The Impact of Operational Technology Requirements in Maritime Industries

Jussi Simola[1], Pia Satopää[2], Jarkko Paavola[2] and Jani Vanharanta[2]
[1]University of Jyväskylä, Finland
[2]Turku University of Applied Sciences, Finland

jussi.hm.simola@jyu.fi
pia.satopaa@turkuamk.fi
jarkko.paavola@turkuamk.fi
jani.vanharanta@turkuamk.fi

Abstract: The maritime ecosystem and industry require more efficient and coordinated cybersecurity governance. No common cybersecurity mechanism in the maritime sector may steer the whole supply chain management, for example, in the port areas and fairways. Cyberthreat prevention mechanisms in harbor areas and port terminals must be standardized more in the Western world. It has been recognized that understanding cybersecurity of operational technology in the harbor area is based on a more traditional experience of what it requires. The overall security of the maritime ecosystem requires more than random checks of passengers and vehicles and customs functions on cargo and passenger transportation, which are mainly physical security service routines. Traditional physical threats have changed to a combination of threat types. Hybrid threats may prevent everyday harbor activities so that damage can become long-lasting and harm overall business continuity management. It is crucial to prevent cyber threat factors in the maritime domain. The research provides transnational and EU-level cyber security assessments regarding cyber security regulation. The findings determine where to direct and concentrate a focus maritime domain and why it is essential to survey cyber security requirements set for member states to apply. In Finland, this research belongs to the cybersecurity governance of operational technology in the sector connected to the smart energy networks (CSG) research program. The project aims to develop a common cybersecurity governance model for operational technology.

Keywords: Operational Technology, Overall Situational Awareness, Maritime Cybersecurity, Governance Model

1. Introduction

The cybersecurity governance of operational technology in the sector connected to smart energy networks (CSG) research program will create a new governance model for the energy sector actors by developing operational technology standardization. One of the project's main aims is to develop a common cybersecurity governance model for operational technology. The maritime ecosystem is crucial to critical infrastructure protection. Transportation is a central national economic factor that allows the national-level supply chain to continue. If the supply chain is disrupted, security maintenance and continuity management prevent overall security. The research will find the main challenges concerning the cybersecurity governance of the industrial organizations in maritime clusters that use operational technology-related technology in their daily businesses.

Maritime cybersecurity has become increasingly crucial due to the growing and ever-evolving cyber threats. Stakeholders in the maritime industry must recognize their role as critical infrastructure operators and manage cybersecurity risks and threats that could impact maritime security, service continuity, or broader logistics chains.

2. Key Concepts

2.1 Maritime Situational Awareness

Ministry of Defence (2010) describes situational awareness as the understanding of the advisors and decision-makers of what has happened, the circumstances under which it happened, the goals of the different parties, and the possible development of events, all of which are needed to make decisions on a specific issue or range of issues. A common definition of situational awareness is the perception of the elements in the environment within time and space, the comprehension of their meaning, and the projection of their status soon (Endsley, 1988). It is knowing what is going on around you. It consists of continuous monitoring of relevant sources of information regarding actual incidents and developing hazards (Homeland Security, 2008).

The maritime cluster comprises several maritime-connected sectors that create the interacting entity (NESA 2020, 2021). Achieving common or Shared Situational Awareness (SSA) requires a common understanding of shared situational awareness that consists of similar unchanged elements at every stage. Sectors of the maritime

domain cannot cooperate by forming their understanding of the entity independently from other actors. Thus, common maritime situational awareness is crucial in undistributed continuity management. It is useful to classify sector-based situational awareness for creating coherent entities. System of system-level thinking depends on the human ability to understand the dependencies of supply chains. Developing a framework for the smaller components is only possible if we can influence the relationships regarding the system and business dependencies.

Situational awareness can be divided as follows. Technological – Organizational – Situational awareness of human resources – Situational awareness of business management – Situational awareness of transportation – Situational awareness of regulations and policies. If all segments are well-defined and linked to each other in a way that information sharing and exchange support core functions, shared situational awareness could be achievable. Common situational awareness differs from shared situational awareness. In a concept meaning, common means a level of understanding (Endsley, 1995;1998).

