Governance for Cyber Threat Intelligence (CTI) Exchange Across the DYNAMO Resilience Cycle

Jyri Rajamäki and Anup Nepal
Laurea University of Applied Sciences, Espoo, Finland

Jyri.rajamaki@laurea.fi
Anup.Nepal@student.laurea.fi

Abstract: Cyber threats continue to escalate in complexity and frequency, underlining the need for effective Cyber Threat Intelligence (CTI) exchange to secure critical infrastructures across various sectors. However, the sharing of CTI is often impeded by concerns relating to security, trust, compliance, and coordination among stakeholders. Existing frameworks such as NIST's Risk Management Framework (RMF) and ENISA's CTI Maturity Model provide foundational guidance. Still, they are inadequate in fully addressing the sector-specific challenges realised by industries such as healthcare, energy, and maritime. This paper explores the need for a governance framework for CTI exchange by analysing existing literature, frameworks and use cases from critical sectors. The objective is to identify areas where governance is essential for ensuring secure, efficient, and compliant CTI exchange, with a particular focus on sector-specific challenges. The DYNAMO project, a European Union initiative, serves as a key case study for demonstrating how governance principles can be integrated into practical CTI exchange systems. The governance needs for CTI exchange are examined across six phases of the resilience cycle i.e. Prepare, Prevent, Protect, Respond, Recover, and Learn & Adapt. This analysis highlights how a structured governance framework can enhance the effectiveness, security, and compliance of CTI exchange in critical infrastructure sectors. By aligning governance principles with each phase of the resilience cycle, the paper demonstrates how sector-specific challenges can be addressed through improved coordination, regulatory adherence, and continuous learning. The paper concludes that while existing frameworks provide a solid foundation, sector-specific governance models are needed to address the unique risks and regulatory requirements of critical infrastructures. As DYNAMO's tools are piloted in healthcare, energy, and maritime sectors, future research will focus on validating the proposed governance model through real-world applications, ensuring that it is adaptable to evolving cyber threats and sectoral needs.

K**eywords**: Cyber threat intelligence, Governance, Resilience cycle, DYNAMO, Critical infrastructure

1. Introduction

1.1 Cyber Threat Intelligence (CTI) Overview

Cyber Threat Intelligence (CTI) has become a crucial component of modern cybersecurity, enabling organizations to proactively address cyber threats by sharing information about adversarial tactics, techniques, and procedures (TTPs). As cyberattacks grow in complexity and frequency, organizations face increasing challenges in protecting their critical infrastructure. CTI sharing across sectors and organizations has become essential for building robust cybersecurity defences (Rajamäki & Katos, 2020). However, the process of sharing threat intelligence is not without its challenges. Key issues include ensuring data security, fostering trust among participants, maintaining compliance with regulations, and coordinating actions across diverse stakeholders (Veerasamy, 2017).

While CTI exchange offers significant advantages, existing practices are often hindered by inefficiencies. These challenges stem from a lack of interoperable standards, inadequate mechanisms for governing sensitive information, and difficulties in validating the quality of shared data (El Amin et al., 2024). Although frameworks such as NIST's Risk Management Framework (RMF) and ENISA's CTI Maturity Model (ENISA, 2018) provide valuable, foundational guidelines for CTI exchange (NIST SP 800-150, 2016; ENISA, 2020), they are designed to be broadly applicable and adaptable. Sectors with specific operational challenges or stringent regulatory requirements such as healthcare, energy, and maritime often require more specialized governance models that address the unique complexities and risks inherent in these industries. In such cases, sector-specific frameworks or adaptations of existing guidelines are needed to ensure that CTI exchange is aligned with the distinct needs of critical infrastructures, regulatory standards, and operational environments. Similarly, Sukhabogi and Anusha (2021) emphasize the importance of robust CTI frameworks that support dynamic threat response, underscoring the need for effective CTI-sharing tools and platforms to facilitate real-time data flow and responsiveness to emerging cyber threats.

