E-EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector

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

Jyri.Rajamaki@laurea.fi
Asfaw.Feyesa@student.laurea.fi
Anup.Nepal@student.laurea.fi

Abstract: The integration of traditional energy technologies with modern digital technologies increases the risks of cyber-attacks and data breaches. Sharing cyber threat intelligence (CTI) is important for the common defense. The DYNAMO project has chosen the ECHO Early Warning System (E-EWS) as a tool for CTI information sharing. The management of E-EWS becomes the basis for guiding the ethical and efficient operation of the DYNAMO platform and the wider energy sector. The governance framework defines roles, responsibilities, and procedures that are tailored to sharing information, enhancing collaboration, and ensuring the integrity of shared information. Effective governance promotes transparency, compliance, and trust among stakeholders, which ultimately strengthens the security posture of the DYNAMO platform and improves the energy industry's resilience against cyber threats. This paper proposes a governance framework for the DYNAMO platform, including a committee, data security policies, and NIS2 and GDPR compliance. It emphasizes user-friendly collaboration tools, access control, continuous monitoring, stakeholder training, compliance, and phased implementation. The goal is iterative improvements through continuous evaluation.

Keywords: Governance Framework, Cyber Security, Cyber Threat Intelligence, DYNAMO Project, Energy Sector, Information Sharing

1. Introduction

The production and utilization of renewable energy in buildings has been a popular topic for decades, and it is still an important part of future sustainable urban energy systems (Braeuer, et al., 2022). To operate energy-efficiently, it needs digitization. The integration of digital technologies in the energy sector presents both opportunities and challenges. Advanced technologies such as artificial intelligence, machine learning, internet of things, and blockchain are employed to enhance operational efficiency (Yadoshchuk, 2023). However, this digital transformation also exposes the sector to increased cyber threats, particularly targeting critical infrastructure essential for business continuity management (BCM) and information security (Marc & Aloys, 2023). Consequently, a collaborative and dynamic cybersecurity approach becomes imperative.

The DYNAMO project addresses this need by developing a platform for connecting BCM and Cyber Threat Intelligence (CTI), which focuses on promoting dynamic data collection, analysis, sharing, and collaboration between different stakeholders in critical sectors such as energy (Hytönen, et al., 2023). With its emphasis on "dynamic adaptation for mitigation and optimization," the project employs specific principles and structures to fortify the security and resilience of the energy sector. Central to the DYNAMO project is the practice of information sharing, where stakeholders and partners exchange data to collectively understand and preempt cyber threats. To ensure business continuity and the effective use of digital technology for customer service, the DYNAMO project leverages the ECHO Early Warning System (E-EWS) for collaborative efforts among stakeholders. However, the effectiveness and sustainability of these tools require a well-coordinated and organized approach. Therefore, the DYNAMO platform relies on Information Security Governance (ISG) as a key element. ISG, a strategic approach guiding information systems management (Nicho, 2018), provides oversight, accountability, and strategic direction. It defines roles, responsibilities, policies, and procedures for information sharing and collaboration within the DYNAMO framework, crucial for the long-term success and resilience of the project and the energy sector.

As the energy sector witnesses increased adoption of digital technology and cyber threats, there is a pressing need for a collaborative and organized effort to bolster cybersecurity. This work-in-progress paper proposes a governance framework supporting the E-EWS information-sharing strategy under the DYNAMO platform. The paper investigates the prospect of governance in implementing E-EWS in the energy sector within the DYNAMO platform and proposes a governance framework. The research question is “How do partners collaborate in EU projects, particularly in the context of CTI information sharing, and how does governance contribute to effective collaboration in this regard?” The hypothesis is that “governance is a crucial element for organizations to

function effectively, ethically, and legally, providing oversight, accountability, and strategic direction for the DYNAMO project and the energy sector".

The rest of the paper is organized as follows: after this introduction, section 2 examines different information-sharing tools based on the literature. Section 3 deals with an overview of the governance models of the information-sharing ecosystem. Section 4 analyzes the legislative and ethical environment for sharing cyber threat intelligence in the energy sector. Section 5 presents the E-EWS-based governance framework created based on previous analyses for sharing cyber threat information in the energy sector. Finally, Section 6 summarizes this study and suggests further steps.

