Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment

Allan Nganga
Department of Maritime Studies
Western Norway University of Applied Sciences
Haugesund, Norway
e-mail: allan.kevin.nganga@hvl.no

Joel Scanlan
Department of Maritime Studies
Western Norway University of Applied Sciences
Haugesund, Norway
e-mail: josc@hvl.no

Margareta Lützhöft
Department of Maritime Studies
Western Norway University of Applied Sciences
Haugesund, Norway
e-mail: mhl@hvl.no

Steven Mallam
Department of Maritime Operations
University of South-Eastern Norway
Borre, Norway
email: Steven.Mallam@usn.no

***Abstract*— In response to the growing maritime cyber threat landscape, the International Maritime Organization (IMO) developed guidelines on maritime cyber risk management, part of resolution MSC.428 (98). One of the guidelines' functional requirements calls for the development and implementation of activities necessary for the timely detection of a cyber event. This has seen the development of Maritime Security Operation Centers (M-SOCs), which give maritime operators and service providers better cyber visibility of vessel systems. In line with the conference theme on situational awareness, the position paper will explore this from the perspective of cyber threat information sharing and its necessity when it comes to enhancing awareness in multi-stakeholder domains. We propose a model that could form as a basis for future maritime cyber threat sharing from an M-SOC analyst's point of view. Gaps that could undermine the effectiveness of this structure are subsequently underscored and form the basis of future research to be conducted in this area.**

Keywords-maritime cybersecurity; situational awareness; information sharing; stakeholders; security operations center.

I. INTRODUCTION

The maritime sector is a complex ecosystem, bringing together stakeholders and organizations of varied sizes, maturity, complexity, and operational scope. With its increasing rate of digitization, and increased levels of connectivity in the near future, the threat environment is steadily becoming more hostile. Cyber-attacks are becoming more frequent with all actors in the digital value chain being targeted by criminal networks and hostile networks [1][2]. Against this backdrop, the IMO, in 2017 adopted resolution MSC.428(98)-maritime cyber risk management in safety management systems and MSC-Fal.1-guidelines on maritime cyber risk management. Recognizing the multi-stakeholder nature of the domain, the resolution called for administrators, classification societies, ship owners, operators, agents, equipment manufacturers, service providers, ports, port facilities and other stakeholders to work towards protecting shipping from current and emerging cyber threats [3] [4]. These regulations highlight that cyber security in the maritime domain is indeed a shared responsibility.

A benefit of stakeholder identification is that it helps in the clear defining of cyber threat information sharing structures and their participating entities [5]. One way of gaining increased cyber situational awareness necessary for the timely resolution of cyber threats is to exchange information with others [6]. It is within this context that we propose cyber threat information sharing as a discussion that needs to be had within the maritime domain.

As a build-up towards this, the position paper will take on the following structure: Section II gives a background on information sharing; Section III looks at legislation and guidelines that have steered information sharing in other multi-stakeholder domains; Section IV discusses information sharing initiatives within the maritime domain; Section V looks into M-SOCs; Section VI discusses the proposed model and the motivation behind its development; Section VII highlights key takeaways from the proposed work with identified implementation challenges framed as directions for future work; Section VIII concludes the paper.

II. INFORMATION SHARING

Information sharing has previously been defined as the act of voluntarily making information possessed by one entity available to another [7]. Within the context of this paper, the type of information we are most interested in is cyber threat information defined as any information that can help an organization recognize, assess, monitor, and respond to cyber threats. Examples of this include indicators of compromise, which are technical artifacts or observables that suggest an attack is imminent or is currently underway; tactics, techniques, and procedures used by threat actors; security alerts; threat intelligence reports; situational awareness data; best practices; and strategic analysis. Vessel mobility makes situational context information particularly important. Information sharing as used within this paper is the exchange of cyber threat information with trusted entities/stakeholders [8]–[10].

The choice of an information sharing model or structure can influence the effectiveness of information sharing between various stakeholders. Subsequently, various information sharing models have been proposed [5] [11].