1.2 The Dynamo Project

The DYNAMO project, a European Union initiative, focuses on enhancing resilience against cyber threats by developing a platform that facilitates CTI exchange across various phases of the resilience cycle: Prepare, Prevent, Protect, Respond, Recover, and Learn & Adapt. The project has developed an integrated system of

tools that help organizations in critical sectors like healthcare, energy, and maritime to anticipate, mitigate, and recover from cyber incidents. The DYNAMO platform incorporates several advanced tools designed to streamline CTI sharing, such as the CTI Extractor which gathers threat intelligence, Fine-Grained Access Control to manage sensitive information, the Cyber Knowledge Graph (CKG) for visualizing relationships between threats and assets, and ThreatLens for prioritizing critical risks. Additionally, the RETA (Resilience Education, Training, and Awareness) framework has been designed to deliver structured training programs and simulation exercises, ensuring that stakeholders are well-prepared and informed on how to address evolving threats. Furthermore, the Business Continuity Management (BCM) and real-time CTI frameworks provide the necessary tools to enhance situational awareness and guide effective decision-making during cybersecurity incidents.

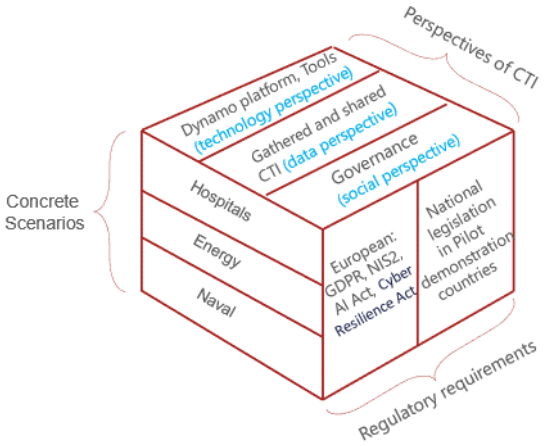

Figure 1: DYNAMO's CTI exchange environment

Figure 1 presents an overview of the CTI exchange within the DYNAMO project. Concrete cyber-attack scenarios have been developed for three critical infrastructure sectors where CTI is examined from three perspectives. The technology perspective focuses on developing the DYNAMO platform and the tools it applies. The data perspective examines the information CTI includes in each use case and demonstration. The social perspective develops the trust environment and governance framework. It is important to note that the solutions being developed must meet the requirements of relevant regulations.

By offering sector-specific solutions, the DYNAMO project seeks to address vulnerabilities unique to each critical infrastructure sector, enabling them to improve their cyber resilience. For instance, in the healthcare sector, DYNAMO helps mitigate risks posed by ransomware attacks and vulnerabilities in medical devices. In the energy sector, DYNAMO aids energy providers in safeguarding operational technologies including SCADA systems, through integrating CTI exchange mechanisms into their cybersecurity frameworks.

1.3 Objective and Structure of Paper

The objective of this paper is to explore the need for governance in Cyber Threat Intelligence (CTI) exchange by analysing existing literature, established frameworks, and real-world use cases. By focusing on sector-specific challenges, particularly in healthcare, energy, and maritime industries, the paper identifies critical areas where governance is needed and offers insights into the development of governance models that enhance resilience throughout all phases of the resilience cycle: Prepare, Prevent, Protect, Respond, Recover, and Learn & Adapt.

The rest of the paper is the following: Section 2 presents the principles necessary for the CTI governance framework through a review of the literature. The research methodology is described in Section 3. Section 4 examines the governance framework across the different phases of the resilience cycle as well as the need for its validation and continuous improvement. Section 5 considers the specific characteristics of different critical infrastructure sectors. Section 6 summarizes the article and presents the next steps.

2. Governance Framework for CTI Exchange

The increasing complexity and frequency of cyber threats necessitate effective sharing of Cyber Threat Intelligence (CTI) among organizations. Structured governance frameworks are essential to ensure secure, compliant, and efficient CTI exchange across sectors. Guidelines from international organizations such as NIST and ENISA, provide foundational insights into these frameworks, emphasizing standardized processes, data security, and the creation of trusted partnerships (NIST SP 800-150, 2016; ENISA, 2018). This literature review

analyses the key principles (Table 1) from academic research and existing frameworks to present a holistic view of CTI exchange governance.

