Enhancing Cyber Threat Intelligence (CTI) Exchange: A Governance Model for the DYNAMO Platform

Jyri Rajamäki[1], Anup Nepal[1] and Ioannis Chalkias[2]
[1] Laurea University of Applied Sciences, Espoo, Finland
[2]Ethniko Kentro Erevnas Kai Technologikis Anaptyxis, Greece

Jyri.rajamaki@laurea.fi
Anup.Nepal@student.laurea.fi
ichalkias@iti.gr

Abstract: The growing complexity of cyber threats, especially within critical infrastructure sectors like healthcare, energy, and maritime, highlights the need for comprehensive frameworks to facilitate the exchange of Cyber Threat Intelligence (CTI). This paper presents a CTI Exchange Governance Model aimed at enhancing the CTI sharing process within the DYNAMO platform, a European Union initiative focused on improving resilience against cyber threats across various phases of the resilience cycle: Prepare, Prevent, Protect, Respond, Recover, and Learn & Adapt. The DYNAMO project provides a suite of tools and strategies to support organizations in critical sectors, enabling efficient threat detection, mitigation, and response while fostering collaboration and compliance with regulatory standards. Sector-specific scenarios have been developed to address unique vulnerabilities in areas like healthcare, energy, and maritime, ensuring practical and targeted solutions for improving cyber resilience. While DYNAMO's integrated tools handle CTI generation and alerts, a standardized and cohesive framework is still needed to guide and streamline CTI sharing across sectors, addressing gaps in current practices that impact interoperability and timely response. This governance model is structured around five key pillars: Collaboration & Trust, Data Sensitivity & Standardization, Compliance & Regulatory Alignment, Real-Time Collaboration & Response, and Continuous Learning & Improvement. These pillars ensure a secure, standardized, and compliant approach to CTI exchange, particularly in sectors vulnerable to increasingly sophisticated attacks. The model is uniquely tailored to align with DYNAMO's mission, offering a sector-specific approach while integrating best practices from established cybersecurity frameworks. The model is operationalized through the DYNAMO platform, leveraging tools like the Early Warning System (EWS) for real-time CTI sharing and a Data Anonymization Tool to ensure privacy and regulatory compliance. As a result, a practical framework has been developed to tailor the model's implementation across healthcare, energy, and maritime sectors, ensuring a scalable and adaptable approach to CTI sharing. Ultimately, the governance model enhances CTI exchange by addressing interoperability challenges and strengthens governance practices to support collaboration, improve incident response times, and foster continuous improvement.

Keywords: Cyber threat intelligence (CTI), CTI exchange, Governance model, DYNAMO Platform, Critical infrastructure

1. Introduction

Cyber Threat Intelligence (CTI) exchange has never been more urgent. CTI enables organizations to detect, anticipate, and mitigate cyber threats collaboratively, leveraging shared intelligence to strengthen sectoral defenses and improve incident response capabilities (Cha et al., 2020; Saeed et al., 2023). Moreover, effective CTI sharing fosters trust and cooperation among stakeholders, creating a unified front against sophisticated threats (Du et al., 2020).

Despite its critical importance, several challenges hinder seamless CTI sharing. Interoperability gaps between tools and protocols, a lack of standardization in data formats, and stakeholder trust issues limit the efficiency of CTI exchanges (Dandurand & Serrano, 2013). Sector-specific regulatory requirements and privacy concerns create significant obstacles to cross-sector collaboration and cyber threat intelligence (CTI) exchange. This is particularly evident in sectors such as healthcare, where protecting sensitive patient data is paramount, or energy and maritime industries, where operational risks are high (Susha et al., 2023). These barriers highlight the need for a structured governance model to guide and streamline CTI sharing, ensuring secure, standardized, and compliant exchanges across sectors.