One notable and highly adopted structure was established by the MITRE Corporation during the development of The Trusted Automated eXchange of Indicator Information (TAXII) [12]. TAXII defines a set of services, messages and protocols that aid in timely and efficient exchange of cyber threat information. As part of the work, three main information sharing models were defined namely hub and spoke, peer-to-peer and source-subscriber. Figure 1 below is reproduced from the work done by [12] and highlights these models.

In a hub and spoke model, a spoke shares information with the hub, which then re-shares this information with all other spokes. A peer-to-peer model is structured in such a way that any number of organizations can function as both producers and consumers of information. A source/subscriber model is one where an organization acts as a sole source of information for all subscribers. Respondents in a 2021 survey by [13] revealed that 58% of their threat intelligence came from peers.

III. MULTI-SECTOR INFORMATION SHARING INITIATIVES

The pivotal role played by information sharing when it comes to enhancing cyber resilience cannot be understated as is evidenced by multiple cross-sector initiatives related to this [14]–[16]. From a regulatory perspective, the United States of America (USA) passed the Cybersecurity Information Sharing Act (2015). This calls for concerned parties to develop procedures for sharing cyber threat information between different stakeholders. The European Union (EU) Network and Information Security (NIS) Directive calls for information exchange and cooperation among operators of essential services within sectors identified as critical. These include energy, transport, banking financial market infrastructures, health, drinking water supply and digital infrastructure.

Aviation regulation, such as European Civil Aviation Conference (ECAC) Doc 30-Part II [16] maps out information sharing relationships from the perspectives of various stakeholders, such as the nation-state, aircraft operators and software/system developers.

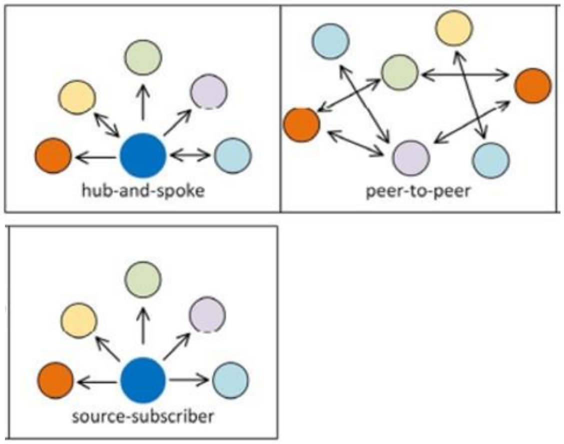

Figure 1: TAXII Information Sharing Model

The Forum of Incident Response and Security Teams (FIRST) recently released an updated version of the Traffic Light Protocol (TLP) that facilitates information sharing based on color categories. Information in the TLP: RED category can only be shared with individual recipients with no additional disclosure permitted. TLP: AMBER category authorizes limited information disclosure on a need-to-know basis within organizations and their clients. TLP: AMBER+STRICT restricts sharing to within the organization only. TLP: GREEN category enables limited disclosure within the recipient's community while TLP: WHITE has no limitation on sharing [17].

Of the sector-specific information sharing initiatives, one that has had considerable effort put in involves the development of Information Sharing and Analysis Centers (ISACs) and Information Exchanges [18][19]. Within their specific domains, these are intended to be trusted entities that promote information sharing and good practices related to cyber and physical threats and their mitigation. The United Kingdom (UK) Center for the Protection of National Infrastructure (CPNI) mapped out information exchanges for various sectors including transport, finance, water security, pharmaceuticals, and aerospace among others [20]. In compliance with the US Presidential Decision Directive-63 [21], the National Council of ISACS was established with various sector-specific ISACS, such as Automotive, communications, elections infrastructure, electricity, and financial services [22]. Likewise, the EU sees ISACs as a way of building a European cybershield [19].

IV. MARITIME INFORMATION SHARING INITIATIVES

Information sharing initiatives within the maritime domain have taken root in the form of legislation, regulatory guidelines, public and private sector collaborations, and funded research projects. These are subsequently highlighted:

A. *Legislation*

Within the EU, the maritime domain, an identified critical infrastructure sector, is required to adhere to the EU NIS directive [15], which calls for information exchange and cooperation among operators of essential services. Specifically related to the maritime domain, this directive requires incident reporting requirements to be met by identified stakeholders, such as companies, ships, port facilities, ports, and vessel traffic services. Additionally, the directive calls for a coherent approach in the satisfaction of reporting requirements by considering international codes and guidelines prepared by entities, such as the IMO.