Table 1: CTI exchange guiding principles

Principle	Explanation	Citation
Collaboration and Trust	Establishing a shared framework for gathering, validating and distributing intelligence across organizations with common interests.	Pöyhönen et al. (2019), Microsoft(2015), Dandurand & Serrano (2013), NIST (2016)
Security and Confidentiality	Implementing clear protocols to safeguard sensitive threat intelligence, ensuring data integrity and preventing unauthorized access.	Microsoft (2015), Veerasamy (2017), ENISA (2020), Henttonen & Rajamäki (2024)
Compliance and Accountability	Defining roles, responsibilities, and accountability measures to ensure all organizations adhere to regulatory requirements and frameworks.	NIST (2016), ENISA (2020), INSA (2024)
Continuous Learning and Improvement	Processes for adapting to emerging threats by learning from past incidents and continuously improving response and security mechanisms.	Microsoft (2015), Nainna et al. (2024), El Amin et al. (2024), Rajamäki & Katos (2020)

2.1 Roles and Responsibilities

A clear definition of roles and responsibilities is critical for an effective CTI exchange governance framework. NIST's Cybersecurity Framework and ENISA's CTI Maturity Model emphasize the importance of assigning specific roles within the CTI ecosystem to ensure accountability and consistent coordination between stakeholders. These roles often span across internal teams such as IT and cybersecurity including external actors like regulatory bodies, CTI providers, and law enforcement agencies (NIST CSF, 2018; NIST, 2016; ENISA, 2018).

Studies such as those by Rajamäki and Katos (2020) emphasize the role of clear responsibilities in promoting a trust-based, sustainable exchange model for early warning systems, while Yatagan (2020) highlights the broader need for coordination between governmental bodies and private sector entities. Improved role allocation and responsibilities in CTI collaboration can enhance information sharing and facilitate burden-sharing among partners (Dandurand & Serrano, 2013) allowing for an organizational structure that facilitates a reliable process of CTI exchanges (Veerasamy (2017).

2.2 Data Classification and Sensitivity Levels

Proper data classification frameworks ensure that sensitive CTI is handled securely, and that access is controlled appropriately. NIST's Special Publication 800-150 advocates for a risk-based classification of CTI, categorizing intelligence into public, confidential, and restricted levels depending on its sensitivity and the potential impact of exposure (NIST SP 800-150, 2016).

ENISA emphasizes that classification schemes should be designed to protect critical assets and confidential data, with clear protocols for sharing only the necessary information with trusted partners (ENISA, 2018). Academic sources such as El Amin et al. (2024) stress the importance of integrating CTI into broader risk management frameworks, highlighting that only relevant information is distributed based on the threat's sensitivity and severity. Moreover, implementing sophisticated encryption systems such as blockchain could ensure data integrity and confidentiality, particularly in multi-stakeholder environments where sensitive data must be classified appropriately (Chatziamanetoglou & Rantos, 2024).

2.3 Communication Protocols

Effective communication is fundamental to CTI sharing, enabling timely distribution of threat intelligence during incidents. Both NIST and ENISA recommend the establishment of formal communication channels that ensure timely sharing, especially in emergency scenarios. NIST highlights the need for various communication methods to facilitate efficient information exchange between public and private entities (NIST SP 800-150, 2016). Similarly, ENISA calls for structured approaches to incident response for cybersecurity incidents, stressing the importance of creating a common language and secure communication channels to enable effective cross-sector communication (ENISA, 2020).

Rajamäki and Katos (2020) emphasize the role of communication in Early Warning Systems (EWS) where timely and accurate information must flow across organizational boundaries to mitigate the impact of cyberattacks. Nainna et al. (2024) also highlighted the importance of establishing standardized frameworks for CTI sharing, citing challenges in Nigerian cybersecurity practices related to competing standards and insufficient protocols. These challenges underscore the need for clear, consistent communication structures to enhance CTI sharing efficiency. Additionally, INSA (2024) outlined best practices for improving communication through leveraging Information Sharing and Analysis Centers (ISACs) in industry-specific organizations.

2.4 Monitoring and Auditing

Continuous monitoring and auditing are essential to maintaining the integrity and effectiveness of a CTI exchange governance framework. NIST's Cybersecurity Framework encourages organizations to adopt automated monitoring tools that provide real-time feedback on security events, helping to detect anomalies and unauthorized access (NIST CSF, 2018).

ENISA also stresses the importance of regular audits (ENISA, 2020). Audit could help ensure periodic reviews to assess whether the shared intelligence is being used appropriately and securely. El Amin et al. (2024) argue that integrating continuous monitoring into cyber risk management frameworks is essential for maintaining situational awareness and adjusting strategies based on emerging intelligence.

2.5 Escalation Protocols

Escalation protocols ensure that critical threats are dealt with promptly and by the appropriate stakeholders. Both NIST and ENISA emphasize the importance of defining threat severity levels and setting clear procedures for escalating incidents. NIST's Incident Response Guidelines (NIST 800-61) provide a detailed framework for escalating incidents based on predefined risk thresholds, ensuring that high-priority threats are communicated to senior management or public authorities as necessary (NIST 800-61, 2012).

