Western Norway University of Applied Sciences

University of South-Eastern Norway

IARIA

Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment

Allan Nganga[1]*, Joel Scanlan[1], Margareta Lützhöft[1], Steven Mallam[2]

[1]Department of Maritime Studies

[1]Western Norway University of Applied Sciences

[1]Haugesund, Norway

[1]Presenter email: aknga@hvl.no*

[2]Department of Maritime Operations

[2]University of South-Eastern Norway

[2]Borre, Norway

Allan Nganga

- Allan Nganga is a Maritime Cyber Security PhD fellow at the Western Norway University of Applied Sciences
- He is part of MarSafe, a cross disciplinary research group within the department of maritime studies focusing on human-centered, system-oriented research in the maritime domain
- His research interests are in human-centered cyber security, cyber risk assessment and cyber situational awareness

Aims and Contributions of the paper

The aims of this position paper were to:

- ✓Explore the state of cyber threat information sharing within the maritime domain with a focus on maritime vessel cyber resilience

Identified gaps in maritime vessel cyber threat information sharing led to the following contributions:

1. The development of a proposed information sharing model between maritime vessel cyber-resilience stakeholders
2. Identification of future themes of research to help in validating the proposed model

What is Information Sharing?[1]

- **Information Sharing**-The exchange of cyber threat information with trusted entities/stakeholders
- **Cyber Threat Information (CTI)**-any information that can help an organization recognize, assess, monitor, and respond to cyber threats.
- **CTI Examples**-Indicators of compromise; tactics, techniques, and procedures used by threat actors; security alerts; threat intelligence reports; situational awareness data; best practices; and strategic analysis.

Information Sharing in Non-Maritime Domains (Legislation)

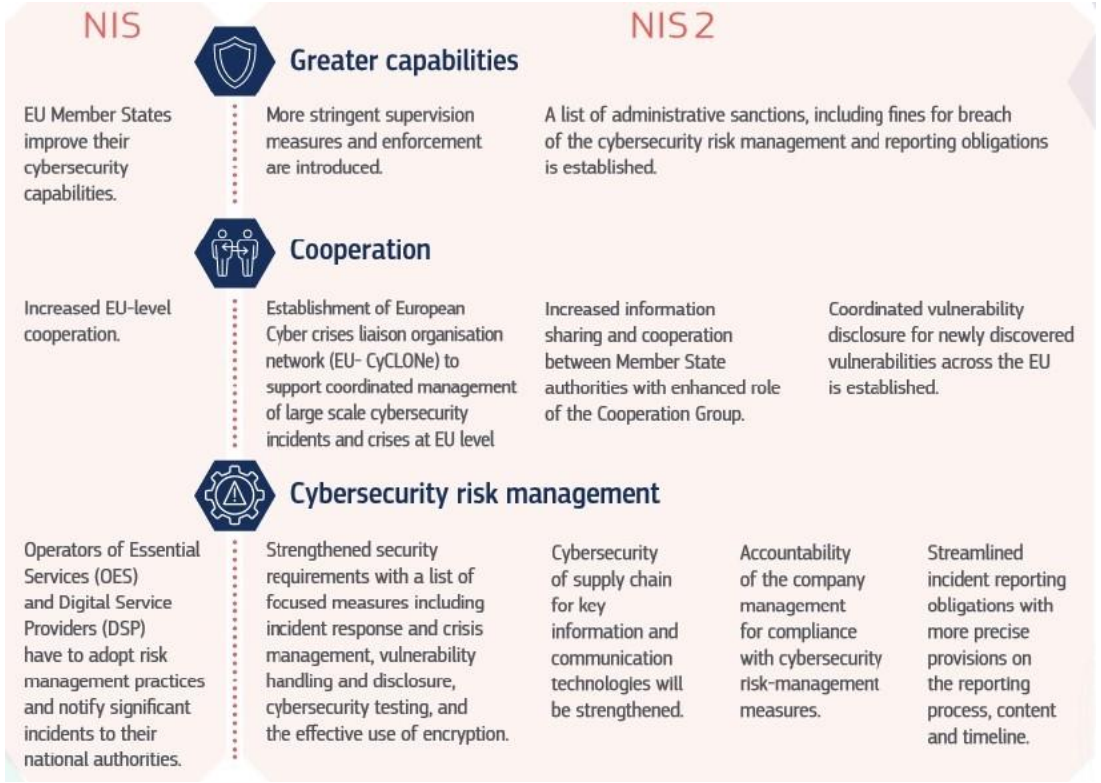
1. **USA-Cybersecurity Information Sharing Act** (**2015**)[2]-Calls for concerned parties to develop procedures for sharing cyber threat information between different stakeholders.
2. **European Union (EU) Network and Information Security (NIS) Directive (EU 2016/1148)**[3] **-**Calls for information exchange and cooperation among operators of essential services in critical sectors such as critical energy, transport, banking.
3. **European Civil Aviation Conference (ECAC) Doc 30-Part II**[4]**-** Maps out information sharing relationships from the perspectives of stakeholders, such as the nation-state, aircraft operators and software/system developers