B. *ISACS*

In compliance with the US Presidential Decision Directive-63 [21], which required the creation of sector-specific ISACS, the maritime domain has two established ISACs namely Maritime ISAC [23], and Maritime

Transportation System (MTS) ISAC [24]. The ever increasing cybersecurity concerns along the lower Columbia river prompted the Port of Vancouver (USA) and MTS-ISAC to launch the Lower Columbia River Maritime Information Exchange (LCR-MIX) to facilitate ease of communication, collaboration and cyber situational awareness among stakeholders [25]. Information sharing partnerships have been actualized by private sector entities, such as the Norwegian Maritime Cyber Resilience Center (NORMA Cyber) and MTS-ISAC who recently signed an agreement that will see both entities exchange maritime cyber threat intelligence information [26].

C. EU ECHO Project (2019)

As part of the EU funded ECHO project [27], the study by [28] adapted the user communities established by the Common Information Sharing Environment (CISE) [29]. It highlighted them as shareholders of sensitive cyber information sharing within the maritime domain. These user communities and their systems are Maritime safety and security; Fisheries control; Marine pollution preparedness and response in Marine environment; Customs; Border control; General law enforcement; and Defense.

D. Danish Maritime Cybersecurity Unit (2019)

The Danish Maritime Cybersecurity Unit developed the cyber and information security strategy [30] in which the Danish Maritime Authority (DMA) will serve as an exchange point between the Center for Cyber Security (CFCS) and various maritime sector stakeholders. The primary responsibilities of the DMA in this information sharing arrangement will be to communicate, procure, create, and validate IT security-related information between the parties, coordination tasks, organizing professional workshops and conferences related to specific IT security issues in the maritime sector.

The strategy [30] also recommends establishing the Maritime Cyber and Information Security Forum, which is coordinated by the DMA, and includes IT security representatives from Danish authorities who are directly involved in maritime activities. The forum is structured to serve as a platform for discussing how various security incidents have been managed by the parties involved and their experiences in managing the various situations. Long term goals of the forum will include identifying and addressing the possibilities of developing a digital hub where information security knowledge is made easily accessible and searchable by, maritime sector authorities and stakeholders.

E. International Association of Classification Societies-IACS (2022)

Recommendation 166 [31], UR E26 [32] and E27 [33] (cyber resilience of systems, for product suppliers) clearly define key vessel cybersecurity stakeholders and their responsibilities. The key stakeholders represented are the shipowner/company, ship designer/shipyard, system integrator, supplier, and classification society. One of the strengths of these regulations is that E26 and E27 become mandatory for new vessels commissioned after 1st January 2024 while remaining non-mandatory guidance tools for existing vessels. Additionally, the 2020 world merchant fleet statistics by Equasis [34] showed that 78% of vessels of a gross tonnage of more than 500 tonnes are classified under the IACS umbrella. An interpretation of the regulations yields TABLE 1, which highlights stakeholder communication instances identified in the IACS regulations.

In certain instances, there was no identified communication between certain stakeholders. For example, there is no direct communication between the ship and classification society. The ship owner has traditionally been responsible for ensuring the vessel complies with regulations and so it is assumed that the authors of this regulation factored that in and created communication between the classification society and ship owner instead.

While these regulations are designed for regulatory compliance, the communication pathways that they mandate between the various stakeholders can be exploited to establish dependable vessel threat information sharing structures.

V. M-SOCs

Entities in the maritime cyber resilience ecosystem that would benefit from increased information sharing are Security Operation Centers (SOCs). A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, and report on cybersecurity incidents. An internal SOC functions as part of the organization it is defending while an external one is contracted as a service provider [35]. An M-SOC is SOC that operates within the maritime domain. There has been a steady increase in the number of maritime operators who have either setup or contracted third party M-SOCs to enable them to have better visibility and cyber awareness of their vessels.

