Operationalizing AI for Cyber Threat Intelligence: Governance Insights from the DYNAMO Framework

Jyri Rajamäki, Nasim Ali, Oskari Kulmala, Dilasha Singh Thakur and Tatu Sorola
Laurea University of Applied Sciences, Finland

jyri.rajamaki@laurea.fi

Abstract: As artificial intelligence (AI) becomes increasingly embedded in cybersecurity operations, the need for structured, compliant, and scalable integration frameworks is more urgent than ever. This paper explores how AI can be operationalized within cyber threat intelligence (CTI) systems, through a qualitative case study in the energy sector, using the DYNAMO framework as a case study. Originally developed to enhance resilience in critical infrastructure sectors, DYNAMO combines business continuity management (BCM) and CTI to support situational awareness and proactive risk mitigation. Although the framework has been applied in the energy sector in this study, its principles apply to other domains that face complex cyber threats. The study investigates how AI—particularly machine learning—can improve CTI sharing by enabling real-time threat detection, pattern recognition, and adaptive response. Drawing on recent academic and industry literature, we analyze the benefits and limitations of AI-enhanced CTI, including improved detection accuracy and faster response times. However, challenges such as adversarial attacks, model poisoning, and the need for high-quality training data are also addressed. We further examine the governance implications of integrating AI into CTI platforms, especially in light of the EU Cyber Resilience Act (CRA). The paper highlights the importance of aligning AI deployment with regulatory requirements, such as 24-hour incident reporting, post-market monitoring, and data sovereignty. The ECHO Early Warning System (E-EWS), a collaborative platform developed under the EU Horizon 2020 program, is presented as a practical example of cross-sectoral CTI sharing that incorporates AI capabilities. Our findings suggest that AI can significantly enhance cyber resilience when embedded within a governance-aware framework like DYNAMO. We recommend a phased implementation strategy that includes stakeholder training, regulatory alignment, and continuous monitoring. The paper concludes by emphasizing the need for interdisciplinary collaboration between AI developers, cybersecurity professionals, and policymakers to ensure responsible and effective AI integration in CTI systems.

Keywords: Artificial intelligence (AI), Cyber resilience, Cyber threat intelligence (CTI), Critical Infrastructure, DYNAMO Framework, EU Cyber Resilience Act (CRA), Regulatory compliance

1. Introduction

As artificial intelligence (AI) becomes increasingly embedded in cybersecurity operations, the need for structured, compliant, and scalable integration frameworks is more urgent than ever. This paper explores how AI can be operationalized within cyber threat intelligence (CTI) systems, using the DYNAMO framework as a case study. Originally developed to enhance resilience in critical infrastructure sectors, DYNAMO combines business continuity management (BCM) and CTI to support situational awareness and proactive risk mitigation. Although the framework has been applied in the energy sector in this study, its principles apply to other domains that face complex cyber threats.

As cyber threats grow in complexity and scale, CTI remains essential to cybersecurity, particularly for critical energy infrastructure (CEI). This work-in-progress paper investigates the role of AI—especially machine learning (ML)—in improving CTI sharing to detect, anticipate, and mitigate threats in real time. A thematic and comparative analysis of academic, industrial, and policy literature highlights AI's potential to enhance detection accuracy and response speed. The paper also examines integration frameworks such as the ECHO Early Warning System (E-EWS), which enables collaborative CTI sharing while safeguarding data sovereignty. Despite AI's benefits, challenges such as resource demands and adversarial attacks persist. The study concludes with recommendations for integrating CTI platforms with AI, drawing on examples like the EU-funded DYNAMO project.

2. Literature Review

The collection and analysis of CTI have become increasingly critical due to the rapid evolution of cyberattacks, which are now more organized and multi-vectored than in the past. CTI contributes to cybersecurity across tactical, operational, and strategic levels (Kure & Islam, 2019). A key challenge in cybersecurity is the information asymmetry between attackers and defenders, making threat intelligence sharing a vital mechanism for reducing this gap (Du et al., 2020).