The DYNAMO platform [1], an initiative of the European Union, aims to address these challenges by providing a suite of tools and strategies for CTI collection, analysis, and dissemination. Tools such as the Early Warning System (EWS) for real-time threat sharing, Data Anonymization Tool, and Fine-Grained Access Control for privacy compliance enhance situational awareness and strengthen cyber resilience. However, while these tools address

[1]DYNAMO https://horizon-dynamo.eu/about/

specific technical aspects of CTI generation and sharing, a cohesive governance framework is needed to standardize practices, foster collaboration, and ensure interoperability across sectors.

This paper proposes a CTI Exchange Governance Model, structured around five key pillars: Collaboration & Trust, Data Sensitivity & Standardization, Compliance & Regulatory Alignment, Real-Time Collaboration & Response, and Continuous Learning & Improvement. Drawing on established frameworks such as NIST SP 800-150 and ENISA's guidelines, the model is uniquely tailored to the DYNAMO platform and addresses sector-specific challenges in healthcare, energy, and maritime. The governance model operationalizes CTI sharing through practical tools and processes, ensuring a scalable, adaptable, and secure approach to improving cyber resilience across critical infrastructure sectors.

1.1 Research Questions and Hypothesis

This paper explores the following research questions:

RQ1: How can a governance model address interoperability and standardization challenges in CTI sharing among the critical infrastructure sectors?

RQ2: How can DYNAMO tools operationalize the proposed governance model for effective CTI exchange?

> *A structured governance model and operationalization framework will streamline CTI exchange within the DYNAMO platform, addressing gaps in interoperability, standardization, and sector-specific needs.*

1.2 Structure of the Paper

Section 2 reviews related work, including existing CTI frameworks and sectoral challenges. Section 3 describes the DYNAMO platform and its tools. Section 4 explains the methodologies used. Section 5 introduces the proposed governance model, followed by Section 6, which details the operationalization framework. Finally, the discussion and conclusion reflect the model's implications, challenges, and future opportunities.

2. Background and Related Work

2.1 Cyber Threat Intelligence (CTI) and CTI Exchange

Cyber Threat Intelligence (CTI) is defined by the National Institute of Standards and Technology (NIST) as information that aids in identifying, analyzing, and responding to cyber threats by providing actionable insights (NIST, 2016). CTI plays a pivotal role in cybersecurity by enhancing situational awareness and enabling organizations to anticipate, identify, and mitigate potential attacks (Cha et al., 2020; Saeed et al., 2023). Integrating CTI into cybersecurity strategies significantly strengthens an organization's security posture through proactive threat management, improved detection and response capabilities, and increased collaboration among stakeholders (Ofoegbu et al., 2023; Saeed et al., 2023).

While CTI is crucial for defending against known threats, its full potential is realized through the exchange of intelligence, which enhances an organization's security awareness and preparedness. Effective intelligence sharing fosters collaboration and allows organizations to address threats more comprehensively (Pahlevan & Ionita, 2022), regardless of their complexity or scale. For instance, CTI sharing equips organizations to anticipate and counter sophisticated threats such as Advanced Persistent Threats (APTs) (Jin et al., 2024).

The importance of CTI exchange lies in the need for collaborative, secure, and scalable processes that facilitate seamless intelligence sharing among internal and external stakeholders. To achieve this, platforms for CTI exchange must support the collection, analysis, and processing of diverse threat data while ensuring privacy, traceability, and governance compliance to maintain trust among participants (Alaeifar et al., 2024).

2.2 Existing Tools and Frameworks in CTI Sharing

Several frameworks and tools have been developed to facilitate CTI sharing, including:

- STIX/TAXII: STIX provides a unified language for representing Indicators of Compromise (IoCs), Tactics, Techniques, and Procedures (TTPs), enabling structured and interoperable CTI sharing.[2] Paired with TAXII for automated data exchange, it facilitates collaboration and integration with tools like SIEM systems. While its setup and learning require time investment, STIX improves clarity, consistency, and scalability, making it a cornerstone of modern CTI sharing (Jin et al., 2024; Nicole Gong, 2024).