TABLE 1:IACS STAKEHOLDER COMMUNICATION

	Classification Society	Ship Owner	Ship	System Integrator	Shipyard	Supplier
Classification Society	▨					
Ship Owner	X	▨				
Ship		X	▨			
System Integrator	X	X	X	▨		
Shipyard	X	X	X	X	▨	
Supplier	X	X	X	X	X	▨

Examples of these include Norma Cyber [36], Marlink [37], Port-IT [38], Cyber-Owl [39], Port of LA [40], and Port of Singapore [41] among others.

These real-time monitoring units play a vital role in not only producing cyber threat information but also consuming the same when it comes from entities, such as equipment vendors and suppliers. It is, therefore, pivotal for M-SOC analysts to have complete domain awareness of the vessel cybersecurity ecosystem and information sharing complexities that exist between all the stakeholders within this ecosystem so that they can tailor their communication appropriately.

VI. PROPOSED VESSEL THREAT INFORMATION SHARING MODEL

Work on the proposed model was inspired by a similar outcome in the aviation domain and highlighted in the ECAC Doc 30-Part II regulation, which is currently active and enforceable [16]. In the case of this regulation, the authors developed three information sharing models from the perspectives of three critical stakeholders namely, nation state, operator, and software/system developer. Figure 2 shows the outcome of the process from the software/system developer perspective. The recommended actions of the software/system developer with regards to information sharing were then highlighted, which included identifying external stakeholders, information they would want to receive, communication channels to be used, vulnerability response/disclosure process, and finally assessing all the above with the identified stakeholders and regulators. Additionally, Figure 3 shows the outcomes of a similar process but from the perspective of the operator.

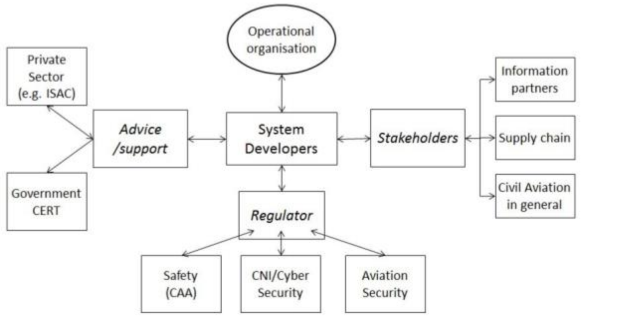

Figure 2: Aviation Information Sharing-Software/System Developer Perspective

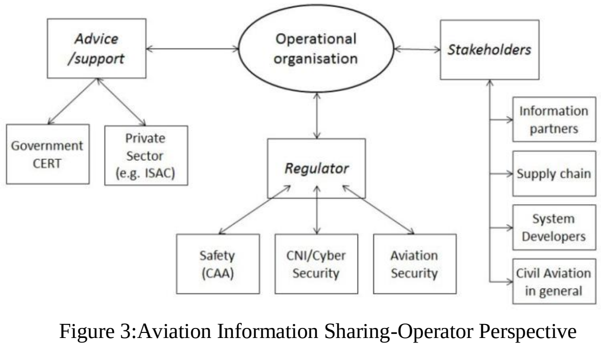

Figure 3:Aviation Information Sharing-Operator Perspective

Development of the proposed vessel threat information sharing model, shown in Figure 4, began by identifying the key stakeholders highlighted in the three IACS documents that focus on vessel cyber resilience, Recommendation 166 [31], UR E26 [32] and E27 [33] (cyber resilience of systems, for product suppliers). These were identified to be the classification society, shipowner, supplier, ship designer/shipyards and system integrator. The ship is the primary asset of focus and so has also been included. The next step involved establishing any instances of communication that are highlighted in each of the documents. As shown in TABLE 1, there are instances of communication between all stakeholders. Examples of statements in the regulations that guided this process include:

- E26: The Supplier shall design and document testing procedures suitable to verify the performance of measures adopted to fulfil relevant requirements (Test Plan)
- E26: The Shipyard or System Integrator shall incorporate the documentation provided by the Supplier into an overall Test Plan for the CBSs
- E26: The final Test Plans updated according to the actual CBSs configuration and implementation onboard shall be made available to the Classification Society.
- E26: The Shipowner shall retain onboard a copy of results of execution of tests and an updated Test Plan and make them available to the Classification Society.