The diversification and specialization of modern cyber threats have rendered passive protection methods insufficient. CTI sharing platforms enhance the efficiency of active detection methods, which rely heavily on continuous monitoring and analysis (Du et al., 2020). CTI also plays a central role in threat and risk assessment,

supporting the adaptation of risk management strategies. However, many existing risk management frameworks lack the agility and efficiency needed to anticipate emerging threats and safeguard assets effectively (El Amin et al., 2024).

Critical energy infrastructure (CEI), encompassing energy generation, transmission, and distribution, is essential for both economic stability and societal functioning. CEI is deeply interconnected with other sectors such as water distribution and telecommunications, and its complex technological landscape presents a broad attack surface (Govea, Gaibor-Naranjo, & Villegas-Ch, 2024). Machine learning and other algorithmic approaches are increasingly employed within CEI, not only for cybersecurity—particularly in attack detection—but also for operational tasks such as grid stability and energy optimization (Szczepaniuk & Szczepaniuk, 2023).

Examples of CEI include power grids and oil and gas facilities. These systems are highly vulnerable to cyber-attacks due to their reliance on industrial control systems and operational technologies, which present numerous entry points for malicious actors (Daniel & Victor, 2024). More broadly, network intrusion detection systems (NIDS) are evolving from traditional signature-based models to machine learning-based systems. These newer systems are better equipped to handle zero-day attacks and persistent threats through behavioral analysis and adaptive techniques (Manoharan & Sarker, 2022).

In the context of CTI, the utility of simple indicators of compromise (IoCs) diminishes over time as systems evolve or are remediated. While machine learning and deep learning models demand more computational resources, they offer superior capabilities in characterizing complex threats. However, their integration can also expand the attack surface of the systems they aim to protect (Preuveneers & Joosen, 2021).

Kure and Islam (2019) proposed a unified CTI framework for critical infrastructure using Structured Threat Information Expression (STIX) and Common Weakness Enumeration (CWE) standards. Their model includes strategic, tactical, and operational components: strategic intelligence focuses on threat actors and attack processes; tactical intelligence identifies network and system indicators; and operational intelligence involves trend analysis, control deployment, and vulnerability mapping.

Ammi and Jama (2023) presented a case study utilizing the MISP threat intelligence sharing platform. Their architecture integrates open-source intelligence (OSINT) feeds into MISP, which then distributes data to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), followed by aggregation in a Security Information and Event Management (SIEM) system, and finally visualized through a web interface.

In a study focused on CEI, Govea, et al. (2024) addressed the growing threat surface by integrating AI systems capable of anticipating, detecting, and responding to security incidents. Their evaluation of various AI technologies considered detection efficiency, scalability, resource requirements, and cost. Through an iterative integration process, they achieved a detection rate of 94.7%, significantly outperforming traditional systems, which reached only 74.9% on the same dataset.

3. Methodology

This study investigates the integration of AI in CTI sharing within the energy sector, through a qualitative case study in the context of the DYNAMO framework, complemented by governance analysis aligned with EU cybersecurity regulations. The research adopts a qualitative approach, drawing on data collected from peer-reviewed academic publications, industry reports, policy documents, public materials of the ECHO and DYNAMO project, and technical evaluations of threat intelligence platforms. To ensure relevance to current cybersecurity challenges, the study focuses on sources published within the last five years.

A thematic analysis was conducted to identify recurring patterns and themes related to AI integration in CTI sharing. In addition, a comparative analysis was performed to examine differences across various approaches, platforms, and frameworks. This dual analytical strategy enhances the validity of the findings by enabling a nuanced understanding of the advantages, limitations, and scalability of different AI applications in CTI systems.

The research adheres to our university's guidelines for research integrity and complies fully with the General Data Protection Regulation (GDPR). All data sources used in the study are publicly accessible and open, and no personal or sensitive data were collected during the research process.