2. Overview of Information-Sharing Tools

Today, information is a crucial commodity, and the strategic sharing of relevant information has become an invaluable resource. Effective information sharing is a crucial aspect of organizational data management. Without a robust data-sharing mechanism, operational capacity and decision-making processes may face disruptions. The chosen system for information sharing must be organization-wide compatible to prevent unnecessary transcription and rekeying of data when transferred between systems. Additionally, key requirements for information-sharing systems include easy accessibility and swift data retrieval. If required information is not readily available, it can lead to frustration and hinder overall organizational effectiveness (Gordon, 2013).

Information sharing can be categorized into internal and external components. Collaborative interactions within the workplace contribute to increased cooperation and enhanced work performance (Peters & Manz, 2007). Effective internal communication fosters inspiration, engagement, and productivity. However, selecting the appropriate internal communication system that aligns with the organization's culture can be challenging. Traditional methods like newsletters and emails may not be sufficient; instead, internal channels should be immediate, fast, targeted, measurable, and adaptable to mobile platforms. An organization's internal communication tools may include department-specific mailing lists or a comprehensive intranet for seamless information access. External information sharing can be facilitated through the organization's website or by creating a specific extranet for collaboration with external partners. Well-established communication channels play a vital role in stakeholder engagement and effective collaboration with end-users (Ruoslahti & Tikanmäki, 2019).

In the field of cyber security, the sharing of critical information among the entities of the ecosystem is key in combating cyber threats. Sharing cybersecurity information among different organizations is highly beneficial, improving threat response, defending against potential attackers, and mitigating damages. It also fosters better relations and trust between organizations. However, challenges may arise, including legal issues stemming from differing definitions of classified information protection across countries. Therefore, employing appropriate information-sharing models and frameworks is crucial to achieving efficient data sharing between organizations (Rajamäki & Katos, 2020). Especially, care must be taken in the sharing process, which requires careful consideration of the type of information shared and the recipients (Kokkonen, et al., 2016). Numerous open-source data-sharing tools are readily available in the market and organizations can utilize them based on their specific requirements. When implementing these sharing tools, several actors jointly decide on the nature and scope of the information to be exchanged. Microsoft (2016) has developed a framework, shown in Figure 1, that is tailored for cybersecurity information sharing and risk mitigation.

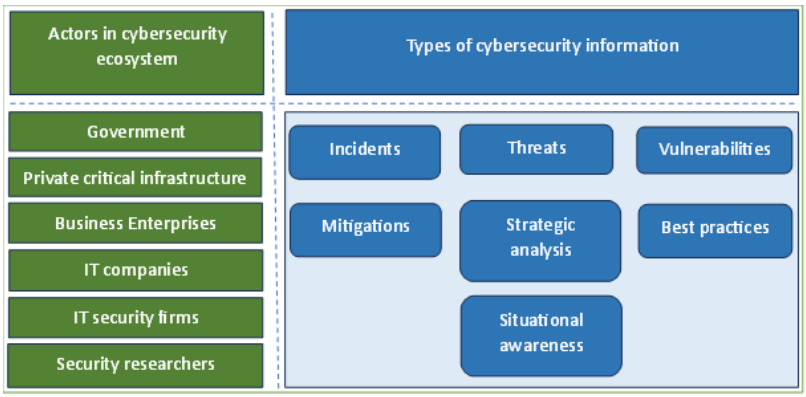

Figure 1: Microsoft's cybersecurity information-sharing platform and different types of governance structure

Effective threat information sharing in collaborative environments offers a multitude of advantages. It facilitates faster responses against hybrid threats, contributing to the development of a robust cyber-ecosystem within smart societies. By enhancing cybersecurity and risk management practices, organizations gain a deeper understanding of the threat landscape, enabling them to identify affected platforms and implement protective measures promptly. Additionally, knowledge maturation through the correlation of seemingly unrelated observations provides valuable insights into threat indicators and tactics. This process not only increases the degree of protection by reducing viable attack vectors but also fosters greater defensive agility, allowing organizations to adapt to evolving threat landscapes. Despite these benefits, challenges such as building and maintaining trust, achieving interoperability, and safeguarding sensitive information underscore the complexity of collaborative information-sharing efforts. Addressing these challenges is crucial to ensuring secure and effective information exchange in collaborative environments (Rajamäki, 2019).