Information Sharing in the Maritime Domain (Legislation)

1. **European Union (EU) Network and Information Security (NIS) Directive (EU 2016/1148)-**Requires incident reporting requirements to be met by identified maritime domain stakeholders, such as companies, ships, port facilities, ports, and vessel traffic services. Currently under revision to NIS2

2. **US Presidential Decision Directive 63**[5]-Required the creation of sector-specific Information Sharing and Analysis Centers (ISACS). This subsequently led to the formation of the Maritime ISAC and Maritime Transportation System (MTS) ISAC

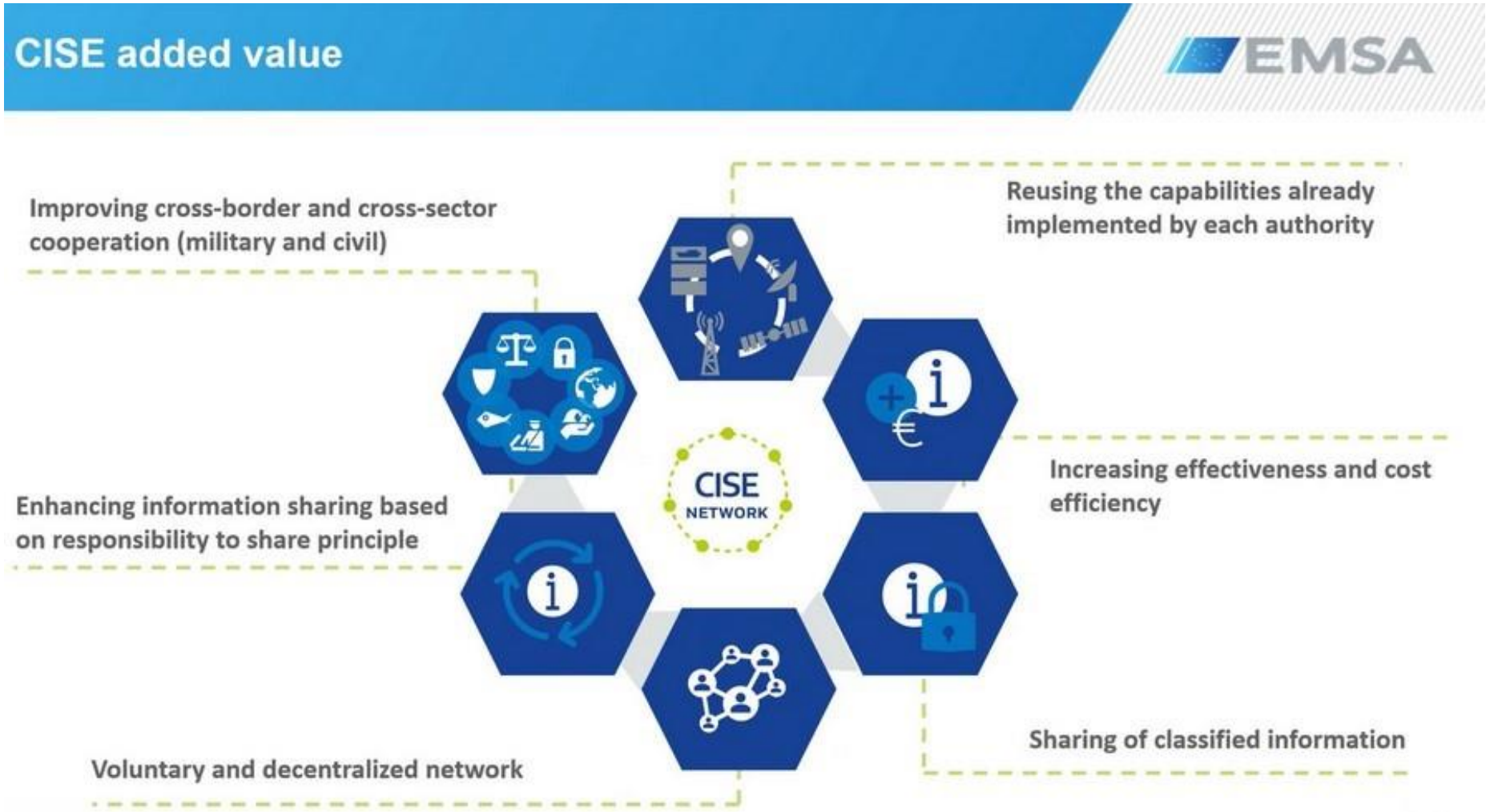
NIS Directive (EU 2016/1148)