4. Findings

The analysis revealed several key insights regarding the integration of artificial intelligence (AI) into cyber threat intelligence (CTI) sharing within the energy sector.

First, machine learning algorithms significantly enhance threat detection capabilities. AI-based systems have demonstrated detection accuracies of up to 94.7%, compared to 74.9% for traditional methods (Gandham, 2025). This improvement is attributed to AI's ability to process large volumes of data, identify complex patterns, and adapt to evolving threats in real time. However, the integration of AI is not without challenges. These include the need for high-quality training data, vulnerability to adversarial attacks, and the continued necessity of human oversight to ensure interpretability and accountability (Yaseen, 2023).

A notable example of cross-sectoral CTI sharing is the ECHO Early Warning System (E-EWS), developed under the EU's Horizon 2020 program. E-EWS facilitates the exchange of machine learning models and integrates various monitoring solutions. One such solution is the MonSys Bridge prototype, which connects external Security Information and Event Management (SIEM) tools to E-EWS, enhancing threat detection and response capabilities (ECHO Network, 2020).

Despite the benefits, AI integration demands substantial computational resources and robust infrastructure. Threats such as model poisoning underscore the importance of strong data validation, continuous monitoring, and anomaly detection mechanisms (Grant Thornton, 2023). Pre-integration assessments and strategic planning are essential to minimize operational disruptions and ensure secure deployment (Bhalsod, 2024).

Organizations in the energy sector are increasingly adopting advanced CTI practices, including layered system architectures and standardized data formats such as STIX and TAXII (Kravensecurity.com, 2023). These standards support efficient, automated information exchange. Furthermore, combining open-source and proprietary threat intelligence sources enhances both scalability and the depth of insights (Seerist, 2025).