[2] STIX. Introduction to STIX. https://oasis-open.github.io/cti-documentation/stix/intro

- MISP: MISP (Malware Information Sharing Platform) is an open-source tool for sharing, analyzing, and managing cyber threat intelligence. It enables organizations to collaborate on indicators of compromise (IOCs), attack patterns, vulnerabilities and supporting formats like STIX. Widely used by CERTs and SOCs, MISP enhances situational awareness and automates threat intelligence sharing. [3]
- Blockchain-enabled Platforms: Emerging technologies that enhance trust, traceability, and data security in CTI sharing but face challenges such as scalability and interoperability. The papers by Cha et al. (2020) and Pahlevan & Ionita (2022) propose solutions to address these bottlenecks.

2.3 Challenges in CTI Sharing

Despite the above-mentioned tools and framework for CTI sharing, key challenges persist:

- Interoperability Gaps: Variations in data formats and sharing protocols complicate integration across organizations and sectors (Dandurand & Serrano, 2013; Keyamo et al. 2024; NIST, 2016).
- Privacy and Security Concerns: Sharing sensitive information involves risks, particularly when data originates from unverified sources or lacks adequate anonymization (Alaefar et al., 2024) or if the data holds personal information (Cha et al. 2020).
- Limited Real-Time Capabilities: Current frameworks often lack the ability to rapidly exchange actionable intelligence during active cyber incidents. However, emerging AI and ML technologies are paving the way for tools that facilitate automation and improve speed (Santoso, 2024).

Sector-specific challenges further complicate CTI sharing. In healthcare, protecting sensitive patient data must be balanced with addressing vulnerabilities in medical devices. The energy sector deals with threats to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, while the maritime sector faces risks related to vessel tracking and communication networks.

These gaps underscore the need for a structured governance model that ensures standardized, secure, and sector-specific CTI sharing.

3. The DYNAMO Platform

The DYNAMO project, an initiative of the European Union, addresses the growing complexity of cyber threats targeting critical sectors such as healthcare, energy, and transport. With increasing digitalization and evolving cyber risks, safeguarding critical infrastructure has become essential for ensuring business continuity. DYNAMO brings together experts and end-users from diverse backgrounds to develop and refine tools into a unified platform designed to enhance resilience against cyber threats across the resilience cycle: Prepare, Prevent, Protect, Respond, Recover, and Learn & Adapt.

Concrete cyber-attack scenarios have been developed within DYNAMO to address vulnerabilities unique to three critical infrastructure sectors: healthcare, energy, and maritime. These scenarios are analyzed from three perspectives:

- Technology Perspective: Focuses on the development and application of the DYNAMO platform and its tools.
- Data Perspective: Examines the information included in CTI use cases and demonstrations.
- Social Perspective: Develops trust environments and governance frameworks to foster collaboration and compliance with regulations.

Figure 1 illustrates the CTI exchange environment within the DYNAMO project, highlighting the interconnectedness of tools, stakeholders, and governance mechanisms.

[3] MISP. Malware Information Sharing Platform (MISP) Available at: https://www.misp-project.org/#:~:text=The%20MISP%20is%20an%20open,incidents%20analysis%20and%20malware%20analysis.

