, campaigns, affiliations, motives, exploit code and tools, Response and mitigation strategies, Recommended courses of ac-		

	tion, User screen captures (e.g., error messages or dialog boxes)		
Forensic toolkits and dynamic and/or virtual execution environments	Malware samples, system artifacts (network, file systems, memory)		

Handling requirements for shared threat information

There are many methods to share designations of threat information. The TLP specifies a colour-based set of restrictions that indicate which restrictions apply to a particular record. The Traffic Light Protocol provides a framework for expressing sharing designations.[44]

The TLP is widely used mechanism to classify threat information. Despite the mechanism, it would be necessary identify a mechanism to ensure that the confidentiality of TLP-marked information was not compromised through Freedom of Information (FOI) e.g. National Act on the openness of government activities. It is good to conclude anonymization by National Regulatory Authority (NRA) when sharing information at the European level.

In the TLP, red specifies the most restrictive rule with information sharable only in a particular exchange or meeting, not even within a participant's own organization. TLP consists four colours for different threat levels. The amber, green, and white colour codes specify successively relaxed restrictions. RED It is not for disclosure and it is restricted to participants only. Sources may use RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party´s privacy, reputation or operations if misused. TLP-AMBER illustrates limited disclosure and it is restricted to participants' and organizations. Sources may use TLP-AMBER when information requires support to be effectively acted upon, yet carries risks to privacy or operations if shared outside of the organizations involved. TLP-GREEN is for limited disclosure and it is restricted to the community. Sources may use TLP-GREEN when information is useful for the awareness of all participating organizations but also with peers within the community or sector. TLP-WHITE is not limited. Sources mays use TLP-WHITE when information carries minimal or no foreseeable risk of misuse.

Comparing features of the information sharing models

The main international working groups are Association for Computing Machinery (ACM), National Institute of Standards and Technology (NIST) Institute of Electrical and Electronics Engineers (IEEE) European Telecommunications Standards Institute (ETSI), international Federation for Information Processing (IFIP). NIST Framework is most commonly used of these mentioned above.

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. Table 2 illustrates five different type of models has chosen to more detailed review.

Table 2. Examples of information sharing models.

Organization // Name // System/model or framework type	Main tasks/ features	Special tasks	Major areas of cyber impacts	Instruments
MITRE// CORA // Assessment of cyber operations Based on NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing. MITRE is 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		External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	Using indicators to 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 (incorporates threat information into its regular security practices).		External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	Sensors (IDS, HIDS); (IOC) or attack activity such as phishing email addresses, IP addresses and URLs of malicious sites, host-based indicators such as files, registry keys, and process elements.
ENISA// ISAC// Member driven organization model ENISA is a centre of expertise for cyber security in Europe Country-focused ISAC	Sharing knowledge about incidents and cybersecurity. It helps raise the level of cybersecurity in the member organization and prevent/ respond to	ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It provides information	a) a common practice to establish so called “circles of trust.” Some information (e.g. technical details about threats and incidents) can be shared	web portal/platform (following a specific template) and encrypted emails

Sector specific ISAC// Focused on the sectorial level of critical infrastructure or essential/vital sector International ISAC	the incidents which occur (ISAC is a fast and efficient way to get all the knowledge and experience which normally takes a lot of time. ISAC is a good way of networking and meeting people from different organizations. It also provides knowhow)	about threats and incidents. (close cooperation with the industry, public entities get better understanding of the private sector)	widely with all members b) the shared information is more detailed in internal circle c)use of the (TLP) to share information	
ENISA// PPP// Cooperative model	Access to public funds		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
	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 – allows to meet different people and get to know them; because of that, it allows to have better information and proactive attitude in case of crisis.			
NIST// Framework// Framework The National Institute of Standards and Technology is part of U.S Department of Commerce	NIST FW targeting on risk management, procedures and privacy preservation aspects. The guidelines included in the ISO/IEC27010 standard, itis oriented toward the protection of the data exchanged in the information sharing process, as well as to the collection, analysis and correlation of cyber incidents in order to obtain an effective mitigation strategy.		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

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.[45] The entire information-sharing mechanism will not work well if the hub is not working well. 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. There must be deeper trust in environment. Environment should be strengthened through face-to-face meetings and individuals who have a long history of personal rapport. 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 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.