2.2 Background of the Cybersecurity Governance

EU's cybersecurity strategy is the upper-level framework for national-level cybersecurity (European Commission, 2020a, 2022). The Western world has a common vision of achieving the strategies' goals (Lété, 2017;ENISA, 2023). NIS2 directive (European Commission, 2022a) states that every EU member state has been required to adopt a National Cybersecurity Strategy (NCSS) and establish a cyber security governance model. At a general level, as a part of corporate governance, several elements are related to the formation of cybersecurity governance. The frameworks are connected to each other in an essential way. Crucial vulnerability elements of security and cyber security consist of people, processes, and technical aspects (European Commission 2022a; 2023).

Port facility's cyber risk management requires a collective effort; the organization should define who has overall oversight of the cyber risk program. Owners, shareholders, and institutional investors (e.g., private equity) evaluate cyber risk in terms of risk to investments.

Operational cyber risk management oversight lies with those individuals who have ultimate responsibility, for example, in the governance of the port authority or port facility. That could be the CEO, Managing Director, or other designee, and their responsibility includes Board-level reporting (IAPH,2020;2021).

The European Union Agency for Cybersecurity ENISA (2023) proposed a governance model consisting of four main layers with 10 sub-categories, providing 28 practices. The main principles are demonstrated in Table 1.

Table 1: Tiers of Governance Model by Enisa (2023)

Layers of the governance	The Main Principles
Political governance	Political processes. Roles and responsibilities; and legal measures.
Strategic governance	Strategy itself and its implementation; and Risk identification and mitigation.
Technical governance	International standards and technical guidelines; and use of technology, tools, and certification schemes
Operational governance	Awareness raising. Incident response; and Information sharing.

The Operational Technology Governance process includes the following minimum requirements. a) The OT cybersecurity policy is established and communicated. b) OT cybersecurity roles and responsibilities are coordinated and aligned with the internal roles and external partners. c) legal and regulatory requirements regarding OT cybersecurity, including privacy, are understood correctly and managed. d) The cybersecurity risks are integrated into corporate risk management processes (NIST, 2023). According to the CISA (2024), features of the Cybersecurity Governance strategy may consist of the following issues: Accountability frameworks – Decision-making hierarchies –Defined risks related to business objectives – Mitigation plans and strategies – Oversight processes and procedures (CISA, 2024)**.** Cybersecurity governance has been understood in different ways. Cybersecurity governance may consist of the following tiers.

2.2.1 Vision and Strategy

There should be a common understanding between national regulation and organizations' cyber security strategy connected to corporate governance strategy. The crucial elements are connected to human resource training, risk management, information sharing, and security of the business processes and technologies. Vendors and investors must be informed about cybersecurity's vulnerabilities and risks. Third-party-related partners have crucial roles in the framework. Every organization that is connected to the critical infrastructure must create cybersecurity governance based on the EU regulations.

2.2.2 Exact Roles and Responsibilities

Organizations have to create clear plans about who is responsible for risk management and cybersecurity risk management, and they have to early warn authorities and other sector-based operators within 24 hours. The observed vulnerability, cyber-attack, or potential threat must be reported to national cybersecurity authorities within 72 hours (European Commission, 2022b).

2.2.3 Combined Risk Management - MSMS Maritime Cyber Security Management System.

Workable risk analysis requires an assessment of the potential vulnerabilities and risks. That is connected to the organization's business strategy. It has been determined what the acceptable risk level is and how to react against cyber or cyberphysical risks. Crucial is how the auditing process is done.

2.2.4 Cyber Security Steering Group

There should also be a steering group that supervises other decision-makers regarding cybersecurity. The steering group gathers and shares the relevant information and transfers information to other closely linked managing groups.

2.2.5 Cyber Security Programme

Cyber security strategy requires a cyber security program to achieve the strategic goals. It is not enough for management or the board of directors to understand what issues are included. Employees must know and understand what they must do to achieve the details and how they reach the goals set by the company.

2.2.6 Measurement and Reporting at all Business Hierarchy Levels

In a wider perspective, companies must implement measures that support maintaining situational awareness. Companies must have business measures that guide the direction of the business. The cyber security measures are only one part of the clarification of the state of the company. Costs must stay the same, but it costs more if cybersecurity requirements still need to be implemented.