The examples above, while only representing a small portion of the regulations, already highlight how the development and maintenance of a test plan involves all stakeholders. The directional arrows in the model are a direct interpretation of the stakeholder communication responsibilities. Because the model has not been evaluated, we opted to leave them as is to act as a guide. Testing of the model will determine the actual cyber threat information sharing responsibilities between stakeholders, which may lead to a variation in the direction of communication.

The increased adoption of M-SOCs as highlighted in Section V means that that they will be a key source of real-time vessel threat information. Interviews we have conducted with a few M-SOC vendors, part of on-going work to be published in future, reveals that most are currently operating as a service provided to ship operators to help them increase asset visibility from a cyber security perspective. The service level agreement between them would therefore mean that any cyber threat information that the M-SOC gathers from the vessel would be shared with both the operators and the vessel. We therefore position them in the model between the operator and the vessel. The M-SOC is highlighted in a different shade because they are not one of the key stakeholders identified in the IACS guidelines used above. However, from a threat information perspective, they are a primary stakeholder. Additionally, the green dotted outline encompassing the M-SOC, ship owner and ship shows the current limited scope of information sharing due to the limiting nature of service agreements.

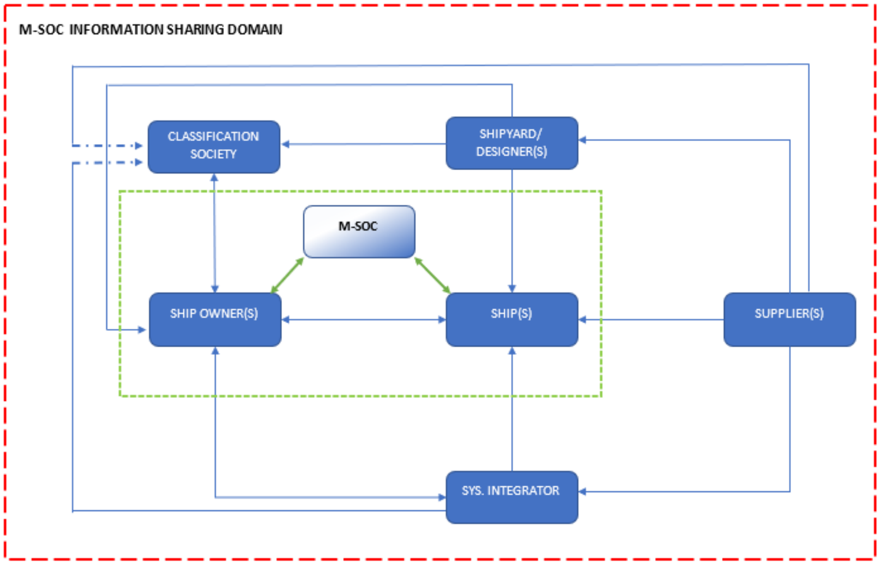

Figure 4: Proposed Vessel Threat Information Sharing Model

It is important to highlight the assumptions made when developing this model. The first assumption is that all the vessel resilience stakeholders identified in the guidelines are also key when it comes to sharing of threat information. It is possible that some stakeholders may have been left out of the model or some have been included who are not critical in the process. As an example, we added M-SOCs in the model because they are a key producer of real-time vessel cyber threat information. Closely related to this is also the fact that stakeholder cyber resilience responsibilities vary during the lifecycle of a vessel from design, commissioning, construction, and operation [32]. However, as the model is yet to be tested, the assumption made is that there is uniform responsibility, something that we anticipate will change once validation of the model begins.

The second assumption made is that pre-existing mandated communication between stakeholders, albeit currently for regulatory compliance, would make it easier to establish threat information communication pathways. It is assumed that it is easier to build upon a pre-existing relationship rather than proposing an entirely new one where none existed before. It is for this reason that the connections between stakeholders are made this way. However, we acknowledge that this could change once testing the viability of the model begins.

