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]

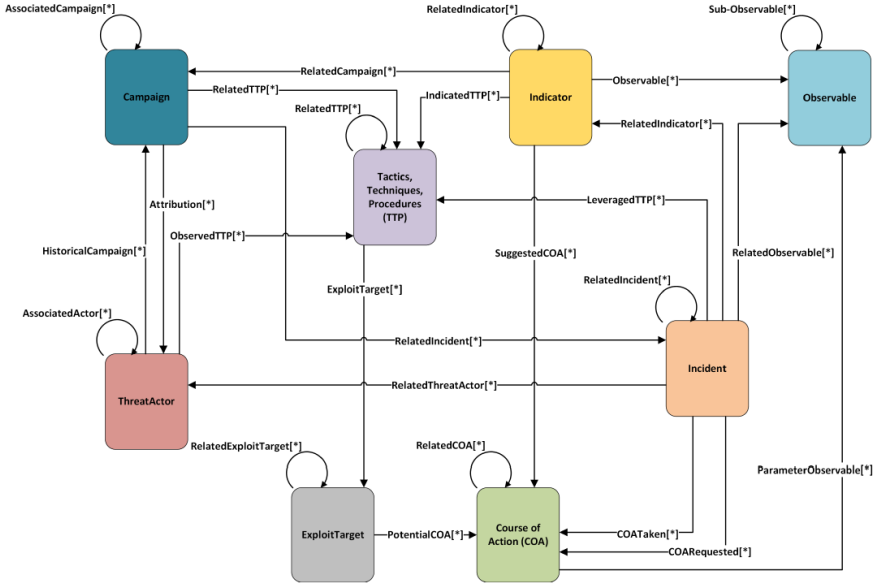

Figure 1: Architecture of STIX™.[18]

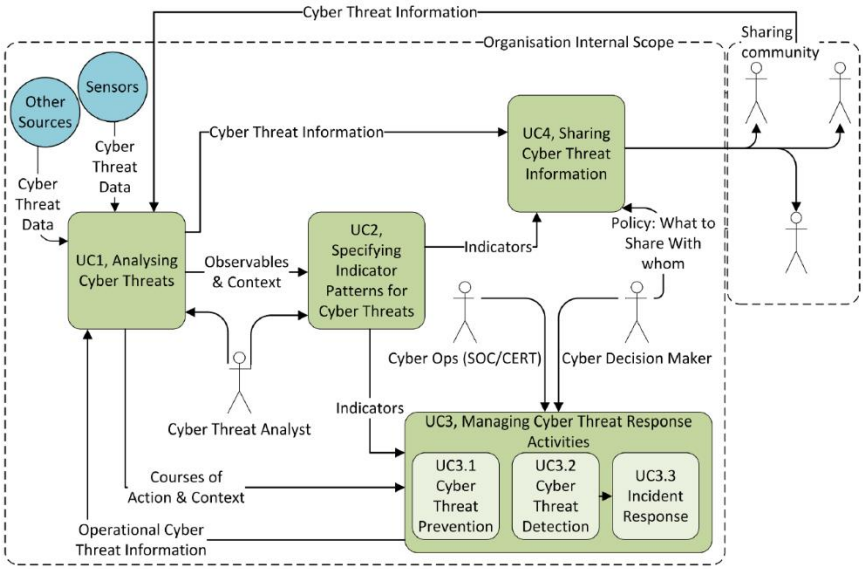

Figure 2: Example of STIX™ use case.[18]

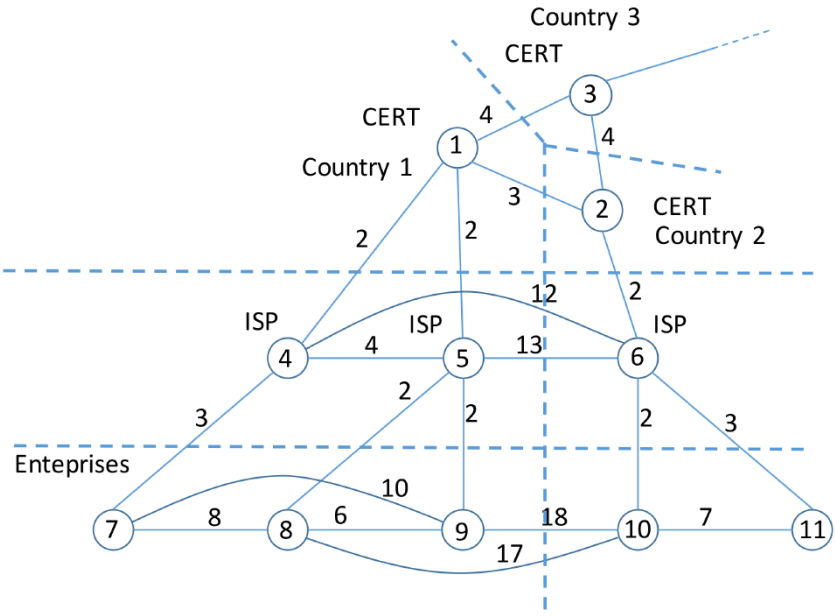

Figure 3: Cyber security information sharing community.[18]

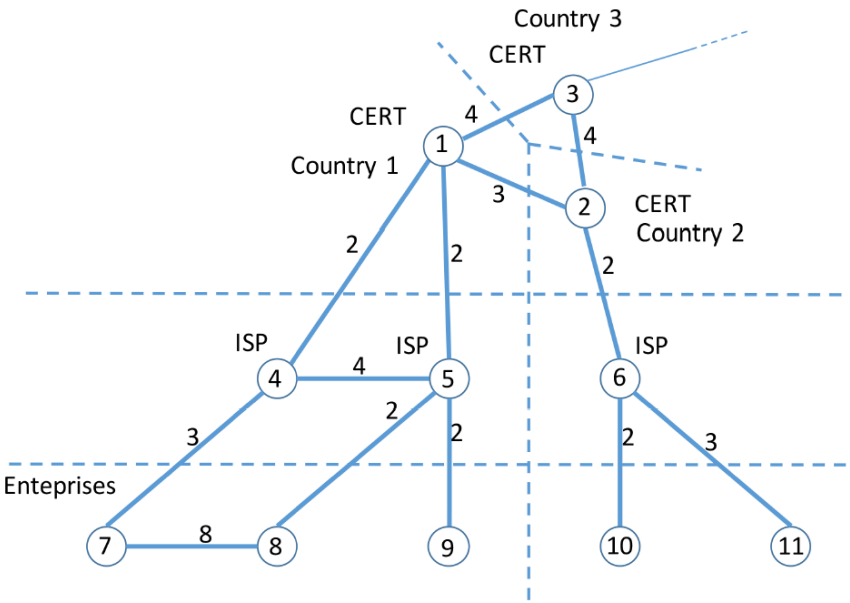

Figure 4: Cyber security information sharing topology with a minimum risk level implementation.[18]

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).

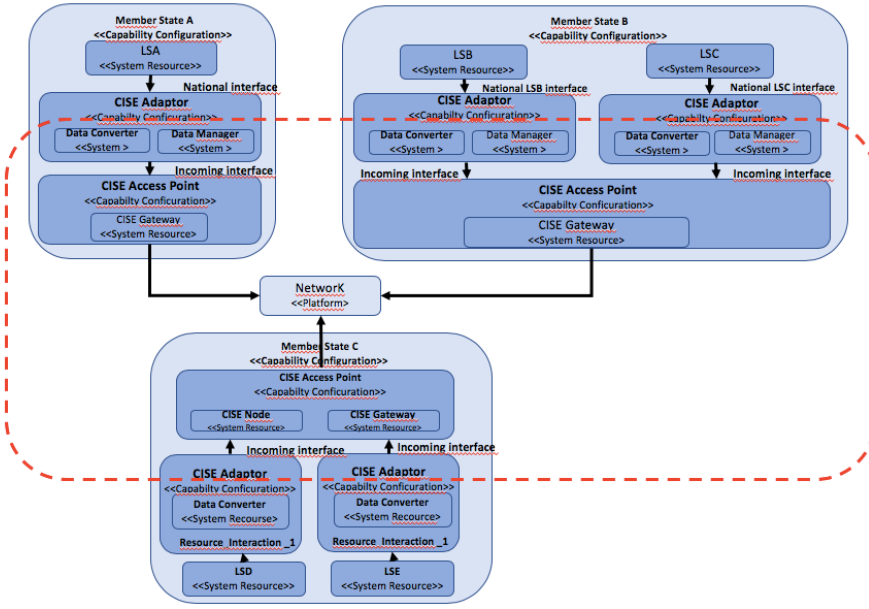

Figure 5: Logical Architecture of EUCISE2020 configurations A, B and C.

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.

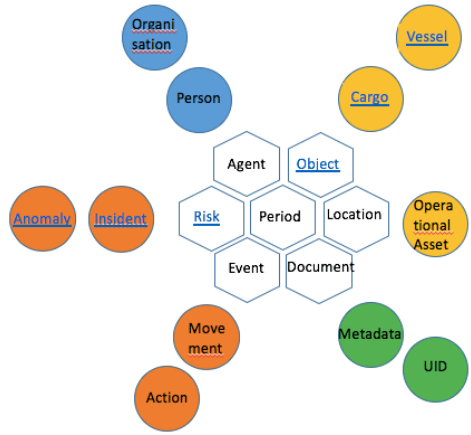

Figure 6: CISE data model (EUCISE2020 D4.3 Annex B).

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.