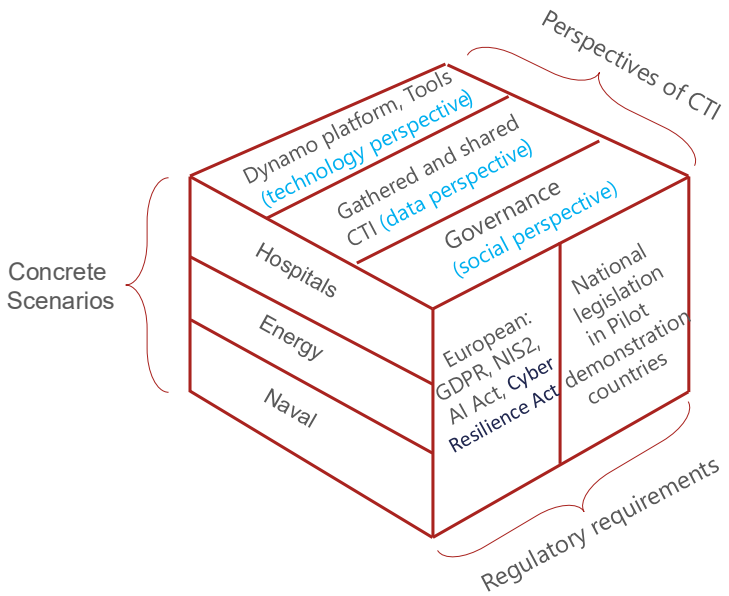

Figure 1: DYNAMO CTI exchange environment

By offering sector-specific solutions, DYNAMO addresses vulnerabilities unique to each domain. For example, in healthcare, it mitigates risks from ransomware attacks and medical device vulnerabilities. In the energy sector, it safeguards operational technologies such as SCADA systems by embedding CTI exchange mechanisms into cybersecurity strategies. In the maritime domain, it addresses risks related to vessel tracking, port security, and communication systems.

Through its comprehensive and adaptive framework, the DYNAMO project empowers critical infrastructure sectors to enhance their cyber resilience and respond effectively to the dynamic threat landscape.

3.1 DYNAMO Tools for CTI Exchange

The project provides a comprehensive suite of tools to support critical sectors in anticipating, mitigating, and recovering from cyber incidents. The DYNAMO platform integrates advanced tools designed to streamline CTI generation and dissemination to improve decision-making.

These are three DYNAMO tools focusing on CTI exchange:

- DYNAMO EWS: A near real-time tool for coordinating and sharing cyber-incident information across organizational boundaries. It supports collaborative incident management, impact assessment, and seamless integration with existing tools.
- DYNAMO Fine-Grained Access Control Solution: Based on Attribute-Based Encryption (ABE), this solution enables secure and flexible data sharing by enforcing granular access policies and ensuring efficient access revocation for sensitive information.
- DYNAMO Data Anonymization Tool: A tool with a user-friendly interface that guides users through dataset anonymization, supporting reusable privacy configuration to ensure compliance with data protection standards.

4. Methodology

This study employs a qualitative approach to evaluate and refine the proposed CTI Exchange Governance Model within the DYNAMO platform. The methodology integrates insights from existing frameworks, DYNAMO project documentation, and academic literature to address CTI sharing, interoperability, and sector-specific challenges.

The main phases of the study were:

- Framework and Regulation Analysis: Examination of standards such as NIST SP 800-150 and ENISA's guidelines, alongside regulations like GDPR and HIPAA, to establish foundational principles for governance.
- DYNAMO Documentation Review: Analysis of tools, use cases, and technical specifications, ensuring alignment between the governance model and platform capabilities.

- Literature Review: Review of sector-specific challenges and CTI best practices to contextualize the model.
- Model Development: Integration of findings to design the five-pillar governance model and an operational framework with measurable KPIs.

5. CTI Governance Model

The proposed CTI Exchange Governance Model is structured around five pillars (Fig 2): Collaboration & Trust, Data Sensitivity & Standardization, Compliance & Regulatory Alignment, Real-Time Collaboration & Response, and Continuous Learning & Improvement. Each pillar is specifically tailored to meet the needs of the DYNAMO platform, ensuring that CTI sharing processes are effective, secure, and interoperable. The model aligns with the insights and best practices from established frameworks such as NIST SP 800-150 for CTI sharing and ENISA's guidelines for cybersecurity practices.