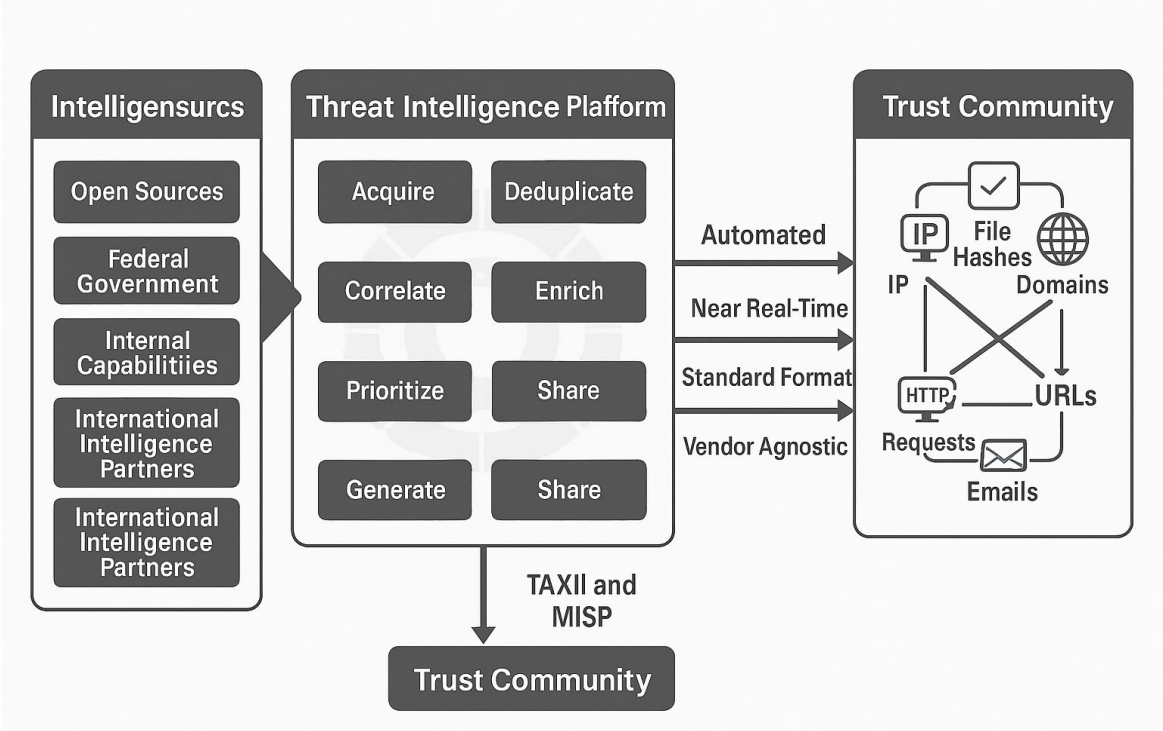

Figure 1: Cyber threat intelligence sharing workflow (modified from Amazon Web Services, 2025)

Finally, secure data sharing and trust are critical. DYNAMO's E-EWS emphasizes data sovereignty, enabling collaboration without compromising sensitive information (Rajamäki, Feyesa & Nepal, 2024; De Vecchis, 2020). Figure 1 presents Amazon Web Services' example, in which CTI flows from diverse sources through a threat intelligence platform that processes and enriches data, then shares indicators (IPs, domains, URLs, file hashes, emails) with a trust community via TAXII and MISP using automated, near real-time, standardized, vendor-agnostic exchange (Amazon Web Services, 2025).

5. Discussion and Conclusions

This research highlights both the potential and the complexity of integrating AI into CTI sharing systems within the energy sector, using the DYNAMO project as a contextual framework. The findings demonstrate that AI—particularly machine learning—can significantly enhance threat detection in terms of accuracy, speed, and scalability. Empirical evidence suggests up to a 20% improvement in detection efficiency compared to traditional methods (Gandham, 2025).

However, the study also identifies several practical and strategic challenges. The effectiveness of AI systems is highly dependent on the availability of high-quality training data, the integrity of that data, and the reliability of the supporting infrastructure. Deep learning models, while powerful, require substantial computational resources and are themselves susceptible to threats such as model poisoning and adversarial manipulation. Addressing these vulnerabilities necessitates robust data governance, rigorous testing, and continuous monitoring.

The case of E-EWS within the DYNAMO architecture illustrates the practical feasibility of AI-enhanced CTI sharing across sectors. E-EWS supports the exchange of ML models and integrates tools such as the MonSys Bridge, which connects external SIEM systems to the platform. The use of standardized formats like STIX and TAXII further enhances interoperability and automation, making CTI sharing more efficient and scalable. Despite these technological advancements, organizational readiness remains crucial. Compliance with emerging regulations, such as the EU AI Act, and the responsible use of AI are essential for sustainable implementation. Based on the findings, the following recommendations are proposed:

- **Foster collaboration** between public and private stakeholders to enhance knowledge sharing and resource pooling.
- **Provide targeted training** for energy sector personnel on AI technologies and threat intelligence analysis.
- **Develop structured integration plans** to ensure that AI adoption does not disrupt existing cybersecurity operations.

While AI offers transformative potential for CTI sharing in the energy sector, its successful implementation requires a balanced approach that combines technological innovation with strategic planning, regulatory compliance, and human oversight.

Acknowledgements

Acknowledgments are paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601, and to the project *"Development of Cybersecurity Education and Related Collaboration in Higher Education"*, funded by the Finnish Ministry of Education and Culture under the national program for strengthening cybersecurity competencies and collaboration among universities. The views and opinions expressed are solely those of the authors only and do not necessarily reflect those of the European Union, European Commission, or Finnish Ministry of Education and Culture. Neither the European Union nor the granting authorities can be held responsible for them.

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

AI declaration: Figure 1 was drawn with AI assistance. The paper's spelling was verified using the artificial intelligence tool.