2.3 Regulation and Guidelines

The minimum level of the NIS 2 directive (2022/2555) for national regulation will be implemented in October

2024, and legislation will be applied to the operational environment in 2025. It will create cybersecurity measures and require organizations, and EU member states to inform EU-level agencies about cyber threat events and incidents. The NIS2 concentrates mainly on cyber security risk management, strategy planning, and information exchange concerning situational awareness of governance (European Commission, 2022a). The European Cyber Resilience Act (CRA) 2019/1020 aims to create framework conditions for developing secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout the product lifecycle (European Commission, 2022b) It also aims to create conditions under which users can consider cybersecurity when choosing and using products with digital elements. Critical Entities Resilience (CER) (2022/2057) Directive consists of minimum regulation whose purpose is to enhance cyber resilience. It is based on the security strategy of the European Union (European Commission, 2020b).

International Maritime Organization´s (IMO) International Maritime Solid Bulk Cargoes Code (IMSBC Code) IMO Resolution MSC.428(98) offers views of the cyber risks, which companies should try to address as far as possible in the same way as any other risk that may affect the safe operation of a ship and protection of the environment (IMO, 2022). IMO has released with the International Labour Organization (ILO) the International Ship and Port

Facility Security (ISPS) Code of Practice on port security, which contains requirements relating to the ship's security and the immediate ship/port interface. Global BIMCO is the largest international shipping association representing the interests of ship owners, charterers, brokers, and agents. The BIMCO's primary role is the preparation of global regulations and policy recommendations in many areas related to maritime training services, from the environment, crew support, and insurance to maritime safety and security and digitalization, including guidelines for maritime cybersecurity. (Atlantic Council, 2021). European Maritime Safety Agency (EMSA) works under the European Union and serves the EU's maritime interests for a safe, secure, green, and competitive maritime sector in Europe and worldwide. EMSA is an essential stakeholder in the maritime cluster in Europe and beyond. It provides services to the EU Member States and the Commission but is also an innovative knowledge hub for the European maritime environment. (European Maritime Security Agency 2022).

2.4 Security Operations Center (SOC) and Cyber Risk Management

The Security Operations Centers in harbors have risen as the potential for hybrid threats increases in the maritime domain (U.S Coast Guard, 2020). Cyber and physical threats as a part of overall security management must be understood so that security personnel and the cyber emergency response team maintain shared situational awareness based on joint guidance and codes.

2.5 Port State Control (PCS)

Port authorities may use the Port community system as a part of the security management systems. As previous studies regarding maritime security indicate in Finland, we do not have advanced digitalized systems that comprise crucial security features under the same umbrella (Simola, Pöyhönen, Lehto, 2023a).

3. Processes, Humans, and Technologies Comprise Common Situational Awareness

Thinking from the view of technology or human processes in their daily work. it has been seen that requirements for understandable language are almost the same. It is crucial to analyze how people and technology communicate with each other. Devices must understand each other, but humans must also have a common language to understand different kinds of events and how they should react to them. Interfaces play a crucial role. Processes have an essential role in supporting each other. All these factors have to create seamless connections. For example, if stakeholders use different kinds of taxonomy in their information or data exchange procedures, advanced technology doesn't generate added value. As Mica Endsley discussed, situational awareness is based on a common level of understanding and creating a mental model for the stakeholders (Endsley, 1995;1998), as Figure 1 illustrates.

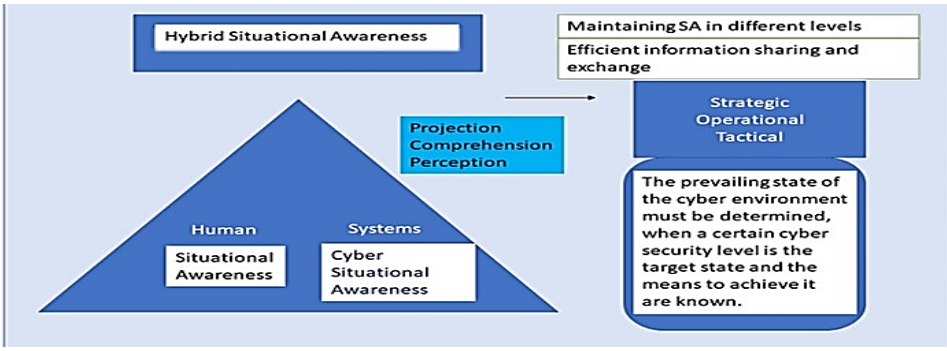

Figure 1 Formation of hybrid situational awareness (Simola, Pöyhönen & Lehto 2023b)

Maintaining situational awareness at the goal state requires a coherent strategic, operational, and tactical level of semantic functionalities where human and system-based information is shared understandably. The capability to understand threats and events creates a fundamental base to maintain everyday situational awareness. Cybersecurity strategies, threat prevention mechanisms, and prevention measures are equally important at a general level.