While the guidelines identify the stakeholders as distinct separate entities, it is assumed that the same happens in actual operation where it may not always be the case. There are examples of shipyards also providing system integration services to their clients, which would therefore lead to a merging of those two entities in the model presented [42]. However, we have opted to maintain all stakeholders as distinct separate entities as highlighted in the guidelines.

VII. KEY TAKEAWAYS AND FUTURE RESEARCH DIRECTIONS

The key contribution of this position paper is the proposal of a maritime vessel cyber threat information sharing model. This model differs from previous maritime information sharing initiatives highlighted in Section IV in that this is more specific to vessel cyber resilience and focuses on the stakeholders considered critical to the secure posture of the same. Its development was motivated by similar work done in the aviation domain as highlighted in Figure 2 and Figure 3 contained in the presently active ECAC Doc 30-Part II regulation [16].

Having the information sharing model allows us to be more targeted in what we want to uncover with regards to the state of maritime information sharing because we now have well defined stakeholders to start with and hypothesized relationships which testing will help us refine. Additionally, we also aim to explore the following implementation challenges that we feel would impede the successful adoption of such a model:

A. *Identifying Information Sharing Stakeholder gaps*

While the stakeholders involved in vessel cyber resilience have been identified, research on their roles with respect to threat information sharing is still a significantly under researched area with the potential of revealing glaring gaps that could undermine the information sharing process. For example, a 2021 study [43] conducted by the US transport department identified gaps in vulnerability and exploit information sharing between various transportation stakeholder groups, such as:

- Indirect communication between equipment manufacturers and Infrastructure Owner Operators (IOOs), which occurs mostly through contractors, distributors, and intermediate agents

- Equipment manufacturers lacking procedures to manage unsolicited reports from security researchers; manufacturers reporting of the long time taken to disseminate patches to all devices
- IOOs believing vulnerabilities are a problem that equipment manufacturers should take ownership of and address in case any problem arises.

In order to overcome this challenge and optimize cyber information sharing within the maritime sector, future research will focus on understanding communication gaps, and variations in information sharing perceptions between the stakeholders presented in the model. This will also help determine the validity of one of the assumptions made during development of the model whereby it is easier to build threat information pathways on top of pre-existing stakeholder communication.

B. Stakeholder Specific Actionable Cyber Threat Information Needs

Actionable cyber threat information has previously been defined by multiple researchers as constituting multiple dimensions. Research by [44] established that actionable information is determined by correctness, relevance, timeliness, usefulness, and uniqueness. [45] defined actionable threat intelligence based on timeliness, prioritization, implementation, resolution, relevance, integration, automation, trustworthiness, and context. The European Union Agency for Cybersecurity (ENISA) [46] highlighted that actionable information has to be Relevant, Ingestible, Accurate, Complete, and Timely within the context of the particular recipient organization or stakeholder. An acknowledged consequence of the highlighted dimensions is that different stakeholders will have varying perspectives on what constitutes actionable threat information. Indeed, this is reflected in surveys conducted by [13] who established that less than 50% of respondents considered the intelligence they received as being accurate and actionable with timeliness being the worst rated by only 29% of respondents. In the same study, only 33% of respondents acknowledged having effective processes for handling actionable threat intelligence from external sources. Actionability of threat intelligence was also ranked, at 61%, as the most essential element during calculation of risk scores.

Overcoming this challenge will require further research into how the various stakeholders define what constitutes actionable cyber threat information and exploring how the same fosters their participation in the information sharing ecosystem. It also ensures that everyone contributes in the information sharing process to reduce the problem of free-riding [5][44].

VIII. CONCLUSION

This position paper began by introducing information sharing and its role in enhancing cyber resilience in multi-stakeholder domains. Specific to the maritime domain, various information sharing initiatives were highlighted through articles of legislation, funded projects, and regulatory authority guidelines. The IACS regulations [31]–[33] are the closest that the maritime sector has in terms of a communication structure between the various vessel cyber resilience stakeholders. However, these were tailored towards compliance with regulatory requirements rather than to be used as cyber threat information sharing structures.