Henttonen and Rajamäki (2024) emphasize the importance of timely and prioritized CTI sharing among the stakeholders to ensure swift responses to threats. Introducing escalation protocols could build on these findings by directing critical threats to senior decision-makers and relevant stakeholders, enhancing the overall responsiveness and effectiveness of cybersecurity measures.

2.6 Training and Awareness Programs

Continuous training is necessary to ensure that stakeholders involved in CTI exchange remain well-informed about emerging threats and changes in governance protocols. NIST recommends regular cybersecurity awareness training, particularly for personnel involved in CTI exchange to improve incident response, intelligence interpretation and regulatory compliance (NIST CSF, 2018; NIST 800-150, 2016).

ENISA also stresses the need for structured training programs that keep pace with advancements in CTI technologies and the evolving threat landscape (ENISA, 2020). The DYNAMO RETA framework developed as part of the DYNAMO project, offers a structured approach to education that ensures that CTI stakeholders are adequately trained to respond to new and emerging threats. This framework focuses on continuous learning and simulation exercises to improve resilience and readiness in cyber defence strategies.

2.7 Compliance with Regulations

Compliance with regulatory frameworks such as GDPR, HIPAA, and EPCIP is critical for CTI sharing. Both NIST SP 800-150 and ENISA emphasize the need for maintaining compliance with national and international standards (ENISA, 2020) to ensure secure and effective CTI (NIST, 2016). INSA (2024) further highlights the importance of adhering to legal frameworks, especially in the context of cross-sector CTI sharing.

Nainna et al. (2024) emphasize the importance of integrating regulatory compliance mechanisms into CTI sharing to ensure that data-sharing practices align with privacy laws and ethical standards. Rajamäki and Katos (2020) discuss the regulatory challenges associated with cross-border CTI sharing particularly in industries like healthcare and energy where compliance requirements can vary significantly between regions.

2.8 Risk Management

Risk management is a core component of both NIST and ENISA frameworks. NIST's Risk Management Framework (RMF) guides on identifying, assessing, and mitigating overall risks while NIST SP 800-150 focuses on risks related to CTI sharing. ENISA similarly advocates for a risk-based approach, recommending that

organizations continuously assess the potential impact of cyber threats and adjust their CTI strategies accordingly (ENISA, 2020).

El Amin et al. (2024) emphasize the need for a dynamic risk management framework that integrates CTI into its processes, enabling organizations to better understand adversarial tactics and proactively adjust their defence strategies. Rajamäki and Katos (2020) also stress the need for continuous evaluation of risks in Early Warning Systems, advocating for real-time threat monitoring and proactive threat mitigation strategies.

3. Methodology

This paper employs a qualitative research approach to explore the need for governance in the Cyber Threat Intelligence (CTI) exchange. The research is based on a comprehensive analysis of existing literature, established cybersecurity frameworks, and real-world use cases, with a focus on sector-specific challenges faced by industries such as healthcare, energy and maritime.

The methodology draws insights from recognized frameworks including NIST's Risk Management Framework (RMF) and ENISA's CTI Maturity Model, as well as practical tools and documentation from the DYNAMO project. These sources provide a foundation for identifying gaps in governance and areas where more structured approaches are needed to ensure secure, compliant and efficient CTI sharing.

Rather than proposing a governance model, this paper synthesizes findings from these varied sources to highlight critical areas where governance needs to be further developed. The analysis is structured around the six phases of the resilience cycle i.e. Prepare, Prevent, Protect, Respond, Recover, and Learn and Adapt—to ensure that governance principles are adaptable to the unique operational environments and regulatory demands of each sector. By focusing on the integration of governance into practical applications and real-world challenges, this methodology aims to provide insights for further development of sector-specific governance models on CTI exchange.

4. Synthesis

The literature review established the importance of key governance principles such as collaboration, security, and compliance in CTI sharing, drawing on best practices from existing frameworks. Furthermore, the literature also elaborates on key governance elements such as structured roles, clear communication protocols, continuous monitoring and so on which are crucial for fostering trust and ensuring the effective sharing of threat intelligence. However, existing frameworks may not fully address the sector-specific challenges or operational complexities in fields such as healthcare, energy, and maritime.