3. Overview of Governance Models in Information-sharing Ecosystem

Organizations' governance functions play crucial roles in setting their strategic direction. According to the Chartered Governance Institute UK & Ireland (2022), corporate governance is defined as "the system of rules, practices, and processes by which a company is directed and controlled." This framework serves as a toolkit for management and the board to effectively navigate the challenges of running a company. One key aspect of corporate governance is ensuring the implementation of appropriate controls and decision-making processes that balance the interests of all stakeholders. It is particularly significant in meeting legal requirements such as the General Data Protection Regulation (GDPR) or the Network and Information Security (NIS) Directive.

Information governance, on the other hand, focuses on the overall strategy for managing information, encompassing policies, systems, people, and processes. By utilizing its various elements, organizations can establish and maintain relevant policies and procedures that align with data privacy requirements. Information governance seeks to balance the risks associated with information against the value it provides. This encompasses various aspects such as information security and protection, compliance, data quality, data governance, electronic discovery, risk management, privacy, data storage and archiving, knowledge management, business operations and management, audit, analytics, IT management, master data management, enterprise architecture, business intelligence, big data, data science, and finance.

The management functions within an organization take the strategic direction set by governance and translate it into actionable steps that bring the organization closer to achieving its strategic goals. A Management Information System (MIS) is employed for decision-making, coordination, control, analysis, and visualization of information within an organization. MIS involves the integration of people, technology, and processes within an organizational context. In corporations, the aim of using MIS is to enhance the value and profitability of the business through IT tools supporting various processes, operations, and intelligence. Information sharing is recognized as a crucial method to enhance organizational efficiency and performance (Yang & Maxwell, 2011).

In the pursuit of diving into governance models the research, it is imperative to establish a clear understanding of the concept of governance. While different sectors may offer varied definitions, a common thread defines governance as the systematic direction, control, and administration of an organization or system. According to the Government Institute of Australia, governance entails the structures and processes that oversee and guide an organization, inclusive of mechanisms for ensuring accountability. This broad concept encompasses ethics, risk management, compliance, and administration. Notably, Wang and Ran (2023) highlight the prevalence of confusion surrounding various governance concepts, with different types often exhibiting overlap or interchangeable usage. This confusion persists despite these concepts being integral to the operations of diverse systems.

This research focused on governance related to information systems, more definitely information-sharing-related governance systems. To narrow it down, IT governance can be classified as a subset of corporate governance, to facilitate the management of IT services and deliver value including information sharing among the organization (IT governance). A crucial aspect of this value proposition involves effective information sharing among various components of the organization, underlining the interconnected nature of IT governance (Weill & Ross, 2004). Information-sharing governance within IT governance plays a pivotal role in fostering collaboration, enhancing decision-making processes, and ensuring the secure and efficient flow of information across the organization. Effective governance in this context involves establishing policies, procedures, and controls that not only facilitate seamless information sharing but also address potential risks, safeguard sensitive data, and ensure compliance with relevant regulations (Calder, et al., 2008). Moreover, in an era where digital

transformation is pervasive, understanding and implementing robust information-sharing governance systems become paramount. This involves adapting to evolving technologies, staying ahead of cybersecurity threats, and incorporating best practices in information management to harness the full potential of IT services for organizational growth and success (Luftman, 2003).

To establish an efficient governance structure for the DYNAMO project, facilitating information sharing among partners, we analyzed existing governance structures. Our objective was to identify a suitable model that aligns seamlessly with the project's requirements. Figure 2 presents diverse governance taxonomies sourced from literature and thoughtfully compiled in the ECHO deliverable (Rajamäki, 2019).

Government-Centric Model:	**Sector-Based ISACs**	**Corporate-Initiated Groups**
• Centralized approach • Single organization leadership • Examples: Department of Homeland Security • Emphasis on open, standard data formats • Centralized coordination and control	• Government-prompted, industry-centric • Non-profit organizations • Facilitate government-industry information sharing • Vital collection points for peer-to-peer sharing	• Privately sponsored and independent • Initiated by corporations • Tailored information sharing for specific member needs
Individual-Based Groups	**Open Communities and Platforms**	**Diverse Governance for Cyber Information Sharing**
• Small online communities • Collaborative cyber attack response • Reliance on high trust levels among members	• Open-source platforms like MISP • Foster collaboration in the cybersecurity community • Use formats such as STIX indicators and open-source intelligence feeds	• Reflects the multifaceted nature of IT sector information sharing • Accommodates various organizational structures and collaboration levels • Adaptive approach crucial in the rapidly evolving cybersecurity landscape