3.1 The Need for Common Situational Awareness in the Maritime Cluster

The maritime cluster is a crucial factor in the security of maintenance. If maritime industry-related stakeholders cannot secure the maritime cluster from supply chain-related vulnerabilities, it is possible that cyberattacks may cause interruption, and continuity management becomes difficult. According to Chubb N., Finn P., NG D., (2021),

the maritime industry has a critical role in the global supply chain. But the industry also relies on its own supply chain. That means the supply chain means how reliable the movement of products from port to port or from the production line to the customers, but also how information and data are transferred from the technical level to the operational and strategical level and vice versa. There are several elements that affect each other.

4. Cybersecurity Threats in Maritime

Cybersecurity threats in maritime are diverse and can target various entities, including port operators, logistics in ports, communication and surveillance systems, satellite and navigation systems, and the vessels' own systems. Cyberattacks can lead to severe issues such as alterations in ship routes, cargo losses, or even accidents. Future cyber threats may become more complex with the increasing digitization and automation of maritime traffic. The deployment of autonomous vessels, for example, may open new opportunities for cyber-attacks. A large ship with many electrical onboard components and systems forms a complex cyberphysical system-of-systems. Navigational systems, propulsion systems, electrohydraulic ballast tanks, intering tank stabilizers and several other industrial control systems (ICS) are vital to the safe operation of the ship. The operational technology (OT) onboard, similarly to control systems in the past, are often considered as isolated and disparate control systems which are operated only by onsite personnel in physically controlled limited-access-areas. In practice, however, the level of automation and the number of ICT systems interfacing with OT has been on the incline, effectively exposing some of the OT to the internetwork (NESA, 2021; Tuomala, V. 2023).

According to the (NESA, 2021), current Identified Threats in the Cyber Dimension may include:

1. Cyber-Physical Attacks: Targeting physical systems, such as a ship's navigation or engine systems, with the aim of disrupting their operations.
2. Ransomware: Attackers may seize control of a system and demand a ransom for its release.
3. Phishing Attacks: Attackers may send deceptive messages appearing to come from a trusted source, aiming to trick users into revealing passwords or other sensitive information.
4. Insecure IoT Devices: IoT devices used on ships can be vulnerable to attacks if not properly secured.
5. Supply Chain Attacks: Attackers may target a ship's systems through a third party, such as a supplier or subcontractor.
6. Insider Threats: Individuals within the organization may intentionally or unintentionally pose cybersecurity risks.
7. Outdated Software: Aging software may contain vulnerabilities that attackers can exploit.
8. Weak Authentication: Poor password practices or inadequate authentication methods can allow unauthorized access to systems.
9. Data Breaches: Attackers may infiltrate systems and steal sensitive information.
10. State-sponsored Cyber Espionage: States may use cyber attacks for intelligence purposes or to disrupt the operations of other states.

4.1 Hardest Managed and Detected Risk Scenarios

The research Simola, Pöyhönen, Lehto (2023b) indicates that third party-related factors cause essential challenges in maritime clusters, as shown Table 2 below. Those are mainly related to the service providers.

Table 2: Threat scenarios

Examples of threat scenario sources	Threat sources
Lack of human resource management (part-time employees, accountancy services, maintenance companies)	3d party service providers (Companies and their governance)
The software consists of a threat base.	3d party Compromised legitimate software (hijacked ICS software)
The vulnerability on hardware components.	3d party hardware, port equipment, cameras, drones, routers, sensors, devices and other unknown adverse components'
Intentional and unintentional human errors caused by lack of training, changing personnel, management of rights of access and use	Human errors

5. Research Approach

This research concentrates on industry-specific cybersecurity requirements in the maritime cluster. The members involved in this analysis process are researchers and research methods. Cybersecurity experts from the research program advocate Delphi: "The Delphi method is an iterative process to increase consensus-building and, in the end, to have consensus among experts from an examined case (Garson, 2018).