4.1 CTI Governance Across the Dynamo Resilience Cycle Phases

Building upon these theoretical foundations, this section explores how governance principles could be applied in the DYNAMO project across the six phases of the resilience cycle: Prepare, Prevent, Protect, Respond, Recover, and Learn and Adapt. Each phase represents a unique set of challenges and governance needs, especially when integrating DYNAMO tools such as the CTI Extractor, ThreatLens, and CKG.

While DYNAMO's approach shows promise, this section highlights the critical areas where governance needs further attention, especially in ensuring secure, compliant and efficient CTI exchange. Each phase presents distinct governance challenges that require careful consideration, and the DYNAMO tools offer potential solutions that must be evaluated in real-world sectoral contexts.

Table 2: Mapping the governance objectives with corresponding DYNAMO application use cases

Resilience Phases	Governance Objectives	DYNAMO Application
Prepare Phase	• Identify **critical assets** and infrastructure that require protection. • Establish clear **roles and responsibilities** for collecting, sharing, and using CTI. • Implement **training and awareness programs** to ensure stakeholders understand how to contribute to and benefit from the CTI exchange. • Foster collaboration across sectors, utilizing tools like the **RETA framework** to simulate attacks and enhance preparedness. • Develop agreements for **data sharing** and **intelligence classification** to ensure that only relevant and validated threat intelligence is exchanged.	• DYNAMO's CTI and BCM frameworks can be used to help organizations identify risks and develop situational awareness during this phase, providing a structured approach to preparedness. • Dynamo Tools such as **CTI Extractor, Fine-Grained Access Control, CKG**, etc. to extract threat intelligence, define access rules for handling sensitive intelligence and visualize relation between threat, assets and vulnerabilities to map critical assets and threats effectively.
Prevent Phase	• Implement **risk management** protocols to use CTI for identifying and addressing both known and unknown threats. • Ensure that CTI is shared in a **timely** and **actionable** manner, allowing organizations to take preventative measures based on shared intelligence. • Establish protocols for continuously **validating** and **updating** shared threat intelligence to ensure it remains relevant.	• DYNAMO's **real-time CTI framework** helps in forecasting potential threats and anomalies, which should be integrated into the governance model to ensure proactive threat prevention. • Tools like **EWS** and **ThreatLens** provide timely alerts and prioritize critical risks, while **Data Anonymization** ensures sensitive intelligence is shared securely.
Protect Phase	• Define **data protection policies** for handling sensitive intelligence shared across the CTI exchange. • Mandate **continuous monitoring** of critical systems for early detection of threats, based on shared intelligence. • Establish **automated or manual response protocols** to rapidly mitigate identified threats using CTI.	• **DYNAMO's BCM** framework enables situational awareness and offers real-time mitigation plans based on threat intelligence. Tools such as **Cyber Knowledge Graph (CKG)** protect by mapping real-time threats to specific assets, helping organizations adjust their defenses. **Fine-Grained Access Control** ensures that sensitive intelligence is accessible only to authorized personnel, reducing exposure to insider threats. Additionally, **ThreatLens** helps prioritize mitigation efforts by identifying the most critical risks that need immediate attention, while **Data Anonymization** protects privacy when sharing intelligence with external parties.
Respond Phase	• Develop clear protocols for **sharing real-time threat intelligence** during an active incident, ensuring timely dissemination across all relevant stakeholders. • Establish **coordinated response procedures**, where multiple organizations can act based on shared intelligence to contain and mitigate the impact of the attack. • Create **escalation pathways** for high-priority intelligence, ensuring the most critical threats are addressed first.	• Utilize DYNAMO's **real-time situational awareness tools**, which enhance response coordination. The governance framework should formalize how threat intelligence will be shared and used to guide response efforts. • DYNAMO's **real-time tools** such as **EWS** and **CTI Extractor** enable fast, coordinated responses by sharing actionable intelligence across stakeholders. **CKG** maps the attack's progression while **ThreatLens** prioritizes urgent risks. **Fine-Grained Access Control** ensures that only authorized users handle sensitive response activities.