Figure 2: Different types of governance structure

4. Policy Analysis

The European Union (EU) Treaty defines the legal basis for the creation of the European Internal Energy Market (IEM). Its goal is to create a well-functioning pan-European electricity and gas market that puts fair access and a high level of consumer protection at the center while ensuring sufficient generation and interconnection capacity across the continent (Manolkidis, 2021). Over the years, EU-derived legislation (regulations, directives, and recommendations) has built a path from a historically defined monopolistic system to a well-functioning free market. Today, the EU has a common policy on energy. According to the Energy Union 2015, this energy policy aims to ensure the security, sustainability, and competitiveness of energy supply and consumption in the EU. One of the key aspects of this policy is information sharing among the EU member states and institutions, as well as with third countries and international organizations. Information sharing on energy matters can help to improve coordination, cooperation, and transparency, as well as identify and address potential risks and challenges (REGULATION (EU) 2018/1999). The EU has established several mechanisms and platforms for information sharing on energy issues, each platform has specific goals, such as the 'Energy Policy' greatest the general principle:

- The Energy Union Governance System, Regulation (EU) 2018/1999
- The Energy Community, The Energy Community Legal Framework.
- The Energy Charter Treaty,
- The European Network of Transmission System Operators for Electricity (ENTSO-E) and Gas (ENTSO-G), Regulation (EC) 715/2009
- The Agency for the Cooperation of Energy Regulators (ACER), EU Regulation 1227/2011
- The European Energy Forum
- The Strategic Energy Technology Plan (SET-Plan).

These mechanisms and platforms cover various aspects of the energy sector, such as electricity, gas, oil, coal, nuclear, renewable, and low-carbon sources, energy efficiency, innovation, research and development, market

integration, infrastructure development, security of supply, climate change mitigation and adaptation, and external relations.

The DYNAMO project, funded by the European Union, proposed E-EWS as a tool to share information on cybersecurity among stakeholders. The energy sector is a critical infrastructure under the NIS Directive, which obliges member states to establish competent authorities and computer security incident response teams (CSIRTs) for the sector and to ensure that OES in electricity, oil, and gas subsectors report significant cyber incidents to the authorities. The EU also encourages the creation of information sharing and analysis centres (ISACs), such as the EE-ISAC, which enable voluntary and trust-based data and information sharing among utilities, regulators, vendors, and researchers. The EU's goal is to promote a culture of cyber resilience and cooperation in the energy sector and to identify and address gaps and challenges in the policy framework (Energy policy: general principles).

The EU information-sharing policy on energy is based on the principles of solidarity, subsidiarity, proportionality, and confidentiality (JOIN(2022) 49). This means that the EU member states and institutions share information on energy matters in a timely, accurate, and comprehensive manner while respecting the national competencies and interests of each member state, as well as the protection of sensitive data and information. The EU information-sharing policy on energy also aims to promote dialogue and consultation with relevant stakeholders, such as industry, consumers, civil society, and academia.

4.1 Legal Considerations

Information sharing on cybersecurity in the energy sector is a complex and sensitive issue that involves legal and ethical considerations. On one hand, information sharing can enhance the collective security and resilience of the energy sector by enabling timely detection, prevention, and mitigation of cyber threats. On the other hand, information sharing can pose risks to the privacy, confidentiality, and competitiveness of the energy sector actors, as well as potential liability and compliance issues. Therefore, a legal and ethical analysis of information sharing on cybersecurity in the energy sector should balance the benefits and risks of information sharing, considering the relevant laws, regulations, standards, and best practices, as well as the rights and interests of the stakeholders involved.