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. The notable problem is that all countries in EU are not full member of NATO. Most of the member countries of European Economic Union belongs to NATO alliance. Organizational aspect does not mean that Finland or Sweden are outsiders in all sectors in this military alliance. Partnership makes it possible to utilize ready-made information sharing networks developed by NATO. It is important to understand the difference between a partnership and a membership. 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." NATO is currently dependent on the cyber defence ability of the United States and the EU has no ability to respond to external cyber threats.

As many politicians and officers has mentioned functionalities between cyber situation centres within European Union are too scattered. Separate functionalities in the member states are not only problem. When the common goal is to im-

prove 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 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.

Conclusions

There is tendency in Europe that private actors are allowed more rights to handle citizens' privacy data. For example, the bank sector has had opportunity to process and handle account data of customers. At the moment, this right is being expanded to other activities. Legislation is not the only factor which affects the chances to completely secure the cyber ecosystem. It is important to notice that information sharing systems or frameworks are useless without features and functionalities. The USA and its public safety cyber defence organizations have ability to combat cyberattacks against vital functions, but also to counterattack. This is one of the most important features in protecting the western world. Cooperation and collaboration in triangle EU-NATO-USA is therefore particularly important. 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 trust organization's functionalities is occasional. What are the organisations, which handle the databases concerning privacy issues and what for they handle it? Where companies and organisations are registered? Does it cause obstacles and can they be overcome when the aim is to catch cyber criminals or find out state level actor utilising cyber or hybrid attacks. The differences between the functionalities and features of information sharing models in USA and NATO versus European Union models for information exchange are converging only if EU develops towards a federal state.

Acknowledgement

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943.

References

1 ENISA, "Good Practice Guide – Network Security Information Exchanges," 2009.

2 The Department of Homeland Security (DHS), "Blueprint for a Secure Cyber Future – The Cybersecurity Strategy for the Homeland Security Enterprise," DHS, 2011.

3 Ministry of the Interior of Finland, "National Risk Assessment," Helsinki, 2018.

[4] Secretariat of The Security Committee of Finland, *Finland´s Cyber Security Strategy – Government Resolution* (Helsinki: Ministry of Defence, 2013).

[5] Matthew P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (National Institute of Standards and Technology, NIST, April 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018.

[6] Barrett, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.

[7] Victoria Y. Pillitteri and Tanya L. Brewer, *Guidelines for Smart Grid Cybersecurity*, Volume 2, "Privacy and the Smart Grid" (National Institute of Standards and Technology, September 25, 2014), https://doi.org/10.6028/NIST.IR.7628r1.

[8] ENISA, "Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS)," European Union Agency for Network and Information Security, 2013.

[9] Latif Ladid, Jart Armin, and Heidi Kivekäs, "Whitepaper: The Finish Electronic Communications Regulator TRAFICOM – A Cybersecurity Reference Model for Europe," Helsinki, SAINT Consortium/Traficom, 2019.

[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," *Official Journal* L 194, July 19, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[11] ENISA & ITE, "Information Sharing and Analysis Centers (ISACs) Cooperative Models," European Union Agency for Network and Information Security, 2017.

[12] Greg White and Rick Lipsey, "ISAO SO Product Outline," ISAO Standards Organization, May 2, 2016.

[13] Electrical Technology, "Internet of Things (IOT) and Its Applications in Electrical Power Industry," last update 2016, http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html, accessed August 11, 2016.

[14] National Institute of Standards and Technology, Guide for Conducting Risk Assessments, SP 800-30 Rev. 1, Publication 800-30 (Gaithersburg, MD: U.S. Department of Commerce, 2012), https://doi.org/10.6028/NIST.SP.800-30r1.