References

Amazon Web Services. 2025. AWS Prescriptive Guidance: Cyber threat intelligence sharing on AWS. https://docs.aws.amazon.com/prescriptive-guidance/latest/cyber-threat-intelligence-sharing/introduction.html

Ammi, M. & Jama, Y. 2023. Cyber Threat Hunting Case Study using MISP. *Journal of Internet Services and Information Security 13 (2)*, 1–29. https://jisis.org/wp-content/uploads/2023/06/2023.I2.001.pdf

Bhalsod, S. 2024. AI Cybersecurity Challenges: Navigating Emerging Threats and Opportunities. *DEV Community*. https://dev.to/siddharthbhalsod/ai-cybersecurity-challenges-navigating-emerging-threats-and-opportunities-4fd1

Daniel, S. & Victor, S. 2024. Emerging trends in cybersecurity for critical infrastructure protection: a comprehensive review. *Computer Science & IT Research Journal 5(3)*, 576–593. https://fepbl.com/index.php/csitrj/article/view/872

De Vecchis, F. 2020. ECHO Early Warning System (E-EWS). *ECHO Network*. https://echonetwork.eu/echo-early-warning-system-e-ews/

Du, L., Fan, Y., Zhang, L., Wang, L. & Sun, T. 2020. A Summary of the Development of Cyber Security Threat Intelligence Sharing. *International Journal of Digital Crime and Forensics 12(4)*, 54–67. https://www.igi-global.com/gateway/article/full-text-pdf/262156

ECHO Network. 2020. Prototypes. *ECHO Network*. https://echonetwork.eu/prototypes/

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

Flare.io. 2023. *Threat Intelligence Sharing: 5 Best Practices*. https://flare.io/learn/resources/blog/threat-intelligence-sharing/

Gandham, D. 2025. Understanding AI-Driven Threat Detection and Response Systems: A Technical Deep Dive. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 10 (4), 1–6. https://ijsrcseit.com/index.php/home/article/view/CSEIT251112324

Govea, J., Gaibor-Naranjo, W. & Villegas-Ch, W. 2024. Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems 12(5)*. https://www.mdpi.com/2079-8954/12/5/165

Grant Thornton. 2023. Anticipate cybersecurity and privacy risks in AI. *Grant Thornton*. https://www.grantthornton.com/insights/articles/advisory/2023/anticipate-cybersecurity-and-privacy-risks-in-ai

Kravensecurity.com. 2023. STIX/TAXII: A Full Guide to Standardized Threat Intelligence Sharing. https://kravensecurity.com/stix-and-taxii-a-full-guide/

Kure, H. & Islam, S. 2019. Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. *Journal of Universal Computer Science 25(11)*, 1478–1502. https://lib.jucs.org/article/22673/

Manoharan, A., & Sarker, M. 2023. Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. *International Research Journal of Modernization in Engineering Technology and Science 4(12)*. DOI: https://www.doi.org/10.56726/IRJMETS32644 , 1.

Preuveneers, D. & Joosen, W. 2021. Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. *Journal of Cybersecurity and Privacy 1(1)*, 140–163. https://www.mdpi.com/2624-800X/1/1/8

Rajamäki, J., Feyesa, A. & Nepal, A. 2024. E-EWS-based governance framework for sharing cyber threat intelligence. *European Conference on Cyber Warfare and Security, 23(1),* s. 398–406. https://papers.academic-conferences.org/index.php/eccws/article/view/2073

Seerist. 2025. Integrating Threat Intelligence Feeds into Your Security Strategy. *Seerist*. https://seerist.com/blog/integrating-threat-intelligence-feeds-into-your-security-strategy/

Szczepaniuk, H. & Szczepaniuk, E. 2023. Applications of Artificial Intelligence Algorithms in the Energy Sector. *Energies 16(1)*, 347. https://www.mdpi.com/1996-1073/16/1/347

Yaseen, A. 2023. AI-Driven Threat Detection and Response: A Paradigm Shift in Cybersecurity. *International Journal of Information and Cybersecurity* 7(12), 25–43. https://www.researchgate.net/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen