Implementing CTI Exchange: A Framework for the DYNAMO Project Pilot Phase

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

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

Abstract: Effective Cyber Threat Intelligence (CTI) exchange is essential for strengthening cybersecurity resilience across critical sectors such as healthcare, energy, and maritime. While theoretical CTI governance models exist, their real-world implementation remains challenging due to issues with trust, compliance, interoperability, and real-time collaboration. This paper aims to address these challenges by proposing a practical knowledge transfer framework for the pilot phase of CTI Exchange governance implementation. Building on two prior research studies that developed a CTI exchange governance model specifically tailored for the DYNAMO platform, this paper focuses on putting that model into practice. By utilizing the insights and methodologies from previous work, the study presents a structured approach to applying, testing, and refining governance principles in real-world settings, ensuring effective operationalization of the model through the DYNAMO platform's capabilities. The DYNAMO project, an EU initiative, offers a comprehensive approach to cyber resilience and business continuity, providing organizations with tools and strategies for threat intelligence generation, analysis, and dissemination. The proposed framework includes strategies for piloting DYNAMO tools with pilot preparation, stakeholder engagement, sector-specific governance adaptations, and evaluation metrics. It also defines clear roles and responsibilities to support consistent application of governance mechanisms, with continuous refinement based on empirical feedback. The framework also emphasizes the importance of cross-sector collaboration, ensuring that various stakeholders, including governmental bodies, private organizations, and technical experts, are actively involved throughout the process. Tailored guidelines for the healthcare, energy, and maritime sectors address sector-specific regulatory and operational challenges. Although the pilot phase has not yet been executed, the guidelines presented here provide a robust roadmap for preparing, launching, and iteratively refining CTI exchange pilots. Ultimately, this work lays the foundation for scalable, secure, and compliant CTI-sharing governance that enhances collaboration and cyber resilience across critical infrastructure environments.

Keywords: Cyber threat intelligence, CTI exchange, Governance model, Knowledge Transfer, DYNAMO Project, Piloting

1. Introduction

Cyber Threat Intelligence (CTI) plays a pivotal role in organizational cyber resilience by enabling stakeholders to proactively identify and address threats, learn from past incidents, and anticipate future risks (Johnson et al., 2016). The importance of real-time CTI sharing is especially pronounced in multi-organization contexts, timely exchange of threat insights allows partners to coordinate responses and contain incidents more effectively (CISA, 2023). Within the DYNAMO project (an EU-funded cyber resilience initiative)[1] , the need for rapid and secure CTI sharing among partners is critical to support a shared situational awareness and synchronized defense across healthcare, energy, and maritime sectors.

However, practical challenges related to governance, including legal compliance, mutual trust, data sensitivity, and technological interoperability, often hinder seamless intelligence exchange (Rajamäki & Nepal, 2025, Fan et. al., 2019). These governance issues can create reluctance in sharing information and limit the benefits of collective cyber defense (ENISA, 2017). DYNAMO has developed a suite of cybersecurity tools that support proactive threat detection, analysis, and incident response across critical infrastructure sectors such as health, maritime and energy . CTI exchange mechanisms are central in this toolset, ensuring that actionable intelligence (e.g. indicators of compromise, TTPs, and warnings) is disseminated securely among stakeholders. To fully leverage DYNAMO's capabilities, a structured governance framework is required so that these CTI-sharing tools can be integrated in practice. Effective governance would provide common standards (such as using STIX/TAXII for threat data format) and policies (e.g. defining trust groups and data handling rules) that enable organizations to share intelligence confidently and in compliance with regulations (Johnson et al., 2016). In essence, governance acts as the key element that drive the technical CTI platform with the participating organizations'

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

processes and regulatory obligations, facilitating a smooth operationalization of cross-sector threat intelligence sharing (Rajamäki et al., 2025).

Recognizing these needs, prior studies have explored what kind of governance model best suits the DYNAMO platform's CTI exchange requirements. For example, Rajamäki et. al., (2025) developed a tailored CTI exchange governance model emphasizing trust agreements, standardized data formats, regulatory compliance, real-time collaboration, and continuous learning.

This paper builds on such groundwork by moving from theory to practice. Specifically, we extend the earlier conceptual model into a pilot implementation framework for DYNAMO's tools, with a strong focus on CTI exchange. In doing so, this study addresses the gap between high-level governance principles and their application in real-world settings, aiming to support that the DYNAMO platform's CTI sharing capabilities are adopted and utilized effectively across its partner organizations.

1.1 Research gap and Objectives

While various governance models for CTI exchange exist, many lack concrete implementation guidelines that can be directly applied in structured pilot programs or real operational environments (Rajamäki & Nepal, 2025) . In other words, prior frameworks often stop at the policy level and do not provide detailed roadmaps for how to put governance principles into action within organizations or multi-party consortia. This gap is evident in critical sectors where generic cybersecurity frameworks (e.g., NIST's Risk Management Framework or ENISA guidelines) offer foundational guidance but may not account for sector-specific challenges and the nuances of inter-organizational collaboration (Rajamäki & Nepal, 2025). There is a clear need for a practical approach that translates governance theory into actionable steps for pilots, ensuring that well-intended policies yield improved information-sharing outcomes on the ground.

Objectives: This paper aims to bridge the above gap by developing a practical, sector-specific implementation framework for governance-driven CTI exchange. Key objectives include:

- Develop a comprehensive implementation framework for governance-driven CTI exchange.
- Provide structured guidelines for piloting CTI governance using the DYNAMO platform across critical sectors.
- Ensure that the piloting framework supports both CTI exchange governance and the broader implementation of DYNAMO tools.
- Outline knowledge transfer approaches for adoption, evaluation, and iterative refinement.

1.2 Research Methodologies

This study is based on a qualitative and exploratory approach aimed at developing a practical framework for piloting CTI exchange governance within the DYNAMO project. The methodology involves four key steps:

1. **Building on previous research:** The work draws directly from earlier studies that developed a CTI governance model specifically for the DYNAMO platform. These prior efforts provided conceptual foundations, including the governance pillars and key considerations for secure and effective CTI exchange.
2. **Understanding DYNAMO requirements:** We reviewed the goals, structure, and planned deliverables of the DYNAMO project to support alignment with its technical and strategic needs. This included identifying how CTI sharing tools are expected to function in practice and what governance components are necessary to support them.
3. **Reviewing existing literature and supporting documents:** A literature review was conducted focusing on CTI exchange, governance challenges, and knowledge transfer in cybersecurity contexts. The literature included target keyword searches using mostly google scholar and used keywords such as "Cyber Threat Intelligence governance", "CTI exchange", "cybersecurity knowledge transfer", "knowledge transfer", among others. Literature was selected based on relevance to CTI governance implementation from peer-reviewed articles, conference proceedings, white papers, and institutional reports. In addition, reference materials were sourced from authoritative organizations including CISA, NIST, and ENISA. Findings were thematically categorized and synthesized to design the pilot preparation strategies.
4. **Drawing insights from related pilot projects:** We analyzed example pilot initiatives to understand how governance models have been applied and evaluated in similar multi-stakeholder, critical

infrastructure settings. These cases offered practical insights into piloting strategies, stakeholder engagement, and adaptation across sectors.

This methodology supports that the proposed pilot framework is both grounded in research and tailored to the operational context of the DYNAMO platform and its partner sectors.

1.3 Structure of Paper

The following sections 2 and 3 introduce DYNAMO Platform and related work respectively. Section 4 describes the role of governance in DYNAMO piloting followed by piloting strategies in section 5. Sections 6 and 7 provide an overview of sector-wise CTI governance adaptation and KPIs respectively. The final two sections are discussion and conclusion.

2. The DYNAMO Platform

DYNAMO is a European Union initiative designed to enhance cyber resilience in critical infrastructure sectors such as healthcare, energy, and maritime. The project integrates advanced cybersecurity tools to support proactive threat intelligence exchange and response coordination. By fostering collaboration among experts and stakeholders, DYNAMO supports that organizations can effectively counter evolving cyber threats while maintaining compliance with industry regulations.

DYNAMO emphasizes a structured resilience cycle encompassing preparation, prevention, protection, response, recovery, and continuous adaptation. Sector-specific risk scenarios are developed to simulate cyber-attack impacts and refine strategies to combat the cyber defenses with collaboration, development of advanced tools and CTI-sharing mechanisms. The project considers three key perspectives:

- **Technology perspective** – Development and optimization of cybersecurity tools to enhance threat detection and mitigation.
- **Data perspective** – Analysis of gathered data, ensuring relevant, actionable intelligence for stakeholders.
- **Social perspective** – Establishment of governance policies and trust-building measures for secure and effective collaboration.

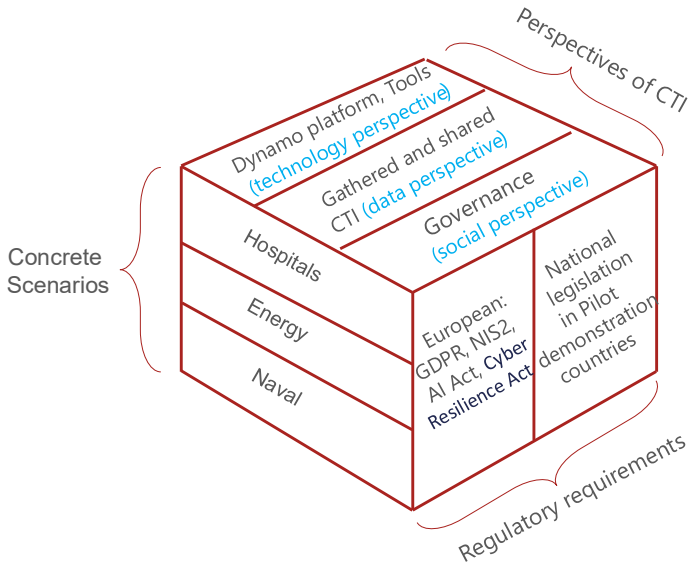

Figure 1: DYNAMO CTI perspective, regulatory requirements and use cases

By offering tailored security strategies, DYNAMO mitigates threats such as ransomware in healthcare, SCADA vulnerabilities in energy infrastructure, and navigation system compromises in the maritime sector. The platform's integrated approach enables organizations to build robust defense mechanisms against cyber risks.

3. Related Work

3.1 CTI Exchange, Governance and Existing Implementation Examples

Several prior works have laid the foundation for understanding CTI, its exchange mechanisms, and the governance challenges that accompany them. Johnson et al. (2016) provided a framework for understanding the benefits and limitations of CTI sharing, emphasizing the importance of structured information formats and trust-based networks. Jin et al. (2024) revisited these themes, empirically testing CTI sharing outcomes and highlighting the importance of CTI exchange in a standard manner emphasizing on technical standards like STIX and TAXII have been instrumental in supporting automated CTI exchange. These are further supported by platforms like MISP, an open-source tool explored by Wagner et al. (2016), which offers structured environments for indicator sharing and collaborative analysis. Furthermore, Saeed et al. (2023), who presented a systematic review of CTI practices in organizations and their alignment with resilience objectives and highlighted the importance of CTI implementation.

Despite these technological enablers, governance issues remain central. Rajamäki et al. (2024) addressed this through a proposed governance framework tailored for the DYNAMO CTI Tool, incorporating steering structures, role-based access, and legal alignment with the NIS2 directive. Their work is complemented by Rajamäki et. al., (2025), who refined the model into five governance pillars. The present paper builds directly on these foundations, translating their theoretical model into a pilot-ready framework.

In terms of implementation strategy, this study also draws on lessons from pilot projects like NIST Cybersecurity Framework (CSF) Pilot at Intel (Casey, 2015) and C3ISP (Fan et al., 2019), which demonstrated how piloting in critical infrastructure contexts can identify sector-specific governance requirements. Together, these works underscore the need for practical frameworks that not only outline governance principles but support their staged adoption in diverse operational settings.

3.2 Knowledge Transfer in DYNAMO Context

In the context of this study, knowledge transfer refers to the process of taking previous theoretical work and applying it in a practical setting. Many literatures on knowledge transfer focus on transfer of knowledge between researcher and practitioner (Ward et. al., 2009), inter organizational unit transfer of knowledge (Argote et. al., 2000) and transferring knowledge among employees to build the security posture of an organization (Saad, 2021). However, for the DYNAMO project, it involves translating the governance model introduced in earlier research (Rajamäki et. al., 2025) into a pilot framework that can be tested and implemented with real stakeholders. This governance model, which is structured around trust and collaboration, standardization, regulatory alignment, real-time response, and continuous improvement was developed conceptually, but has not yet been operationalized.

This pilot phase serves as a bridge between theory and practice. While the model outlines governance principles for CTI exchange, implementing it in real-world settings allows for validation, adaptation, and contextual refinement, which we believe are core aspects of effective knowledge transfer in DYNAMO context. Thus, in the DYNAMO pilot, knowledge transfer is not a passive step but a strategic phase of the research, transforming static governance models into practical, adaptable frameworks through stakeholder engagement, iteration, and hands-on experimentation.

4. Governance Model and its Role in Piloting

In the rapidly evolving landscape of cyber threat intelligence (CTI) exchange, establishing a robust governance model is crucial. This section discusses the theoretical governance model, its guiding role in pilot design, the conceptual CTI exchange governance framework for DYNAMO piloting, and the importance of piloting DYNAMO tools for governance validation.

4.1 Overview of the Theoretical Governance Model

Previous research established a governance model tailored to DYNAMO's CTI exchange needs(Rajamäki et. al. 2025). The governance model is structured around five key pillars:

- **Collaboration & trust** – Establishing formal agreements (NDAs, MOUs) to facilitate secure and confidential CTI exchange.
- **Data sensitivity & standardization** – Utilizing structured formats (STIX/TAXII) and anonymization tools for secure data handling.

- **Compliance & regulatory alignment** – Ensuring adherence to regulations (GDPR, HIPAA, NERC-CIP).
- **Real-time collaboration & response** – Implementing automated threat-sharing mechanisms.
- **Continuous learning & improvement** – Conducting periodic training and refinement based on empirical feedback.

4.2 How Governance Guides Pilot Design

Governance principles shape the pilot framework in several ways:

- **Pilot structure** – Governance defines how and what tools are introduced, who oversees the piloting, compliance, training, and how feedback is integrated, and so on.
- **Stakeholder engagement** – Governance mandates who the stakeholders are involved in pilots and their structured roles.
- **Evaluation metrics** – Governance-driven success criteria are set for measuring compliance, trust-building, and regulatory alignment.

This supports that governance is not just an afterthought but the foundation of pilot design, providing an adaptive framework that aligns with sector-specific requirements. The governance model outlined above provides the foundation for structured pilot implementation. By embedding compliance mechanisms, trust-building structures, and regulatory alignment protocols into the pilot, this framework supports that CTI-sharing policies are effectively tested in a controlled setting.

4.3 Conceptual CTI Exchange Governance Framework for DYNAMO Piloting

Figure 2 illustrates the Conceptual CTI Exchange Governance Framework within the DYNAMO Platform, presenting a hypothetical model of how cyber threat intelligence (CTI) exchange could be structured and governed in a pilot scenario. This conceptual framework supports that governance mechanisms, including data classification, sensitivity control, compliance, and risk management, are embedded into the CTI-sharing process to maintain security, regulatory compliance, and trust among participating critical infrastructure (CI) organizations.

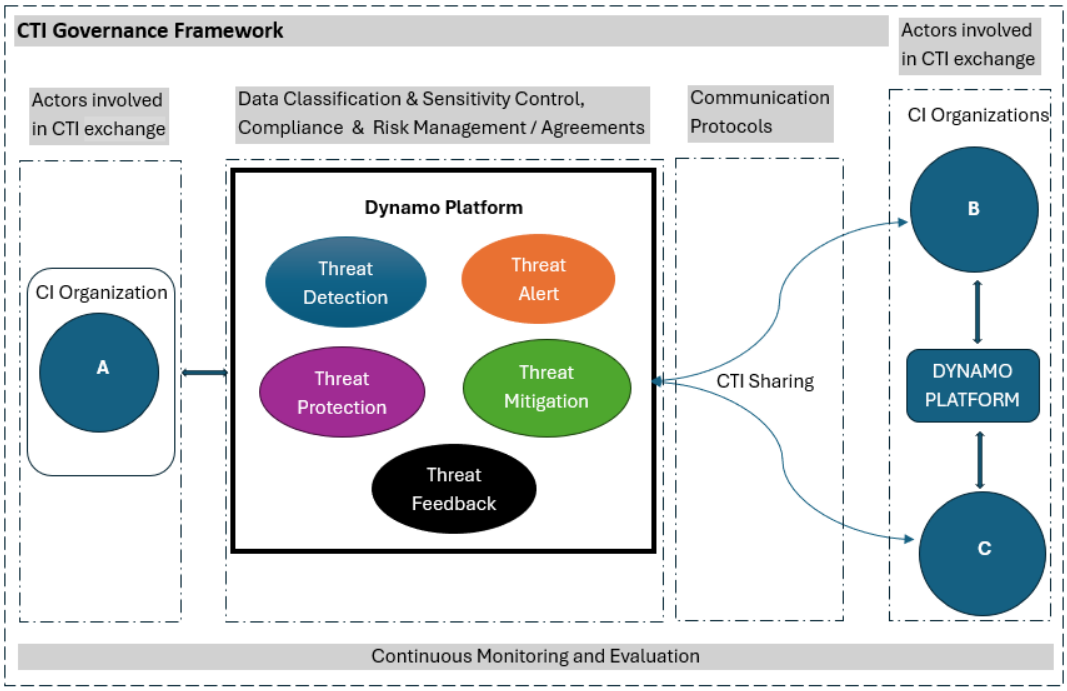

Figure 2: Graphical illustration of CTI sharing governance structure for DYNAMO partners within Single Critical Infrastructure Sector

The components illustrated in Figure 2—Threat Detection, Alert, Protection, Mitigation, and Feedback—represent the core technical functions of the DYNAMO platform. Each of these corresponds to one or more of the five governance pillars (Section 4.1), supporting that CTI-sharing mechanisms are secure, compliant, and adaptable. Furthermore, these components are deployed progressively across the phases of implementation

described in Table 1, for instance, Detection and Alert mechanisms activated during preparation, Protection and Mitigation during execution, and Feedback driving iterative refinement in the final phase.

4.4 Why Piloting DYNAMO tools is key to Governance Validation

DYNAMO tools act as a practical testbed for applying governance principles. This includes:

- Testing governance policies in real-world CTI exchange scenarios.
- Ensuring that DYNAMO's technical capabilities align with governance requirements.
- Validating compliance mechanisms across sectors.

Unlike a standard technical pilot, this pilot measures how well governance models integrate into tool deployment, ensuring that governance-driven insights are applied across industries.

5. Pilot Preparation Strategies and Stakeholder Engagement

This section discusses defining the pilot scope, governance role assignments in the pilot, and stakeholder engagement models. The first subsection explores how the scope of the pilot is defined and delineated. The second subsection focuses on the assignment of governance roles and their importance for the success of the pilot. The third subsection examines stakeholder engagement models and their role in the implementation of the pilot.

5.1 Defining the Pilot Scope

To ensure a comprehensive and effective pilot, it is essential to clearly define the scope, including setting objectives, selecting relevant sectors, and aligning with DYNAMO's capabilities:

- Objective Setting: Define piloting goals and expected outcomes.
- Sector Selection: Justification for piloting in healthcare, energy, and maritime sectors.
- Alignment with DYNAMO Capabilities: How DYNAMO's tools support governance testing.

Table 1 illustrates how the pilot can be conducted in phases.

Table 1: Phased Implementation of the pilot

Phase	Duration	Activities
Preparation Phase	Month xx-xx	Define governance policies, onboard stakeholders, and establish compliance frameworks.
Execution Phase	Month xx-xx	Deploy CTI-sharing governance protocols, monitor compliance, and evaluate interoperability.
Evaluation & Refinement Phase	Month xx-xx	Assess governance adoption, conduct feedback loops, and refine policies based on stakeholder input.

5.2 Governance Role Assignments in Pilot

The Platform Administrator (DYNAMO Central Team) is responsible for technical oversight and platform management, ensuring seamless operation and continuous availability of the platform. Sector-Specific Governance Leads tailor policies to meet the unique requirements of each sector and ensure compliance with relevant regulations. Inter-Organizational Liaison Officers facilitate smooth coordination and communication between different organizations, playing a crucial role in maintaining up-to-date information and seamless collaboration. Compliance and Risk Managers monitor adherence to regulations and report on compliance, ensuring all activities are conducted in accordance with established rules and identifying and managing potential risks. The Monitoring and Evaluation Team collects and analyzes data to refine the governance model, using the gathered information for continuous improvement and enhancement of governance practices. These roles and their responsibilities are summarized in Table 2 and align with the respective phases in Table 1 to ensure a structured implementation.

Table 2: Key pilot roles and responsibilities

Role	**Responsibilities**
Platform Administrator (DYNAMO Central Team)	Technical oversight and platform management.

Role	Responsibilities
Sector-Specific Governance Leads	Tailoring policies per sector and ensuring compliance.
Inter-Organizational Liaison Officers	Ensuring smooth coordination and communication.
Compliance and Risk Managers	Monitoring adherence to regulations and reporting compliance.
Monitoring and Evaluation Team	Collecting and analyzing data for governance refinement.

5.3 Stakeholder Engagement Models

Stakeholder engagement is a critical component for the DYNAMO pilot, to support the fact that governance-driven CTI exchange mechanisms are tested under real-world environment. Effective engagement fosters trust, compliance, and interoperability between public and private sector entities, regulatory bodies, and cybersecurity experts (CISA, 2024). Figure 3 illustrates the Stakeholder Engagement Model, which highlights the essential elements required to establish a structured, inclusive, and collaborative CTI exchange environment. These stakeholder roles are engaged across the phases in Table 1, from preparation to refinement.

The modules shown in Figure 3 mean the following:

- **Identifying Key Stakeholders** – Ensuring participation from sector-specific organizations (Healthcare, Energy, Maritime), regulatory bodies, and cybersecurity experts who will contribute during the pilot and CTI exchange implementation.
- **Building Trust and Collaboration** – Establishing formal agreements (MOUs, NDAs) and fostering Public-Private Partnerships (PPPs) to create a reliable governance environment.
- **Continuous Communication** – Enabling structured feedback loops, communication channels, and reporting mechanisms that support transparency, policy refinement, and stakeholder coordination.

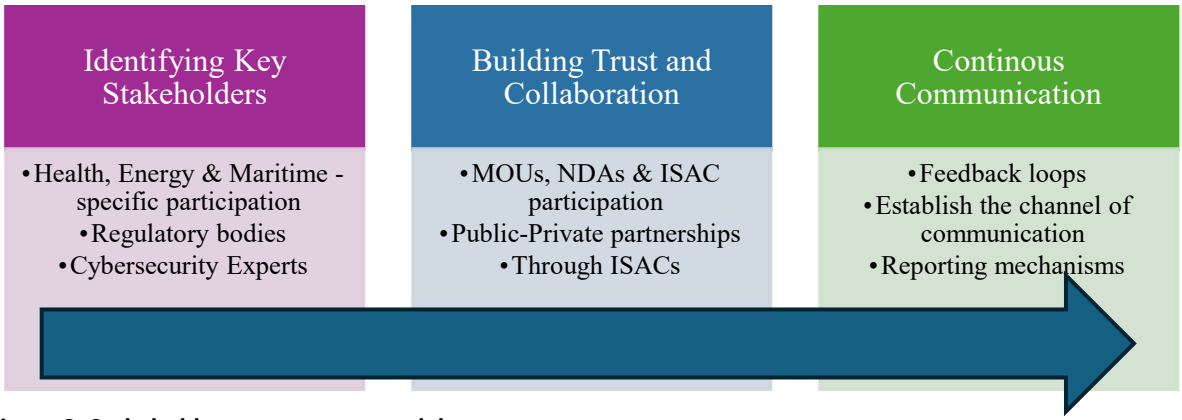

Figure 3: Stakeholder engagement model

Stakeholder engagement within the pilot also facilitates knowledge transfer, ensuring that governance policies are not only tested but also actively refined based on sector-specific insights. By documenting governance interactions, challenges, and best practices, the pilot supports a continuous learning cycle that strengthens governance adoption across different critical infrastructure sectors. This engagement model supports stakeholders actively contribute to governance policy formation, enabling a resilient, well-integrated, and governance-compliant CTI exchange framework.

6. Sector-Specific CTI Governance Adaptations

During the pilot, each critical infrastructure sector requires tailored governance mechanisms to address sector-specific operational challenges, regulatory constraints, and cybersecurity threat landscapes. Effective CTI exchange must accommodate these variations to support the threat intelligence sharing is secure, efficient, and compliant with sector-specific policies. The governance adaptations for each sector reflect the distinct threat environments and organizational structures that impact CTI exchange. Table 3 outlines governance adaptations for key critical infrastructure sectors.

Table 3: Governance adaptations for critical infrastructure sectors

Sector	Key Actors	Threat Vectors	Governance Elements
Energy	SCADA Engineers, IT & OT Security Teams, Regulatory Bodies	SCADA malware, DDoS attacks, phishing campaigns	Compliance such as NERC-CIP , emergency response protocols, SCADA data protection
Healthcare	IT Security Teams, Medical Device Manufacturers, Data Privacy Officers	Ransomware, phishing, medical device vulnerabilities	HIPAA compliance, data anonymization, ISAC partnerships
Maritime	Port Authorities, Coast Guard, Shipping Companies	GPS jamming, AIS spoofing, cyberattacks on navigation	IMO cybersecurity compliance, secure vessel communication, data-sharing agreements

By recognizing these sector-specific needs, the proposed governance-driven pilot ensures that CTI exchange is not a one-size-fits-all approach but a flexible model that can be adapted based on each sector's challenges and requirements. This sectoral governance alignment improves the effectiveness and reliability of cyber threat intelligence sharing, strengthening overall cybersecurity resilience.

7. Evaluation Metrics and Refinement Process

To evaluate the effectiveness of the governance-driven pilot, it is essential to define a set of measurable indicators. These metrics support that governance principles are properly integrated into CTI exchange and allow for continuous refinement of the governance model. Table 4 presents the key evaluation metrics that have been identified.

Table 4: Identified key evaluation metrics

Metric	Example
Governance Adoption Rate	If 8 out of 10 organizations implement CTI-sharing policies, adoption is high.
CTI Sharing Effectiveness	If a simulated threat alert is shared within 3 minutes instead of 5, effectiveness is high.
Regulatory Compliance Score	Full compliance with audit results indicates strong governance adherence.
Incident Coordination Success	If an incident response occurs within the predefined time frame while adhering to governance-defined escalation protocols and data-sharing restrictions, coordination is effective.
Stakeholder Trust Index	If 85% of participants express confidence in CTI sharing procedures, trust is strong.

7.1 Refinement Process

The pilot implementation must be continuously refined based on the evaluation metrics outlined above. A structured feedback loop will be established to capture insights from pilot participants, regulatory bodies, and technical evaluators. The refinement process includes:

- Data Collection and Monitoring – Regular assessment of governance adoption, stakeholder engagement, and technical interoperability.
- Stakeholder Feedback Analysis – Identifying operational challenges, legal concerns, and usability issues in CTI-sharing governance.
- Governance Policy Adjustments – Refining governance mechanisms based on pilot findings, ensuring compliance with regulatory standards and industry best practices.
- Technical Enhancements – Improving automation of CTI-sharing workflows, streamlining compliance enforcement, and enhancing threat intelligence dissemination.
- Final Pilot Assessment – A comprehensive evaluation after the pilot phase to validate governance model effectiveness and identify areas for further improvement before wider implementation.

By systematically applying these evaluation metrics and refining governance models accordingly, the pilot support that CTI exchange remains secure, compliant, and scalable across different sectors.

8. Discussion

As this paper presents a proposed framework rather than an executed pilot, the discussion focuses on the anticipated challenges, expected benefits, and strategic importance of governance-driven CTI exchange implementation. A governance-driven pilot is essential to bridge the gap between theoretical governance models and real-world application. The governance-driven pilot serves as a controlled environment where governance principles can be assessed, refined, and validated before broader implementation. Unlike a traditional technical pilot, this approach ensures that compliance, trust, and collaboration mechanisms are tested in real-world settings to enhance policy effectiveness. By piloting CTI exchange within the DYNAMO project, organizations can better understand how governance mechanisms operate in practice, allowing for incremental refinement. The key advantage of this approach is that it supports compliance with regulatory requirements while fostering trust and interoperability among stakeholders.

However, implementing such a pilot is not without challenges. A major concern is organizational resistance to information sharing, often due to security risks, liability concerns, and a lack of trust in third-party entities. The key challenge would be to bring the organizations to participate in the piloting activities. Additionally, ensuring regulatory compliance across different jurisdictions poses complexities, as data protection laws vary significantly between sectors and regions. Another challenge is technical integration, where participating organizations may have differing levels of CTI-sharing capabilities, leading to interoperability issues.

Despite these obstacles, the proposed framework provides a structured approach to piloting governance principles in CTI exchange. By defining clear stakeholder roles, establishing sector-specific governance adaptations, and setting evaluation metrics, the pilot will allow stakeholders to assess governance adoption in a controlled environment before full-scale implementation. The inclusion of evaluation mechanisms supports that governance effectiveness can be measured, making it possible to refine governance policies iteratively.

Beyond governance validation, the pilot serves as a structured mechanism for knowledge transfer. Lessons learned from CTI-sharing policies, regulatory compliance challenges, and stakeholder collaboration will inform future iterations of governance models. By ensuring that pilot outcomes are systematically documented and shared, this approach enhances the scalability and long-term effectiveness of governance-driven CTI exchange frameworks.

The key outcome of this governance-driven pilot is expected to be an empirically validated framework that enables scalable and secure CTI exchange. Future research will be required to validate this framework in practice, identify any unforeseen challenges, and refine governance mechanisms based on pilot results. Ultimately, this framework serves as a foundation for long-term cybersecurity resilience across critical infrastructure sectors.

9. Conclusion and Future Directions

This paper presents a governance-driven pilot framework for CTI exchange within the DYNAMO project. By aligning governance models with practical tool deployment, the pilot supports compliance, security, and sector-specific adaptation. The proposed framework offers a structured approach to integrating governance principles into CTI exchange, facilitating improved collaboration across industries.

Future work should focus on expanding governance piloting to additional sectors to test scalability. Incorporating AI-driven compliance monitoring to automate governance enforcement is also essential. Additionally, conducting empirical validation through real-world CTI exchange pilot programs will provide valuable insights. Strengthening trust-building mechanisms is crucial to encourage broader participation in CTI sharing.

By ensuring governance remains the foundation of pilot testing, this work lays the groundwork for scalable, secure, and compliant CTI exchange frameworks. The insights gained will help refine governance models, optimize threat intelligence collaboration, and strengthen cyber resilience across multiple industries. As the cybersecurity landscape evolves, continuous refinement of governance principles will be necessary to address emerging challenges and support sustained effectiveness in CTI exchange.

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.

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: AI models have been used to summarize and extract insights from literature, as well as to correct language and grammar.

References

Argote, L., Ingram, P., Levine, J.M. and Moreland, R.L., 2000. Knowledge transfer in organizations: Learning from the experience of others. Organizational Behavior and Human Decision Processes, 82(1), pp.1–8. Available at: https://doi.org/10.1006/obhd.2000.2883

Casey, T., 2015. The Cybersecurity Framework in Action: An Intel Use Case. Intel Corporation. Available at: https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf

CISA, 2023. Information Sharing. Available at: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing

CISA, 2024. Partnerships and collaboration. [online] Available at: https://www.cisa.gov/topics/partnerships-and-collaboration

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

Fan, W., Dragoni, N., Massacci, F. and Smeraldi, F., 2019. Enabling privacy-preserving sharing of cyber threat information in the cloud. In: 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud) / 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). Paris, France, pp.74–80. Available at: https://doi.org/10.1109/CSCloud/EdgeCom.2019.00-15

Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D. and Kim, H., 2024. Sharing cyber threat intelligence: Does it really help? Network and Distributed System Security Symposium (NDSS). Available at: https://www.ndss-symposium.org/wp-content/uploads/2024-228-paper.pdf

Johnson, C., Badger, L., Waltermire, D., Snyder, J. and Skorupka, C., 2016. Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. Available at: https://doi.org/10.6028/NIST.SP.800-150

Rajamäki, J., Feyesa, A. and Nepal, A., 2024. E-EWS-based governance framework for sharing cyber threat intelligence in the energy sector. In: Proceedings of the 23rd European Conference on Cyber Warfare and Security. Available at: https://doi.org/10.34190/eccws.23.1.2073

Rajamäki, J. and Nepal, A., 2025. Governance for Cyber Threat Intelligence (CTI) exchange across the DYNAMO resilience cycle. In: Proceedings of the 20th International Conference on Cyber Warfare and Security (ICCWS 2025). Available at: https://doi.org/10.34190/iccws.20.1.3208

Rajamäki, J., Nepal, A. and Chalkias, I., 2025. Enhancing Cyber Threat Intelligence (CTI) exchange: A governance model for the DYNAMO platform. ECCWS 2025. In press.

Saad, A., 2021. A model for describing and encouraging cyber security knowledge sharing to enhance awareness. PhD thesis. University of Glasgow. Available at: https://theses.gla.ac.uk/82647/

Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H. and Almuhaideb, A.M., 2023. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), p.7273. Available at: https://www.mdpi.com/1424-8220/23/16/7273

Wagner, C., Dulaunoy, A., Wagener, G. and Iklody, A., 2016. MISP: The design and implementation of a collaborative threat intelligence sharing platform. In: Proceedings of the ACM Workshop on Information Sharing and Collaborative Security (WISCS). Available at: https://doi.org/10.1145/2994539.2994542

Ward, V., House, A. and Hamer, S., 2009. Developing a framework for transferring knowledge into action: A thematic analysis of the literature. Journal of Health Services Research & Policy, 14(3), pp.156–164. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2933505/