The collected case study materials are based on official publications, official reports, and other literary material in this work. The research is based on the guidance of Yin (2014), and it answers questions about where to concentrate. The case study is based on producing detailed information about the researched object (Yin, 2004). Several case studies form knowledge from the environment and are connected to the design science process that generates the artifact; as Hevner (2004) has explained, design science research methodology is based on three iteration cycles that support each other's. The research concentrates on the environment where problem formulation has been done. Understanding the environment under the research (people, organizations, technology) is essential Hevner, A., & Chatterjee, S (2010). Gathering data from the industrial environment is crucial. The critical is to identify the data and information formation from the emergency points, where SOC and detection features must react. In Industrial Control Systems such as Scada, intrusion prevention or detection tools are relevant machines we must have under the secured control of operations. We will apply a widely used design science research methodology that has traditionally been used in software and system development.

5.1 Laboratory Environments

The project team of the University of Jyväskylä and Turku University of Applied Sciences, with their platform, has constructed a testbed environment where to test equipment that both have gotten from the stakeholders. The test environment will create new standardized guidelines for the operational technology-related systems and environments. Testbed -work in the Jyväskylä testing laboratory will be parallel and develop the upper-level reference model. Based on the results of use cases, inner and outer-level specific requirements are considered. The Use-case results from testbed work in a simultaneous environment and analysis of threat assessment-based risk scenarios will generate a proposal for the governance framework. Figure 2 below illustrates the connection between the research elements in the CSG project.

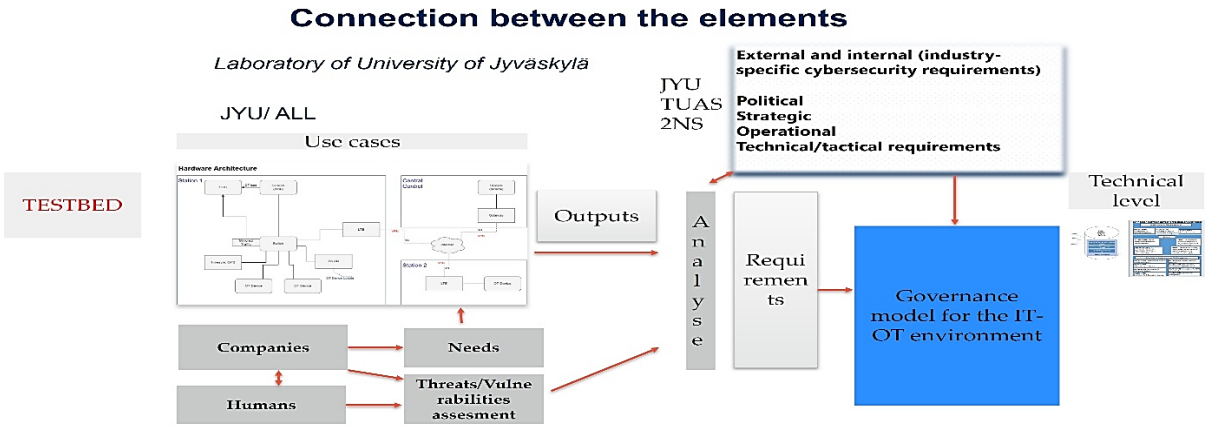

Figure 2: Testing environment

For developing Maritime Situational Awareness, Turku University of Applied Sciences has designed and built a OT test platform (Paavola, 2023), consisting of an Unmanned Surface Vessel (USV) and remote operations center (ROC), to support the industry's and authorities capacity to utilize novel technologies efficiently. The development process has allowed to gain a comprehensive understanding on every aspect of the OT operation of the USV. The built test infrastructure can be used to research the challenges and opportunities of applying AI to remote sensing problems in complex marine environments, such as ship feature recognition, vessel tracking, and abnormal behavior detection. In addition, it offers the platform to develop cybersecurity testing, security operations center (SOC), and cybersecurity situational awareness studies. The test platform consists of two components. Test Vessel e/MS Salama for unmanned operations consists of key components like the hull, motors, and batteries were procured, and sensors for situational awareness were integrated. An ICT subsystem is implemented for data processing and communication. The electrical system is installed following safety

standards. The CAN bus is connected to all relevant systems. The devices in the USV can roughly be divided into four groups, that is equipment for power and propulsion, navigation and communication, sensory and imaging, and safety, security and utility. In the Remote Operation Center (ROC) operators can monitor, support, assist, supervise, and control the USV. The remote operations center can monitor the USV or directly control the USV's systems. The key components for the remote operation of the USV are the USV multi-modal sensoring system, data communication links, and the ROC itself. The USV multi-modal sensoring system provides information about both the USV itself and its environment. The sensor data of the USV transferred to the remote operations center can also be utilized directly in a digital twin of the vessel. The Figure 3 illustrates the OT test platform.