Recover Phase	• Use CTI to inform and guide the **restoration of systems** after an incident, ensuring recovery efforts address the root causes. • Establish processes for reviewing the **effectiveness of recovery efforts,** incorporating lessons learned from the CTI exchange into future recovery plans. • Encourage the use of **AI-driven solutions** to automate recovery efforts, minimizing downtime.	• The DYNAMO framework's **AI-based recovery tools** should be incorporated into the governance model to ensure that organizations can recover quickly and efficiently, based on shared intelligence. Tools such as **CKG** and **ThreatLens** prioritize critical systems for recovery, ensuring efficient restoration. **AI-enhanced analytics** guide recovery strategies by analyzing attack vectors, and **CTI Extractor** feeds relevant intelligence into the recovery process to speed up system restoration.
Learn and Adapt Phase	• Establish a structured process for **reviewing past incidents** and how CTI was used to respond, prevent, and recover from those incidents. • Implement feedback loops to **update CTI policies**, tools, and practices based on real-world events. • Foster ongoing t**raining and education** for stakeholders to adapt to new and emerging threats, ensuring resilience improvement over time.	• DYNAMO's **RETA framework** offers tools for ongoing resilience training and adaptation. Governance should formalize these educational processes, ensuring that CTI users continuously learn from shared intelligence and past incidents. • **CKG** helps analyze historical threat data while **CTI Extractor** gathers post-incident intelligence to improve future defenses. **ThreatLens** further identifies recurring vulnerabilities for adaptation.

4.2 Validation and Continuous Improvement

Drawing on the DYNAMO project documentation, the governance framework for CTI exchange must include mechanisms for continuous validation and improvement. Since governance needs will evolve, it is essential to measure effectiveness through pilot programs and sector-specific tests.

- **Establish KPIs**: Governance must ensure the continuous measurement of metrics such as timeliness, accuracy, and adoptability of CTI.
- **Quantitative and Qualitative Assessments**: Feedback from stakeholders and data from pilots will help assess how well the governance model supports CTI sharing.
- **Sector-Specific Validation:** As DYNAMO tools are applied to sectors like Energy, Healthcare, and Maritime, the governance framework must be customized to meet the unique needs of each sector.
- **Regular Feedback Loops:** Governance should incorporate regular feedback loops that refine CTI sharing policies and processes, ensuring that emerging threats are continuously accounted for.

5. Practical Governance Implementation Across Critical Infrastructure

This section demonstrates how the governance needs identified across the resilience cycle can be practically applied within key critical infrastructure sectors such as healthcare, energy, and maritime. Each sector faces unique challenges in Cyber Threat Intelligence (CTI) exchange, requiring specific governance approaches that ensure data security, regulatory compliance, and operational efficiency.

Table 3: Example of practical governance implementation in Health, Energy and Maritime sector

Critical Infra-structure Sector	Actors	Information Exchanged	Agreements	Tools Used
Healthcare Sector (Hospitals)	Healthcare IT Teams Medical Device Manufacturers Healthcare Providers Regulatory Bodies	Ransomware alerts Vulnerabilities in patient data systems Malware threats in medical devices	Data-sharing agreements aligned with HIPAA and GDPR Clear incident response protocols when patient data systems are compromised	CTI Extractor to gather intelligence on medical device vulnerabilities CKG to map threats to healthcare networks. Fine-Grained Access Control to restrict sensitive data access

Energy Sector	Energy Providers SCADA Engineers CTI Providers Government Agencies	Threat intelligence on vulnerabilities in SCADA systems Real-time alerts for grid attacks. and supply chain risks	Data-sharing agreements with government bodies to align with NERC-CIP standards Incident response plans involving the national energy grid	EWS for real-time alerts on SCADA vulnerabilities. CKG to map threats to energy infrastructure AI-based recovery tools to prioritize and restore critical energy systems
Maritime Sector	Shipping Companies Port Authorities Navigation System Providers Coast Guards	GPS jamming threats Navigation system cyber-attacks Risks to port communication networks	Confidentiality and early warning protocols between port authorities and shipping companies Collaboration agreements with government security agencies	CTI Extractor for navigation system threats, CKG for tracking threats to shipping operations ThreatLens to prioritize and respond to risks

6. Conclusion

This paper examines the necessity for a comprehensive governance framework for Cyber Threat Intelligence (CTI) sharing, with a focus on sectors such as healthcare, energy, and maritime. While established frameworks like NIST and ENISA provide important guidance, the specific operational challenges and regulatory needs of these sectors call for a more tailored approach. For instance, NIST's Risk Management Framework (RMF) presents a structured methodology for risk management but falls short in offering detailed guidance for cross-sector intelligence sharing, a crucial element for interconnected industries.