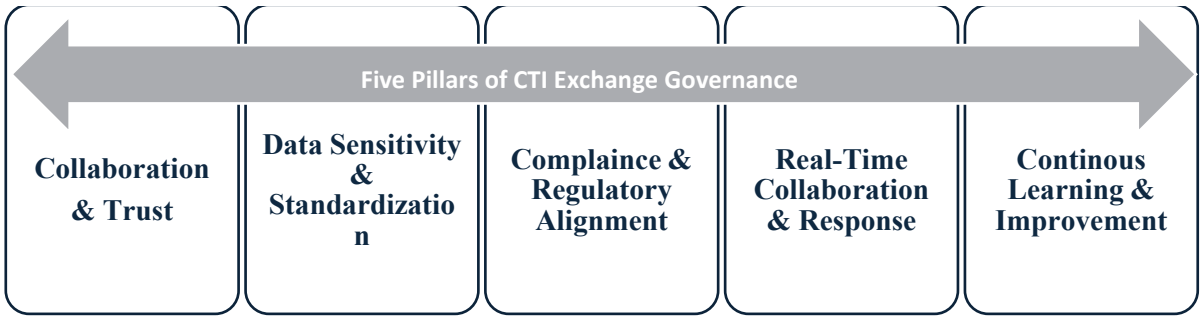

Figure 2: Five pillars of CTI exchange governance

Next, these five pillars will be examined in greater detail, outlining their objectives, key components, and the tools utilized.

5.1 Collaboration and Trust

Objective: Foster mutual trust among stakeholders to enable secure and effective CTI exchange.

Key Components:

- Integration with DYNAMO Partners: Sector-specific trust groups are aligned with ENISA's recommendations for Information Sharing and Analysis Centers (ISACs), which facilitate collaboration and trust among stakeholders in critical infrastructure sectors (ENISA, 2017).
- NDAs and MOUs: Formal agreements such as Non-Disclosure Agreements (NDAs) and Memoranda of Understanding (MOUs) establish clear terms for collaboration and ensure data confidentiality (NIST, 2016).
- Public-Private Partnerships: Public and private entities are brought together on DYNAMO's platform to strengthen collaborative defense strategies, as highlighted by ENISA's Public-Private Cooperation Model (ENISA, 2018).

Tools Used:

- Early Warning System (EWS): Enables near real-time alerts and facilitates information sharing within trust groups.

Goal: Build secure, trust-based ecosystems that encourage collaboration and ensure reliable CTI sharing.

5.2 Dat Sensitivity and Standardization

Objective: Ensure that CTI is appropriately classified and shared in standardized formats to enable interoperability and security.

Key Components:

- Data Classification: Sector-specific classification schemes (e.g. public, confidential, restricted) are implemented.
- Standardized Formats: The use of standard delivery methods such as STIX/TAXII for CTI sharing ensures consistency and interoperability across sectors, as recommended by NIST (2016).

- Metadata Enrichment: Relevant metadata, like Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs), is added to enhance actionable intelligence (NIST, 2016).

Tools Used:

- Data Anonymization Tool: Protects sensitive information in compliance with regulations such as GDPR and HIPAA.
- STIX/TAXII: Enables standardized, secure exchange of threat intelligence.

Goal: Facilitate consistent, secure, and actionable CTI sharing that aligns with interoperability standards.

5.3 Compliance and Regulatory Alignment

Objective: Ensure that CTI exchanges comply with applicable legal and regulatory frameworks, safeguarding privacy and data protection.

Key Components:

- Regulatory Compliance: Adheres to compliance such as GDPR, HIPAA, NERC CIP and other country and sector-specific compliance requirements to protect sensitive data and ensure legal conformity
- Encryption and Privacy: Implements encryption for sensitive data and anonymization for Personally Identifiable Information (PII).

Tools Used:

- Fine-Grained Access Control Framework: Provides Attribute-Based Encryption (ABE), secure, role-based access to sensitive CTI.
- EWS: Ensures secure CTI sharing and regulatory compliance.
- Data Anonymization Tool: Protects sensitive information in compliance with regulations such as GDPR and HIPAA.

Goal: Maintain compliance with sector-specific and international regulations to protect the integrity and security of CTI exchanges.

5.4 Real-Time Collaboration and Response

Objective: Enable rapid and coordinated sharing of CTI to mitigate cyber incidents effectively in real-time.

Key Components:

- Automated Threat Feeds: Disseminates real-time alerts and threat intelligence to stakeholders.
- Collaboration Tools: Regular meetings, encrypted emails, web portals, are employed to ensure secure and efficient communication aligning with ENISA's guidelines for ISACs (ENISA, 2017). In addition to traditional tools, modern platforms like Slack or Microsoft Teams may complement communication workflows to enhance real-time coordination among stakeholders.
- Incident Response Protocols: Develop sector-specific response protocols aligned with NIST's Incident Response Guidelines (SP 800-61) to ensure timely and structured responses (NIST, 2012).

Tools Used:

- EWS: Shares automated alerts and facilitates near real-time data exchange.
- Collaboration Platforms: Enable seamless communication during incident response.

Goal: Minimize the impact of cyber incidents through fast, coordinated, and actionable threat responses.

5.5 Continuous Learning and Improvement

Objective: Enhance the CTI exchange process through stakeholder feedback, post-incident reviews, and ongoing training.

Key Components:

- Post-Incident Reviews: Evaluate incident handling to identify gaps and improve response strategies, as outlined in NIST SP 800-150 (2016).
- Stakeholder Feedback: Feedback loops collect insights from stakeholders to refine processes and tools.

Tools Used:

- DYNAMO Platform: Provides a centralized system for feedback collection and training programs.

Goal: Foster continuous improvement and adaptability to evolving threats.

6. Practical Framework for Operationalizing the Governance Model

Table 1 presents the operationalization framework overview. The framework translates the proposed governance model into actionable processes tailored to real-world scenarios. It leverages advanced tools, methodologies, and clearly defined performance indicators to ensure effective implementation across critical infrastructure sectors. This framework bridges the gap between theoretical principles and practical execution by focusing on scalability, adaptability, and measurable outcomes. The framework also defines Key Performance Indicators (KPIs) to track and evaluate the success of CTI sharing efforts, ensuring continuous improvement and alignment with organizational objectives.

Table 1: Governance model's operational framework overview

Element	Purpose	Key Components	Guiding Questions	Goal	KPIs
Collaboration & Trust	Build trust and facilitate secure CTI exchange.	- ISACs, NDAs, MOUs. - EWS for early warning.	- How can trust be established and maintained among stakeholders? - What mechanisms (e.g., agreements, policies) are required to enable secure collaboration?	Foster collaboration and secure sharing.	- Collaboration Frequency. - Trust Agreement Rate.
Data Sensitivity & Standardization	Ensure standardized and secure data sharing.	- Data Anonymization Tool. - STIX/TAXII.	- How can sensitive data be classified and protected during sharing? - Are current data formats interoperable across stakeholders?	Ensure actionable intelligence sharing.	- Format Compliance Rate. - Data Sensitivity Compliance.
Compliance & Regulatory Alignment	Maintain adherence to regulations.	- Fine-Grained Access Control Framework. - GDPR and HIPAA audits.	- Are all CTI sharing processes compliant with applicable regulations (e.g., GDPR, HIPAA)? - What audit mechanisms are in place to ensure accountability and traceability?	Ensure legal and regulatory compliance.	- Compliance Rate. - Audit Frequency.
Real-Time Collaboration & Response	Enable rapid threat response.	- EWS for automated alerts. - Slack, Teams for real-time communication.	- How can stakeholders effectively coordinate during a cyber incident? - What tools or workflows enable real-time threat sharing and response?	Facilitate timely and coordinated actions.	- Response Time. - Incident Coordination Success.
Continuous Learning & Improvement	Promote process enhancement.	- Post-incident reviews - Training programs through DYNAMO.	- How are lessons learned from incidents integrated into future CTI sharing processes? - What mechanisms are in place to gather feedback and improve practices?	Ensure continuous improvement.	- Incident Review Rate. - Training Participation Rate.