Figure 3: The OT test platforms

Critical Infrastructure Protection in Maritime Cluster

Maritime security consists of several elements that are crucial parts of the national critical infrastructure protection. Sector-connected security is essential because if a sector-based understanding of the functionalities works at a different level, the information flows smoothly.

It has been quite problematic for organizations to be in challenging environments where each organization has used its own systems and processes to tackle physical and cyber threats. It is crucial to analyze the point where humans cause more harm than automation or artificial intelligence and what the state is that automation causes more harm than humans.

The risk assessment must be considered when protecting maritime risks. Vulnerable onboard systems may consist of cargo management systems, bridge systems, propulsion and machinery, management and control systems, access control systems, passenger servicing and management systems, public networks, administrative and crew welfare systems, and communication systems (BIMCO, 2022). Huyler (2022) states that a few vulnerable systems such as human resource management systems, systems of operators, port authority systems, SCADA systems, alarm and monitoring systems, Communication systems, navigation systems, auxiliary machinery systems, security systems, propulsion/steering, mission support systems. The environment is complicated. Despite the different kinds of systems, research indicates that humans are the weakest factors in the working environment (Endsley, 1998;1995).

5.2 Future Cybersecurity Threats in Maritime

Future cybersecurity threats in maritime are expected to increase as vessels' systems become more interconnected with IT systems. This increased connectivity to the external world makes cyber attacks on OT systems more likely and potentially more destructive in the future.

The future threat landscape may include new challenges, such as:

1. Insufficient Funding: The maritime industry has observed insufficient investment in cybersecurity, leaving systems vulnerable to attacks.
2. Effectiveness of Regulations: While regulations may help improve cybersecurity, many organizations struggle to comply with existing rules in the field of risk management and resource allocation.
3. Vulnerabilities in the Supply Chain: Securing the supply chain from cyber threats is challenging and requires comprehensive knowledge of the supply chain, contract management, and a thorough examination of suppliers' cybersecurity requirements throughout procurement, installation, and use of equipment.

4. Lack of Information Sharing: In the maritime industry, information on cybersecurity risks, threats, and incidents is not adequately shared among organizations, limiting the availability of threat intelligence for comprehensive risk assessments or preventing potential incidents.

6. Findings

The research provides transnational and EU-level cyber security assessments regarding maritime clusters. The findings determine where to direct and concentrate a focus maritime domain and why it is important to survey cyber security requirements set for member states to apply.

The big challenge is how to apply European Union-based regulations in the maritime cluster. The cluster is at a different cybersecurity level than inland stakeholders. The research indicates that crucial cybersecurity issues are connected to human activities, so it is crucial to utilize our testbed environments. The formation of Common situational awareness requires that human activities, organizational processes, and technologies are standardized at all three levels; strategic, operational, and technical. Especially in the maritime cluster, there are third-party-related matters that have to be taken into account. Multicomplex environments form challenging atmospheres where partners change, humans are not in different tasks for long periods, and temporary employees are often used.

NIS2 requires cybersecurity training to enhance the critical infrastructure's cybersecurity level. CER identifies and divides the same industry-based organizations as NIS2, which is essential for vital functions.