Similarly, ENISA's CTI Maturity Model is useful for assessing an organization's capabilities but does not adequately address the dynamic threat landscape faced by critical infrastructures, which require sector-specific governance mechanisms. The model's emphasis on individual organizational maturity may limit its effectiveness in adopting coordinated, multi-stakeholder resilience—a necessity for interdependent infrastructures.

Through an analysis of the DYNAMO project and its associated tools, this paper highlights key areas where governance is essential throughout the resilience cycle. This includes defining roles and responsibilities during the Prepare phase, formalizing data-sharing protocols during the Protect phase, and integrating lessons learned during the Learn and Adapt phase. Effective governance is crucial to ensuring the secure, efficient, and compliant exchange of threat intelligence. As DYNAMO's tools are piloted in critical sectors, future research should prioritize validating these governance requirements through practical, real-world applications. Pilot programs in the healthcare, energy, and maritime sectors will provide valuable insights into the effectiveness of the proposed governance structures in addressing sector-specific challenges. Such validation will help ensure that governance models are responsive to the unique needs of each sector while remaining flexible enough to adapt to evolving threats.

Acknowledgements

Acknowledgment is paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

Chatziamanetoglou, D., and Rantos, K. (2024) Cyber Threat Intelligence on Blockchain: A Systematic Literature Review, Computers, 13, 60. https://doi.org/10.3390/computers13030060.

Dandurand, L. and Serrano, O., 2013. Towards improved cyber security information sharing. 5th International Conference on Cyber Conflict (CYCON 2013), pp.1-16.

El Amin H, Samhat AE, Chamoun M, Oueidat L, Feghali A. An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. Journal of Cybersecurity and Privacy. 2024; 4(2):357-381. https://doi.org/10.3390/jcp4020018

ENISA (2018) CTI Capability Maturity Model presentation. Available at https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cti-eu-cti-capability-maturity-model.pdf

ENISA (2020) National Capabilities Assessment Framework (NCAF). Available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool/#/

ENISA(2020) Cyber Threat Intelligence Overview in ENISA Threat Landscape 2020. Available at https://www.enisa.europa.eu/publications/cyberthreat-intelligence-overview

Henttonen, K. and Rajamäki, J., 2024. CTI sharing practices and MISP adoption in Finland's critical infrastructure protection. European Conference on Cyber Warfare and Security, 23, p.10.34190/eccws.23.1.2352.

INSA (2024) Challenges and Opportunities of Enabling Information Sharing. Accessed on 22.10.2024 at https://www.insaonline.org/docs/default-source/uploadedfiles/2024/insa_cyber_information_sharing.pdf.

Microsoft (2015) A framework for cybersecurity information sharing and risk reduction. Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=45516.

Nainna, M. A., Bass, J., and Speakman, L. (2024) Cyber Threat Intelligence Sharing in Nigeria. International Information Management Association (IIMA). Conference Proceedings 2024.

NIST (2012) NIST 800-61: Computer Security Incident Handling Guide, National Institute of Standards and Technology. Available at https://csrc.nist.gov/pubs/sp/800/61/r2/final

NIST (2016) NIST SP 800-150: Guide to Cyber Threat Information Sharing, National Institute of Standards and Technology. Available at https://csrc.nist.gov/pubs/sp/800/150/final

NIST CSF (2018) Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology. Available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

NIST RMF (2018) Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37, Revision 2, National Institute of Standards and Technology.

Pöyhönen, J., Nuojua, V., Lehto, M., and Rajamäki, J. (2019) Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations, Information & Security: An International Journal, 43(2), 236-256. https://doi.org/10.11610/isij.4318.

Rajamäki J., and Katos, V. (2020) Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. Information & Security: An International Journal,46no. 2(2020):198-214.https://doi.org/10.11610/isij.4614

Sukhabogi, R., and Anusha, V. (2021) A Theoretical review on the importance of Threat Intelligence Sharing & The challenges intricated. Turkish Journal of Computer and Mathematics Education. Vol.12 No.3(2021), 3950-3956 Veerasamy, N. 2017. Cyber threat intelligence exchange: A growing requirement. Proceedings of the 16th European Conference on Cyber Warfare and Security, Dublin, Ireland, 29-30 June 2017, p. 513-518. https://researchspace.csir.co.za/items/5d14e816-9223-4dfc-96fa-ceee595909c5

Yatagan C (2022). Interaction between the U.S. intelligence community and the private sector in sharing cyber threat intelligence. [Order No. 29998393]. American University; 2022.