7. Discussion

The CTI Exchange Governance Model, grounded in its five pillars, addresses critical challenges in sharing cyber threat intelligence across diverse sectors. It not only establishes governance principles such as collaboration, standardization, and compliance but also operationalizes them into actionable processes through the DYNAMO platform. This dual approach ensures the model is both theoretically sound and practically viable. By focusing on Collaboration and Trust, the model tackles the long-standing issue of stakeholder reluctance in sharing sensitive data. Mechanisms such as ISACs, NDAs, and MOUs foster secure partnerships, while public-private collaboration strengthens mutual confidence. These strategies align with ENISA's recommendations for cross-sectoral coordination, demonstrating the model's adaptability. The emphasis on Data Sensitivity and Standardization ensures CTI exchanges are interoperable and actionable. The integration of STIX/TAXII

standards, combined with tools like DYNAMO's Data Anonymization Tool, addresses interoperability gaps while maintaining data privacy. This standardization is critical for real-time, cross-sectoral threat sharing, especially in regulated environments like healthcare and energy. Real-time collaboration is further enhanced by the Early Warning System (EWS), which automates threat alerts and facilitates immediate stakeholder coordination. This feature is particularly relevant for critical sectors such as maritime, where timely responses to threats like AIS spoofing can prevent cascading disruptions.

However, the model also faces notable challenges. Smaller organizations may lack the resources to keep up with advanced tools like EWS or conduct regular compliance audits, creating disparities in adoption. Additionally, building and sustaining trust among stakeholders, particularly between private entities and government bodies, requires persistent effort. These challenges highlight the importance of iterative refinement through pilot testing and stakeholder feedback. Maintaining engagement in such iterative processes often depends on clear benefits for participants, such as improved threat detection, strengthened regulatory compliance, and operational security gains. DYNAMO efforts to build resilience and business continuity through its platform is already a great incentive for the critical business sectors to adapt the information sharing mechanisms, however, a more detailed discussion on funding models or incentives for stakeholder commitment over time would be beneficial. Potential models include public-private partnerships, government grants, or industry-led funding mechanisms to support continued engagement. The availability of DYNAMO tools eliminates the need for organizations to develop proprietary CTI-sharing solutions, making participation in the governance model more feasible.

To assess the real-world impact of the governance model, the Key Performance Indicators (KPIs) outlined in Section 6's operationalization framework should be referenced. These KPIs cover aspects such as collaboration frequency, compliance adherence, incident response efficiency, and continuous improvement. By systematically measuring these indicators, organizations can track the effectiveness of CTI exchange and identify areas for iterative refinement. Additionally, comparative analytics can be utilized to assess the differences between organizations that adopt the governance framework and those that do not, providing deeper insights into the model's impact.

The governance model's flexibility presents significant expansion opportunities. Future integration of AI-driven threat detection could further automate processes like anomaly detection and metadata enrichment, making CTI sharing more efficient.

8. Conclusion

The proposed CTI Exchange Governance Model operationalized through the DYNAMO platform provides a robust and structured solution to streamline cyber threat intelligence sharing. By addressing key barriers such as interoperability, trust, and regulatory compliance, the model enhances collaboration and strengthens cyber resilience across critical infrastructure sectors.

The model's sector-specific adaptations ensure its relevance to unique operational and regulatory needs in healthcare, energy, and maritime domains. Its emphasis on real-time collaboration and continuous improvement equips stakeholders with the tools and processes necessary to respond proactively to evolving cyber threats.

While challenges such as resource disparities and stakeholder engagement persist, the model's scalability and adaptability position it as a significant step forward in CTI exchange governance. Future research should focus on refining tools, incorporating AI capabilities, and expanding the model to additional sectors to further enhance its impact. Since the DYNAMO Platform already leverages AI technologies in various aspects of CTI regeneration, expanding their role in CTI exchange could further enhance efficiency, accuracy, and interoperability. One key application would be the automation of compliance checks, ensuring that shared intelligence adheres to regulatory requirements. Additionally, AI and ML play a crucial role in optimizing CTI exchange by classifying and tagging intelligence for seamless sharing, correlating threat indicators from diverse sources, and detecting anomalies that may indicate misinformation or data integrity issues.