The operational level needs sector-based information exchange groups that use the same “language,” such as a taxonomy of what to share, how to share, with whom to share, and what information is required for reporting. Despite that organizations need to know the requirements of future cybersecurity regulations; it is crucial that the national government act efficiently and offer information on how organizations must design their information-sharing mechanisms. Cybersecurity training is crucial, but the training is irrelevant if the mental model is not clear on what business needs are. Without a common understanding of procedures and processes regarding workflow, threat prevention is not possible to take control. The working culture of the maritime cluster is very international; therefore, the standards and certifications set a coherent basement for fulfilling requirements. Active operating environments and various technologies are factors that need attention. The used testbed environments will demonstrate how important it is to analyze for example logs from the operational technology environment. Decisionmakers need to maintain situational awareness and data from the technical level must be transformed as the information and depending on the level where data or information is required, more crucial it is. Operational technology is connected to the IT environment in many ways. Vendors and partners are essential potential factors that add opportunities for supply chain issues. That is why active supply chain management is needed as part of cyber risk management. Workable supply chain management requires a stable flow of data and information. For example, the Cyber Resilience Act (CRA) sets new requirements for digitalized devices and services. CE-marked devices enhance trust and indicate to the stakeholders that Cybersecurity requirements have been taken seriously. Cybersecurity management is not a separate part of business continuity management. Both support Corporate Governance and cyber security governance. A crucial point is that cyber risk classifications have been done with other risk assessments. The cyber risk assessment is an essential part of the overall risk assessment in the maritime cluster. Cybersecurity and security plans must be part of overall risk management and continuity management activities, where policies, regulations, processes, and procedures are defined and implemented. In securing business continuity management, following the risk management guidelines of the Cybersecurity Framework developed by NIST (2024) is advisable. Framework allows to choose correct standards from the other publications. At a minimum level, a standardized environment requires that IT-related functionalities follow the ISO 2700 standard family and Operational Technology-related functionalities apply ISO 62243 standards for controlling Industrial Control Systems. Cybersecurity requirements of the European Union can be achieved by standardization. Certification systems inform stakeholders about the trust level of the company (ISO, 2018: Verve Industrial, 2022). According to the NIST (2024), in additional Special Publication SP 800-161r1 guides how to enhance Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST, 2022).

7. Discussion and Conclusions

7.1 Future Research Needs in Maritime Cybersecurity

Research in cybersecurity is vital for protecting critical infrastructure and maritime traffic itself. It helps maritime operators identify threats and manage cybersecurity risks. Given the continuous evolution and increasing automation in the maritime industry, ongoing research can improve existing best practices for managing maritime cybersecurity. A doctoral dissertation conducted at the University of Jyväskylä has revealed the vulnerability of systems used in maritime and air traffic to cyberattacks. In his research, Syed Khandker (2022) analyzed the security features of two critical surveillance systems in air and maritime traffic, ADS-B and AIS. The study successfully impacted all test devices with attacks, indicating that these attacks could potentially affect the navigation safety of aircraft or ships in real life. Major problems in both systems were related to protocol design, where all security aspects were not adequately considered. According to Khandker (2022), security could be enhanced by introducing encryption or authentication methods. This underscores the importance of research in improving maritime cybersecurity. Maritime cybersecurity is a crucial aspect of contemporary shipping and critical infrastructure protection. The identification and management of threats are key to ensuring safety and efficiency. Further research is needed to understand potential cyber threats and develop effective countermeasures. Securing global trade and the economy through cybersecurity means and preventing environmental damage caused by potential cyberattacks requires continuous research. It is also noteworthy that combating cyber threats requires international collaboration to develop cybersecurity in the maritime industry. Multiple sources indicate that much work must be done to enhance maritime cybersecurity. Essential is how to implement, for example (the ISPS) Code of Practice on port security and cyber security requirements for the ship's security and the immediate ship/port interface to enhance overall security. It must be considered that international means a wider perspective than European or Western aspects. The essential point of view is how to achieve trust in the supply chain and continuity management. Infected companies that have realized threats in the maritime industry are often seamlessly connected to other sectors linked with each other through shared systems. This kind of information-sharing relationship cycle creates more possibilities for cyber attackers.

Acknowledgments

The research was supported by Business Finland (grant number 10/31/2022) and the University of Jyväskylä.

References

Atlantic Council (2021) Appendices: Cooperation on maritime cybersecurity. https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-appendices/

BIMCO (2022) The Guidelines on Cyber Security Onboard Ships v.4 Available: https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf

Chubb N., Finn P., NG D. (2021) The Great Disconnect. The state of cyber risk management in the maritime industry. Cyberowl.