Nevertheless, the increasing adoption of SOCs in the multi-stakeholder maritime domain necessitates the need to have efficient cyber threat information sharing structures, which are critical to vessel safety, security, and timely resolution of cyber incidents. We believe that the communication pathways proposed by the new IACS regulations, enforceable for newly contracted vessels as from January 1st, 2024, provide an excellent starting point as a stable structure. Further research therefore needs to be done to ascertain their usability and applicability for cyber threat information sharing within the vessel cyber resilience domain.

REFERENCES

[1] P. H. Meland, K. Bernsmed, E. Wille, J. Rødseth, and D. A. Nesheim, “A retrospective analysis of maritime cyber security incidents,” *TransNav*, vol. 15, no. 3, pp. 519–530, 2021.

[2] J. D. Scanlan, J. M. Styles, D. Lyneham, and M. H. Lutzhoft, “New Internet Satellite Constellations to Increase Cyber Risk in Ill-Prepared Industries,” in *70th International Astronautical Congress (IAC)*, 2019, pp. 1–12.

[3] IMO, “Guidelines on Maritime Cyber Risk Management.” IMO, pp. 1–6, 2021.

[4] IMO, “Maritime Cyber Risk Management in Safety Management Systems.” IMO, p. 1, 2017.

[5] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions,” *Comput. Secur.*, vol. 87, pp. 1–13, Nov. 2019.

[6] U. Franke and J. Brynielsson, “Cyber situational awareness – A systematic review of the literature,” *Comput. Secur.*, vol. 46, pp. 18–31, Oct. 2014.

[7] A. Y. Akbulut and J. Motwani, “Integration and Information Sharing in E-Government,” in *Encyclopaedia of Networked and Virtual Organizations*, IGI Global, 2008, pp. 729–734.

[8] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, “Guide to Cyber Threat Information Sharing.” National Institute of Standards and Technology, Gaithersburg, MD, p. 43, 04-Oct-2016.

[9] A. Albakri, E. Boiten, and R. De Lemos, “Risks of sharing cyber incident information,” *ACM Int. Conf. Proceeding Ser.*, vol. 10, pp. 1–10, Aug. 2018.

[10] ENISA, “Incentives and Challenges for Information Sharing in the Context of Network and Information Security.” ENISA, p. 56, 2010.

[11] L. O. Nweke and S. Wolthusen, “Legal Issues Related to Cyber Threat Information Sharing among Private Entities for Critical Infrastructure Protection,” *Int. Conf. Cyber Conflict, CYCON*, vol. 2020-May, pp. 63–78, May 2020.

[12] J. Connolly, M. Davidson, and C. Schmidt, “The Trusted Automated eXchange of Indicator Information (TAXII^{TM}).” Mitre Corporation, p. 10, 2014.

[13] Ponemon, “Fourth Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way.” Ponemon, p. 63, 2021.

[14] DOJ and DHS, *Cybersecurity Information Sharing Act of 2015 Procedures and Guidance | CISA*. 2015.

[15] EU, *Directive (EU) 2016/1148*. 2016, p. 30.

[16] ECAC, *ECAC Doc 30, Part II-Cyber Threats to Civil Aviation*. 2018, p. 71.

[17] FIRST, “Traffic Light Protocol (TLP) Version 2.0,” 2021. [Online]. Available: https://www.first.org/tlp/. [Accessed: 23-Oct-2022].

[18] ENISA, “Information Sharing and Analysis Centers (ISACS)-Cooperative Models.” ENISA, p. 51, 2017.

[19] ENISA, “Cross-Sector Exercise Requirements.” ENISA, p. 40, 2022.

[20] A. Powell, “Information Sharing in the UK,” 2010.

[21] National Telecommunications and Information Administration, *Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators*. US, 1998.

[22] NCI, “National Council of ISACs,” 2022. [Online]. Available: https://www.nationalisacs.org/. [Accessed: 23-Oct-2022].