In summary, the governance model and its operational framework offer a practical, actionable approach to improving CTI exchange, ensuring that organizations are better equipped to mitigate risks and safeguard critical infrastructure in an increasingly interconnected world.

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

Alaeifar, Poopak & Pal, Shantanu & Jadidi, Zahra & Hussain, Mukhtar & Foo, Ernest. (2024). Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. Journal of Information Security and Applications. 83. 103786. https://doi.org/10.1016/j.jisa.2024.103786.

Cha, J., Singh, S., Pan, Y., & Park, J. (2020). Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing. Sustainability. https://doi.org/10.3390/su12166401

Dandurand, Luc & Serrano, O.S. (2013). Towards improved cyber security information sharing. 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, 2013, pp. 1-16. Available at: https://ccdcoe.org/uploads/2018/10/25_d3r1s5_dandurand.pdf

Du, Lili & Fan, Yaqin & Zhang, Lvyang & Wang, Lianying & Sun, Tianhang. (2020). A Summary of the Development of Cyber Security Threat Intelligence Sharing. International Journal of Digital Crime and Forensics. 12. 54-67. 10.4018/IJDCF.2020100105.

ENISA. (2017) Information Sharing and Analysis Centers (ICACs) Cooperative models. Available at: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

ENISA. (2018). Public Private Partnership (PPP) Cooperative models. Available at: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

Gong, N. (2018). Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study. Advances in Intelligent Systems and Computing. https://doi.org/10.1007/978-3-030-01177-2_49.

Jin, Beomjin & Kim, Eunsoo & Lee, Hyunwoo & Bertino, Elisa & Kim, Doowon & Kim, Hyoungshick. (2024). Sharing cyber threat intelligence: Does it really help? 10.14722/ndss.2024.24228. Available at: https://www.ndss-symposium.org/wp-content/uploads/2024-228-paper.pdf

Keyamo, C. . A., Attoh, O. M., EDUN, O. P., Adeoye, A. E., Ashioba, N. C., & Yoro, R. E. (2024). Cyber Threat Intelligence Sharing: A Review of Concepts, Platforms, and Legal Considerations. Faculty of Natural and Applied Sciences Journal of Computing and Applications, 2(1), 58–65. Retrieved from https://fnasjournals.com/index.php/FNAS-JCA/article/view/499

NIST. (2012). NIST SP 800-61: Computer Security Incident Handling Guide. Available at: https://doi.org/10.6028/NIST.SP.800-61r2

NIST. (2016). NIST SP 800-150: Guide to Cyber Threat Information Sharing. Retrieved from https://csrc.nist.gov.

Ofoegbu, K., Osundare, O., Ike, C., Fakeyede, O., & Ige, A. (2023). Data-Driven Cyber Threat Intelligence: Leveraging Behavioral Analytics for Proactive Defense Mechanisms. Computer Science & IT Research Journal. https://doi.org/10.51594/csitrj.v4i3.1501.

Pahlevan M, Ionita V. Secure and Efficient Exchange of Threat Information Using Blockchain Technology. Information. 2022; 13(10):463. https://doi.org/10.3390/info13100463

Saeed, S., Suayyid, S., Al-Ghamdi, M., Al-Muhaisen, H., & Almuhaideb, A. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors (Basel, Switzerland), 23. https://doi.org/10.3390/s23167273

Santoso, Putri Ayu. (2024). The Role of Threat Intelligence Sharing in Strengthening Collective Cyber Defense Across Organizations. (2024). Global Research Perspectives on Cybersecurity Governance, Policy, and Management, 8(12), 24-33. https://hammingate.com/index.php/GRPCGPM/article/view/3

Susha, I., Rukanova, B., Zuiderwijk, A., Gil-Garcia, J.R., & Gasco Hernandez, M. (2023). Achieving voluntary data sharing in cross-sector partnerships: Three partnership models. Information and Organization, 33, 100448. DOI: https://doi.org/10.1016/j.infoandorg.2023.100448.