CISA (2024) Cybersecurity Governance. Available: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance

Endsley M. (1995) Towards a theory of situation awareness in Dynamic Systems. Human Factor 37(1)

Endsley M. R., (1998) "Design and evaluation for situation awareness enhancement." in Proceedings of the Human Factors Society 32nd Annual Meeting, pp. 97-101

ENISA (2023a) Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies. DOI: 10.2824/850466

ENISA (2023b) CISA and ENISA enhance their Cooperation https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation

ENISA report (2019) “Port Cybersecurity” Good Practices for Cybersecurity in the Maritime Sector Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk — ENISA (europa.eu)

European Commission. (2020a) The EU's Cybersecurity Strategy for the Digital Decade. Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018

European Commission. (2020b) Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities. COM (2020) 829 final. 2020/0365 (COD). Brussels, 16 December

European Commission (2022a). NIS2 Directive (EU) 2022/2555. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

European Commission. (2022b) Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

European Maritime Safety Agency (2022) This is EMSA. https://www.emsa.europa.eu/about.html

Garson, G. D. (2012) The Delphi method in quantitative research. Asheboro, NC: Statistical Associates Publishers. Available from: https://faculty.chass.ncsu.edu/garson/PA765/delphi.htm, retrieved 24.12.2023.

Hevner A., March, S.T., Park, J., and Ram, S. (2004) Design Science in Information Systems Research. MIS Quarterly.

Hevner, A., & Chatterjee, S. (2010) Design research in information systems: Theory and practice. Springer Science and Business.

Huyler, J. (2022) Modernizing Maritime OT cybersecurity: Unique obstacles and Opportunities. Industrial Defender. https://www.industrialdefender.com/blog/modernizing-maritime-ot-cybersecurity

IAPH (2020) Port Community Cyber Security. https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf

IAPH (2021) Cybersecurity Guidelines for Ports and Port Facilities. https://sustainablewoelports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf.

IMO (2022) Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3 5 July 2017. International Maritime Organization. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf

ISO (2018) 2700:18 Information Technology. Information Technology Security Techniques.

Khandker, S. (2022). Positioning services in different wireless networks : a development and security perspective. https://jyx.jyu.fi/handle/123456789/82425

Lété Bruno and Pernik Piret. 2017 EU–NATO Cybersecurity and Defense Cooperation:
From Common Threats to Common Solutions, Security and Defense Policy.

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

NESA (2020) Kyberturvallisuuden nykytila eri toimialoilla – Kartoituksen keskeiset havainnot

NESA (2021) Maritime Cybersecurity Report – Finnish Maritime Cybersecurity Maturity - Current state report and best practices for the Finnish Maritime sector

NIST (2022) NIST Special Publication SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

NIST (2023) Special Publication SP 800-82r3 Guide to Operational Technology (OT) Security. Available: https://doi.org/10.6028/NIST.SP.800-82r3

NIST (2024) Cybersecurity Framework 2.0. US. Department of Commerce. Available: https://www.nist.gov/cyberframework

Paavola J. (2023) Development of Applied Research Platforms for Autonomous and Remotely Operated Systems, https://urn.fi/URN:ISBN:978-952-216-862-7

Simola, J., Pöyhönen, J., & Lehto, M. (2023a). Smart Terminal System of Systems' Cyber Threat
Impact Evaluation. In A. Andreatos, & C. Douligeris (Eds.), Proceedings of the 22nd European
Conference on Cyber Warfare and Security (pp. 439-449). Academic Conferences International.
Proceedings of the European Conference on Cyber Warfare and Security, 22.
https://doi.org/10.34190/eccws.22.1.1070

Simola, J., Pöyhönen, J., & Martti, L. (2023b). Cyber Threat Analysis in Smart Terminal Systems. In
R. L. Wilson, & B. Curran (Eds.), ICCWS 2023 : Proceedings of the 18th International Conference
on Cyber Warfare and Security (pp. 369-378). Academic Conferences International Ltd.
https://doi.org/10.34190/iccws.18.1.93

Tuomala, V. (2023). Maritime Cybersecurity. Before the risks turn into attacks. Xamk Research https://www.theseus.fi/bitstream/handle/10024/504156/URNISBN9789523443600.pdf?sequence=2&isAllowed=y

U.S: Coast Guard. (2020). Inter-American Committee on Ports. International Port Security Program. Stakeholders management - Port security committees.

Verve Industrial (2022) What is IEC 62443?. https://verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/

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