The European Data Governance Act is increasing trust in data sharing among diverse groups who are using data in the European Union. This exchange of data among various entities, such as organizations, countries, and individuals, involves a certain level of risk. The data may be misused by unauthorized or malicious parties, compromising the privacy and security of the data subjects. Therefore, the European Union has established a set of rules and regulations to govern the transmission and sharing of information, ensuring that the data is protected and used lawfully and ethically:

- **General Data Protection Regulation (GDPR).** If the information process involves any personal data, any processing and transmission should comply with GDPR.
- **Confidentiality and security obligations**. The EU recognizes the importance of confidentiality and security in information sharing. Entities sharing sensitive information, especially in sectors like energy or cybersecurity, are often subject to confidentiality obligations to protect the shared data.
- **Sector-specific regulations**. There may be specific regulations governing information sharing.
- **Trade secrets and intellectual properties**. EU laws protect trade secrets and parties sharing information must take measures to safeguard such business information.
- **EU competition law**. Sharing information may create a conflict of interest. EU-competition law should be respected.
- **Cross-border data transfer**. When sharing information across borders, entities must comply with rules governing international clauses or binding corporate rules, which may be necessary.

The following parts of the NIS Directive, discussed in more detail in the ENISA's document (ENISA, 2022), need to be addressed when designing the governance model for the DYNAMO platform:

- Human resource security – security training programs are required for employees with NIS-related responsibilities.
- Information system security risk analysis – during the designing process, regular risk analyses are conducted so possible risks are assessed as early as possible.
- Information system security audit – considering the regularly updated risk analysis, all critical assets are frequently audited to ensure compliance with regulations.

- Ecosystem mapping – during the design process, all documentation of the governance ecosystem is frequently updated.
- Information system security policy – building up to the risk analysis, an information system security policy will be established and maintained.
- Ecosystem relations – the interfaces between E-EWS and third parties are designed so that potential risks are mitigated.

The new Cyber Solidarity Act (the European Parliament and of the Council, 2023), once finalized and adopted, will contain important measures to strengthen the EU's preparedness, management, and response to cyber security threats and incidents. It is the latest addition to the EU's cybersecurity legislation, which aims to increase the resilience of critical entities against cybersecurity risks and support the coordinated management of large-scale cybersecurity disruptions and crises (Ajmera & Nusselder, 2023). The EU framework already in place consists of the NIS 2 Directive, the Cybersecurity Act, the Directive on attacks against information systems, and the Commission's r Recommendation on coordinated response to large-scale cybersecurity incidents and crises. The new proposal builds on and strengthens existing cyber security frameworks for operational cooperation and crisis management, such as the European cyber crisis liaison organisation network (EU-CyCLONe) and CSIRT network (Ajmera & Nusselder, 2023). Cross-border security operations centers (SOCs) are meant to complement the existing CSIRT network by sharing, connecting, and analyzing information on cyber security threats from both public and private entities. Importantly, the Cyber Solidarity Act proposal does not affect the critical and highly critical areas defined in the NIS 2 Directive. The Cyber Solidarity Act proposal also envisages close cooperation with the private sector. Its goal is to promote cross-border and public-private cooperation in anticipating and countering cyberattacks by combining information from both public and private entities to derive high-quality intelligence on cybersecurity threats. In addition, the EU's cyber security reserve consists of selected private providers of managed information security services that support response and immediate recovery in large-scale cyber security incidents (Ajmera & Nusselder, 2023).

Entities that share CTI information within the EU must understand and follow the legal considerations to comply with the relevant laws and regulations. Organizations should seek legal counsel tailored to their specific circumstances when dealing with the challenges of information sharing under EU law.

4.2 Ethical Considerations of Data

Data sharing is the practice of making data available to other individuals or organizations for various purposes, such as research, innovation, collaboration, or public service. Data sharing can have many benefits, such as increasing the transparency, reproducibility, and impact of scientific findings, fostering discoveries and collaborations, and enhancing the efficiency and quality of data collection and analysis. However, data sharing also poses some ethical challenges, especially in the European context, where data protection and privacy laws are strict and complex. Echo early warning system(E-EWS) is a tool to share information with other stakeholders. Every party who participates in this data-sharing platform should follow some ethical guidelines to make a positive impact for the right purpose of protecting the energy sector assets from different attacks. Next, two European ethical aspects related to the organization's data sharing in Europe are presented.

The protection of the organization's sensitive data: Data should be anonymized or pseudonymized before sharing and should be encrypted or stored in secure platforms. Data sharing should also follow the principles of data minimization and purpose limitation, meaning that only the necessary and relevant data should be shared for a specific and legitimate purpose.

The accountability and responsibility of the data sharers: Data sharing should be done responsibly and transparently, with clear roles and responsibilities for the data sharers, who are the individuals or organizations that share or receive data. Data sharers should adhere to the ethical standards and codes of conduct of their disciplines or sectors and should respect the intellectual property rights and interests of the data owners or creators. Data sharers should also monitor and evaluate the impacts and outcomes of data sharing and report any issues or incidents that may arise.

5. Proposed Governance Framework

As shown in Figure 2, our research indicates that the most suitable fit for the DYNAMO platform is the Diverse Governance Model for Cyber Information Sharing. This model accommodates multiple organizations and embraces an adaptive and innovative approach. Table 1 summarizes the framework we propose based on this

study. The table contains a set of actionable steps to create an effective governance system for information sharing within DYNAMO partners.

Table 1: Proposed Governance Framework

Actions	Description
Formation of Governance Committee	DYNAMO and its partners should form a Governance Committee with representatives from each partner organization. This committee will oversee the implementation of the governance model.
Roles and Responsibilities	Each partner organization designates a Data Steward responsible for data access and sharing within their organization. The Data Stewards play a crucial role in enforcing the governance policies.
Information Sharing Policies	Implement data privacy and security measures that comply with GDPR and other regulations. This includes Data encryption for data at rest and in transit. Access controls to ensure that only authorized personnel can access sensitive information. Incident response procedures to address and report security breaches promptly.
Collaboration Tools	Select and implement collaboration and information-sharing tools that meet the specific needs of DYNAMO and its partners. Ensure that these tools are user-friendly and support secure data sharing.
Access Controls	Establish access controls for the collaboration tools, defining user roles and permissions based on the data they need to access. Regularly review and update access controls as needed
Monitoring and Auditing	Set up continuous monitoring and auditing mechanisms to detect security breaches or policy violations. Use monitoring tools to track data access and sharing activities.
Training and Awareness Programs	Conduct training programs for all stakeholders to ensure that they understand the governance model and policies. Regularly update and provide refresher training sessions.
Compliance and Legal Framework	Ensure that the governance model aligns with EU and local legal requirements and adapts as regulations change. This may involve periodic legal reviews and consultations.
Continuous Improvement Process	Establish a process for ongoing evaluation and improvement of the governance framework. Collect feedback from partners, identify areas for improvement, and make necessary updates to policies and procedures.
Communication Plan	Develop a comprehensive communication plan to inform stakeholders about changes, updates, and important information. Use various communication channels to ensure that all partners are well-informed.
Conflict Resolution Mechanism	Implement a conflict resolution mechanism to address disputes or disagreements among partner organizations related to information sharing. This could involve a designated mediator or a defined process for dispute resolution.
Pilot Implementation	Before full-scale implementation, consider a pilot phase where the governance model is tested with a smaller subset of partners to identify any potential issues and make necessary adjustments.
Full-Scale Implementation	After successful pilot testing and fine-tuning, roll out the governance model to all partners for full-scale implementation.
Monitoring and Evaluation	Regularly monitor the effectiveness of the governance model and evaluate its impact on information sharing, security, and collaboration. Make improvements based on feedback and data.

6. Conclusion

The modern electricity grid is completely dependent on information and supervisory systems that control the production, transmission, and distribution of electricity. Disturbances that impair the functionality of control systems cause disturbances in the power supply, which can endanger human lives and cause financial losses. Resources for resilience that mitigate those losses bring both energy companies and electricity users an advantage that exceeds the initial costs of the network. Therefore, increasing certain resources improves both long-term efficiency and resilience.

The DYNAMO project develops methods and resources for connecting business continuity management (BCM) and cyber threat intelligence (CTI) and creates a platform for sharing CTI among different actors. This paper explores the implementation of governance of the ECHO Early Warning System (E-EWS) tool for CTI sharing within the energy sector. The research investigates the role of governance in E-EWS implementation and proposes a diverse governance framework. Key actions in the framework include forming a Governance Committee, defining roles, implementing information-sharing policies, selecting collaboration tools, and ensuring legal compliance. The document also discusses EU policies on energy information sharing, legal

considerations under the European Data Governance Act, and ethical aspects of data sharing. In essence, the proposed governance framework addresses the complex cybersecurity landscape by fostering collaboration, ensuring legal and ethical compliance, and promoting cyber resilience. It is designed for adaptability and refinement over time, providing a strategic approach to information sharing via the DYNAMO platform.

The target for further research and development is to examine the functionality of the created governance framework in other critical sectors of the DYNAMO project: healthcare and maritime transport. In addition, the principles presented in the framework should be translated into more concrete specifications.

Acknowledgments

Acknowledgment is paid to 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

Ajmera, P. & Nusselder, S., 2023. INTERSECT policy brief 2: Cyber Solidarity Act proposal, Tilburg: Tilburg Institute for Law, Technology, and Society (TILT).

Braeuer, F. et al., 2022. Optimal system design for energy communities in multi-family buildings: the case of the German Tenant Electricity Law. Applied Energy, Volume 305, p. 117884.

Calder, A., Watkins, S., & Gilding, M. (2008). IT Governance: A Manager's Guide to Data Security & ISO 27001 / ISO 27002. Kogan Page.

Chartered Governance Institute UK & Ireland, 2022. What is corporate governance? [Online] Available at: https://www.cgi.org.uk/about-us/policy/what-is-corporate-governance, [Accessed 18 Nov. 2022].

Gordon, K., 2013. Principles of Data Management - Facilitating Information Sharing. Second Edition. Swindon: BCS Learning & Development Limited.

ENISA, 2022. Minimum Security Measures for Operators of Essentials Services. [Online] Available at: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services [Accessed 4 January 2024].

European Parliament and of the Council, 2023. Cyber Solidarity Act proposal, COM(2023) 209 final. [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209 [Accessed 4 January 2024].

Hytönen, E., Rajamäki, J. & Ruoslahti, H., 2023. Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking. International Conference on Cyber Warfare and Security, 18(1), pp. 162-170.

Kokkonen, T., Hautamäki, J., Siltanen, J. & Hämäläinen, T. (2016) Model for sharing the information of cyber security situation awareness between organizations, 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 2016, pp. 1-5, doi: 10.1109/ICT.2016.7500406.

Luftman, J. (2003). Assessing IT/Business Alignment. Information Systems Management, 20(4), 9–15.

Manolkidis, S., 2021. Geopolitical challenges and cooperation in the European energy sector: The case of SE Europe and the Western Balkan six initiative. In: M. Mathioulakis, ed. Aspects of the Energy Union: Application and Effects of European Energy Policies in SE Europe and Eastern Mediterranean. Cham: Springer Nature Switzerland, pp. 101-114.

Marc, A., & Aloys, M. (2023, August 01). Cybersecurity – Is the power system lagging behind? International Energy Agency. [Online]. Available: https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

Microsoft. (2016). Cybersecurity Information Sharing and Risk Reduction. Retrieved from https://www.microsoft.com/en-us/research/project/cybersecurity-information-sharing-and-risk-reduction/.

Nicho, M. (2018). A process model for implementing information system security governance. Zayed University Scholars. [Online]. Available: https://zuscholars.zu.ac.ae/cgi/viewcontent.cgi?article=1227&context=works

Peters, L. & Manz, C. M., 2007. dentifying antecedents of virtual team collaboration. Team Performance Management: An International Journal, 13(3/4), pp. 117-129.

Rajamäki, J. (2019) ECHO Information sharing models. https://echonetwork.eu/wp-content/uploads/2020/02/ECHO_D3.6-ECHO-Information-Sharing-Models-v1.0.pdf

Rajamäki, J. & Katos, V., 2020. Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. Information & Security: An International Journal , 46(2), pp. 198-214.

Ruoslahti, H. & Tikanmäki, I., 2019. Complex Authority Network Interactions in the Common Information Sharing Environment. In: Bernardino, Jorge; Salgado, Ana; Filipe, Joaquim (Eds.) *Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2019).* Setúbal: Science and Technology Publications, pp. 159 – 166

Wang, H., & Ran, B. (2023). Network governance and collaborative governance: A thematic analysis on their similarities, differences, and entanglements. Public Management Review, 25(6), 1187-1211. https://doi.org/10.1080/14719037.2021.2011389

Weill, P., & Ross, J. W. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press.

Yadoshchuk, V. (2023, May 15). Digital Transformation in the Energy Industry: Overview and Tips. [Online]. Available: https://waverleysoftware.com/blog/digital-transformation-in-the-energy-industry/#:~:text=accessible%20user%20interface.-,Conclusion,%2C%20IoT%2C%20and%20blockchain%20technologies

Yang, T. & Maxwell, T., 2011. Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. Government Information Quarterly, 28(2), pp. 164-175.