[15] *Information Technology — Security Techniques — Information security Management for Inter-sector and Inter-organizational Communications*, ISO/IEC 27010:2015, https://www.iso.org/standard/68427.html.

[16] Christopher Johnson, Mark Badger, David Waltermire, Julie Snyder, and Clem Skorupka, "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150 (Gaithersburg, MD: National Institute of Standards and Technology, 2016), https://doi.org/10.6028/NIST.SP.800-150.

[17] Johnson, et al., "Guide to Cyber Threat Information Sharing."

[18] Piret Pernik, Jesse Wojtkowiak, and Alex Verschoor-Kirss, *National Cyber Security Organization: United States* (Tallinn: NATO CCD COE, 2016).

[19] Brad Bigelow, "The Topography of Cyberspace and Its Consequences for Operations," *10th International Conference on Cyber Conflict 2018* (Tallinn: NATO CCD COE, 2018).

[20] Bruce J. Bakis and Edward D. Wang, "Building a National Cyber Information-Sharing Ecosystem," MITRE Corporation, 2017.

[21] ENISA, "Good Practice Guide – Network Security Information Exchanges."

[22] ENISA & ITE, "Information Sharing and Analysis Centers (ISACs) Cooperative Models."

[23] NESA, "EP3R 2013 – Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS)," European Union Agency for Network and Information Security, 2013.

[24] NESA, "Public Private Partnerships (PPP) Cooperative models," European Union Agency for Network and Information Security, 2017.

[25] "Migration and Home Affairs," Information exchange, European Commission, June 17, 2019, https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange_en.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] European Commission, "Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions," Brussels, European Commission, 2013, https://eur-lex.europa.eu/procedure/EN/202369.

[31] European Commission, "EU-U.S. Privacy Shield: stronger protection for transatlantic data flows," Brussels, 2016.

[32] "NIS Directive," Homepage of European Union Agency for Network and Information Security, https://www.enisa.europa.eu/topics/nis-directive.

[33] Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen, Kyberturvallisuuden strateginen johtaminen Suomessa," Julkaisusarja 28/2018 (Helsinki, Valtioneuvoston kanslia, 2018).

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council 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, May 4, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[35] Ibid.

[36] Igor Nai Fovino, Ricardo Neisse, Alessandro Lazari, Gian-Luigi Ruzzante, Nineta Polemi, and Malgorzata Figwer, "European Cybersecurity Centres of Expertise Map – Definitions and Taxonomy," Luxembourg, Publications Office of the European Union, 2018.

[37] Robert K. Yin, *Case Study Research, Design and Methods*, 5 ed. (Thousand Oaks, Sage Publications, 2014).

[38] Johnson, et al., "Guide to Cyber Threat Information Sharing."

[39] Florian Skopik, Giuseppe Settanni, and Roman Fiedler, "A Problem Shared is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense Through Security Information Sharing," *Computers and Security* 60 (July 2016): 154-176.

[40] Clement W. Skorupka and Lindsley G. Boiney, "Cyber Operations Rapid Assessment (CORA): A Guide to Best Practices for Threat-Informed Cyber Security Operations," The MITRE Corporation, February 2016, http://www.mitre.org/publications/technical-papers/cyber-operations-rapid-assessment-cora-a-guide-to-best-practices-for.

[41] MITRE, "Cyber Information-Sharing Models: An Overview," MITRE Corporation, 2012, https://www.mitre.org/publications/technical-papers/cyber-informationsharing-models-an-overview.

[42] Johnson, et al., "Guide to Cyber Threat Information Sharing."

[43] Ibid.

[44] Ibid.

[45] MITRE, "Cyber Information-Sharing Models: An Overview."

About the Author

Jussi Simola is a PhD student of cyber security in University of Jyväskylä. His area of expertise includes decision support technologies, situation awareness systems, information security and continuity management. His current research is focused on the effects of the cyber domain on the hybrid emergency response model.