[23] MSC, “Maritime Security Council,” 2020. [Online]. Available: https://www.maritimesecurity.org/. [Accessed: 23-Oct-2022].

[24] MTS-ISAC, “Maritime Transportation System ISAC,” 2022. [Online]. Available: https://www.mtsisac.org/. [Accessed: 23-Oct-2022].

[25] MTS-ISAC, “Port of Vancouver (LCR-MIX),” 2022. [Online]. Available: https://www.mtsisac.org/post/port-of-vancouver-usa-launches-cyber-security-information-sharing-group-for-lower-columbia-river. [Accessed: 23-Oct-2022].

[26] NORMA_Cyber, “MTS-ISAC and NORMA Cyber,” 2022. [Online]. Available: https://www.normacyber.no/news/the-mts-isac-and-norma-cyber-strengthen-information-sharing-ties. [Accessed: 23-Oct-2022].

[27] echonetwork, “ECHO,” 2022. [Online]. Available: https://echonetwork.eu/. [Accessed: 23-Oct-2022].

[28] J. Rajamäki, I. Tikanmäki, and J. Räsänen, “CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain,” *Inf. Secur. An Int. J.*, vol. 43, no. 2, pp. 215–235, 2019.

[29] EMSA, “Common Information Sharing Environment (CISE) - EMSA - European Maritime Safety Agency,” 2009. [Online]. Available: https://emsa.europa.eu/cise.html. [Accessed: 23-Oct-2022].

[30] Danish_Maritime_Cybersecurity_Unit, “Cyber and Information Security Strategy for the Maritime Sector.” Danish Maritime Authority, p. 13, 2019.

[31] IACS, “Rec 166-Recommendation on Cyber Resilience.” IACS, p. 57, 2022.

[32] IACS, “UR E26-Cyber Resilience of Ships.” IACS, p. 32, 2022.

[33] IACS, “UR E27 Cyber Resilience of On-board Systems and Equipment.” IACS, p. 14, 2022.

[34] Equasis, “The 2020 World Merchant Fleet.” Equasis, p. 105, 2020.

[35] C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*, vol. 1. MITRE, 2014.

[36] NORMA-Cyber, “Norma Cyber,” 2022. [Online]. Available: https://www.normacyber.no/en/home. [Accessed: 23-Oct-2022].

[37] Marlink, “Maritime cyber security solutions and services,” 2022. [Online]. Available: https://marlink.com/solutions/cyber-security/. [Accessed: 23-Oct-2022].

[38] Port-IT, “Port-IT,” 2022. [Online]. Available: https://www.port-it.nl/about/history/. [Accessed: 23-Oct-2022].

[39] CyberOwl, “Cyber Owl - Cybersecurity analytics for operational assets,” 2022. [Online]. Available: https://cyberowl.io/. [Accessed: 23-Oct-2022].

[40] Port_of_LA, “Port of Los Angeles Launches First-of-its-Kind Cyber Resilience Center,” 2022. [Online]. Available: https://www.portoflosangeles.org/references/2022-news-releases/news_012422_csc_ibm. [Accessed: 23-Oct-2022].

[41] maritime_gateway, “Singapore opens cyber security operations centre,” 2019. [Online]. Available: https://www.maritimegateway.com/singapore-opens-cyber-security-operations-centre/. [Accessed: 22-Sep-2022].

[42] Vard, “VARD,” Jan-2022. [Online]. Available: https://www.vard.com/. [Accessed: 24-Oct-2022].

[43] M. C. Ramon, A. T. Dodson, S. R. Institute, and I. Cambridge Systematics, “Transportation Cybersecurity Incident Response and Management Framework: Final Report.” United States. Department of Transportation. Federal Highway Administration, p. 196, 01-Jul-2021.

[44] O. Al-Ibrahim, A. Mohaisen, C. Kamhoua, K. Kwiat, and L. Njilla, “Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence,” Feb. 2017.

[45] Ponemon, “Third Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way.” Ponemon, p. 47, 2017.

[46] ENISA, “Actionable information for security incident response — ENISA.” ENISA, p. 79, 2014.