Information Sharing in the Maritime Domain (Initiatives)

1. **Port of Vancouver (USA) and MTS-ISAC**[6] launched the Lower Columbia River Maritime Information Exchange (LCR-MIX) to facilitate ease of communication, collaboration and cyber situational awareness among stakeholders
2. **Norwegian Maritime Cyber Resilience Center (NORMA Cyber) and MTS-ISAC**[7] signed an agreement that will see both entities exchange maritime cyber threat intelligence information
3. **EU funded ECHO project**[8] adapted the user communities established by the Common Information Sharing Environment (CISE) initiative and highlighted them as shareholders of sensitive cyber information sharing within the maritime domain.
4. **Danish Cyber and Information Security Strategy**[9] recommends establishing the Maritime Cyber and Information Security Forum, which is structured to serve as a platform for discussing how various security incidents have been managed by the parties involved and their experiences in handling the various situations.

EU Common Information Sharing Environment (CISE)[10]



Identified Information Sharing Gaps in Maritime Domain

- ✓No formal framework or structure to facilitate information sharing between stakeholders critical to maritime vessel cyber resilience
- ✓If such a framework was to be developed, who would be the main stakeholders in the information sharing value chain?
- ✓What existing legislation or regulatory guidance can facilitate the development of such a structure?

Development of the Information Sharing Model (M-SOCs)

- **Security Operations Center (SOC)**[11]-Team primarily composed of security analysts organized to detect, analyze, respond to, and report on cybersecurity incidents.
- **M-SOC**-A SOC that operates within the maritime domain. Marked increase in the number of M-SOCs being adopted in the maritime domain e.g., Norma Cyber, CMA-CGM, Marlink, Port of LA, Maersk, Cyber Owl

Why are M-SOCs a critical element of an information sharing model?

- ✓They have real-time visibility into vessel IT/OT systems to detect cyber anomalies
- ✓Key producer of vessel cyber threat information

M-SOCs Adoption in the Maritime Domain

THE PORT OF LOS ANGELES

NORMA CYBER

MPA SINGAPORE

CMA CGM

CYBER OWL

MARLINK

PORT-IT

CYDOME

MAERSK

ABB

Development of the Information Sharing Model (Stakeholders)

We used the latest guidelines from the International Association of Classification Societies (IACS) to identify key stakeholders

1. **April 2020**-IACS Rec. 166 (Recommendation on Cyber Resilience)[12]
2. **April 2022**-IACS Unified Requirements E26 (cyber resilience of ships) & E27 (cyber resilience of on-board systems and equipment)[13][14]
   - E26 & E27 are mandatory for contracts signed after 1st January 2024

These guidelines were chosen because they clearly define who the vessel cyber resilience stakeholders are. These include classification societies, ship owner, shipyard/designer, system integrator and supplier

Focus on the Vessel Cyber Resilience Stakeholders

Interpretation of the three guidelines reveals instances of communication between the main stakeholders.

Examples of such communication are highlighted below:

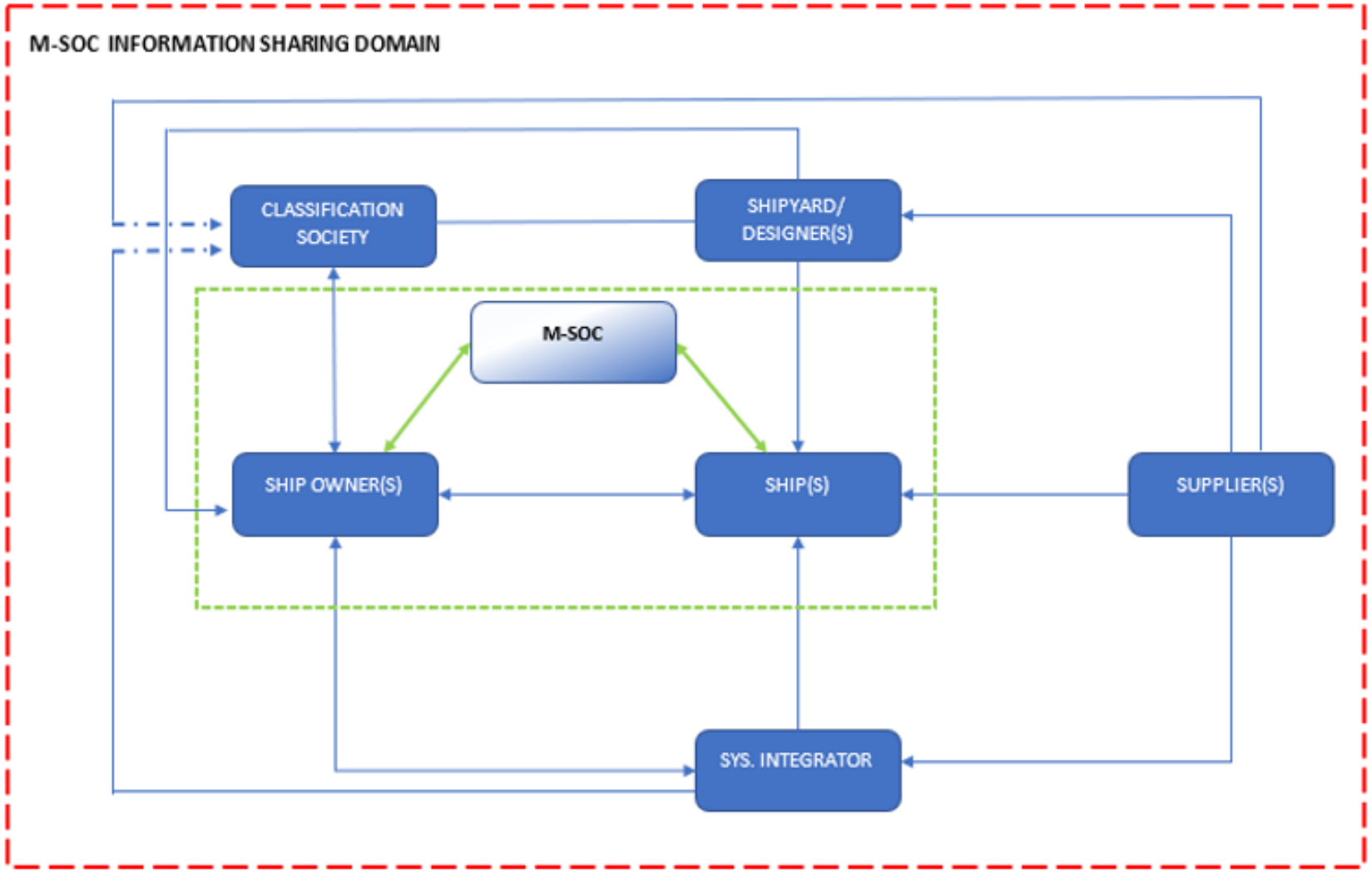
- E26: The Supplier shall design and document testing procedures suitable to verify the performance of measures adopted to fulfil relevant requirements (Test Plan)
- E26: The Shipyard or System Integrator shall incorporate the documentation provided by the Supplier into an overall Test Plan for the CBSs
- 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

Can such communication instances be taken advantage of to develop threat information sharing structures between the various stakeholders?

Identified Stakeholder Communication Instances

	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	

Proposed Vessel Cyber Threat Information Sharing Model



Key Assumptions in Model Development

- ✓All vessel resilience stakeholders identified in the guidelines are also key when it comes to sharing of threat information. Testing of the model will establish if that is the case or if some have been left out. As an example, we added M-SOCs in the model because they are a key producer of real-time vessel cyber threat information.

- ✓It is easier to build threat information communication pathways upon pre-existing mandated communication between stakeholders even though it is currently designed for regulatory compliance.

Conclusion and Future Work

Conclusion

- We proposed a cyber threat information sharing model between stakeholders identified as critical when it comes to vessel cyber resilience

Future Work

In addition to testing the validity of the assumptions made when developing the model, future work will focus on:

- Identifying the Information needs of an M-SOC
- Identifying gaps in information sharing between the highlighted stakeholders in the model
- Determining actionable cyber threat information needs of the various stakeholders

References

[1] 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.

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

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

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

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

[6] 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].

[7] 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].

References

[8] 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.

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

[10] EMSA, “Common Information Sharing Environment (CISE),” 2022. [Online]. Available: https://www.emsa.europa.eu/cise.html. [Accessed: 13-Oct-2022].

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

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

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

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