Challenges and Opportunities for Cross-Domain Cyber Threat Intelligence Sharing Towards Whole-of-Society Resilience

Bandara Dissanayake and Mamello Thinyane
University of South Australia, Mawson Lakes SA, Australia

bandara.diss@mymail.unisa.edu.au
mamello.thinyane@unisa.edu.au

Abstract: The increasing sophistication, frequency, and scale of cyberattacks means that societies cannot rely on isolated and uncoordinated defences but should embrace collaboration and intelligence sharing to remain cyber resilient. In many countries intelligence sharing lies at the heart of national security architecture and is embedded in strategies and in legislation, such as USA's Cybersecurity Information Sharing Act or the Australia's Security of Critical Infrastructure Act. In cybersecurity, cyber threat intelligence (CTI) is data created through the careful analysis of cyber threats and adversary behaviours to produce high-quality, timely, actionable, and relevant insights, allowing organizations to confidently anticipate, detect, prevent, and respond to cyberattacks. CTI provides critical insights into potential threats, enabling real-time responses during incidents, targeted mitigation strategies, and rapid recovery. Cross-domain CTI sharing plays a key role in breaking down silos, fostering cooperation across industries and sectors thus giving recognition to the interconnected nature of today's digital landscape, where a cyber threat in one domain can cascade into and impact other domains. By sharing actionable CTI, organizations can collectively identify vulnerabilities, respond to threats in real time, and protect critical societal functions such as healthcare, finance, energy, and communication while strengthening the overall resilience of interconnected systems. Around the world, enhancing CTI sharing has become increasingly critical and remains a key driver for societal cyber resilience, enabling organizations, communities, and individuals to anticipate, withstand, recover from, and adapt to and thrive amid the ever-evolving complexities of the cyber threat landscape. This study examines the challenges and opportunities for cross-domain CTI sharing through a comprehensive systematic review of literature, focusing on key issues such as protecting sensitive data from adversaries when shared outside every trusted organization in the system, building trust among diverse stakeholders, navigating governmental regulations, and ensuring seamless interoperability to enable stakeholders to remain in sharing and using CTI. The research underscores how collaboration across industries and sectors can foster a stronger, more unified defence against the ever-evolving threats in today's cyber landscape.

Keywords: Cyber resilience, Cyber threat intelligence, Whole-of-society, Cross-domain solutions

1. Introduction

The global digital transformation has seen digital technologies incorporated into different sectors of societies and supporting critical functioning across all these sectors. With this has been an increase in the sophistication, frequency and impact of cyber threats which has seen many countries, governments and organizations finding it hard to keep pace (Alaeifar et al., 2024; Dykstra et al., 2023). The systemic and interconnected nature of the cybersecurity ecosystem means that traditional isolated cybersecurity defences no longer provide the protection they once did (Du et al., 2020). This growing complexity makes collaboration across sectors essential and highlights the need for whole-of-society resilience (Chalkias et al., 2024).

One of the critical areas of collaboration that can enhance the effectiveness of cyber defences across sectors is CTI sharing. CTI sharing helps organizations stay ahead of threats by allowing them to understand, detect, analyse, respond cyber threats, spot adversary tactics, and find vulnerabilities more effectively before they become serious problems (Dykstra et al., 2023; Stojkovski and Lenzini, 2021). Instead of just reacting to incidents, CTI provides security teams with strategic, tactical, and operational insights to be proactive and to stop attacks before they happen. Governments worldwide have set up policies and frameworks to make CTI sharing more structured and effective (Ainslie et al., 2023). These frameworks set expectations for risk management, data security, and intelligence-sharing practices, ensuring that organizations follow standardized procedures to mitigate cyber threats (Ainslie et al., 2023). At the same time, industry standards such as ISO 27005:2022 provide guidance on secure information-sharing practices between sectors, balancing data protection with intelligence accessibility for real-time threat response (Sauerwein et al., 2024). Research has found that those that participate in intelligence-sharing networks gain better situational awareness, which helps them act faster and reduce risks (Du et al., 2020).

Many approaches to address CTI sharing have been proposed including industry models like Information Sharing and Analysis Centres (ISACs); technologies such as Trusted Automated eXchange of Indicator Information (TAXII), Structured Threat Information eXpression (STIX), the Malware Information Sharing Platform (MISP), Traffic Light Protocol (TLP) designations for information classification; and trust taxonomies such as the 5x5x5 scheme and

the Admiralty Code (Arachchilage et al., 2013; Tavakolifard and Almeroth, 2012). Some of these approaches have been shown to be effective in different contexts, for example in closed groups or where trust is preestablished between stakeholders, however, research has shown that CTI sharing remains a challenge mainly due to trust concerns (Wagner et al., 2018). Several factors have been noted to contribute to trust among stakeholders, such as individual stakeholder rating (based on previous engagements and reputation), extent of stakeholder sharing activities (which could expose free riders), CTI source (whether the stakeholders produce the information they share or if it is from unknown sources), and same industry (if the stakeholders are in the same industry) which has the highest impact on trust (Wagner et al., 2018). However, many other factors, beyond trust, affect the effectiveness of CTI sharing especially in cross-domain contexts. Overall, the challenges of cross-domain CTI sharing, encapsulate CTI use challenges in general, as well as CTI sharing challenges within singular entities as depicted in Figure 1. Further, across these different levels, the challenges apply to different elements of the CTI lifecycle. For example, sharing challenges are mainly associated with phases of information collection, dissemination, and feedback.

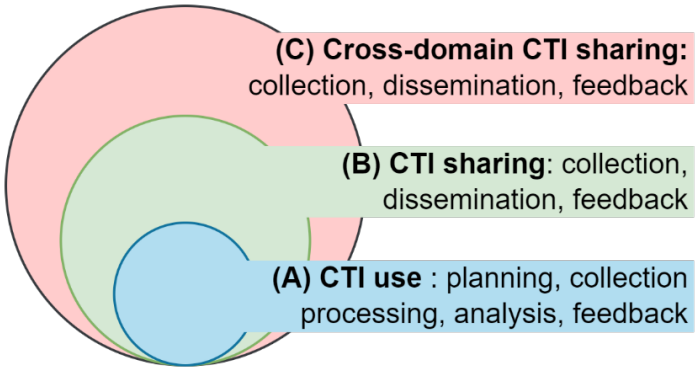

Figure 1: Intersections of CTI use and sharing challenges mapped to CTI lifecycle phases

This research notes the importance of CTI sharing across the whole-of-society, which implies sharing across different domains such as organizational, sectoral, industrial, jurisdictional, societal, and trust domains. As such the research aims to investigate factors that affect the effectiveness of CTI sharing in cross-domain contexts. The next section discusses the methodological approach employed in this research, followed by a presentation of the key findings regarding challenges and opportunities of cross-domain CTI sharing. The paper concludes with a discussion that synthesized an initial taxonomy of cross-domain CTI sharing challenges.

2. Methodology

The inquiry in this research is aimed to review documented opportunities and challenges of CTI sharing at a whole-of-society level. The research employed the systematic literature review (SLR) methodology framed around the question “What are the challenges and opportunities of CTI sharing in cross-domain contexts?”. SLRs are a knowledge synthesis methodology that aims to appraise current knowledge or generate evidence of existing research in order to answer a clearly defined research question (Newman and Gough, 2020). The reporting on the review undertaken in this research is informed by the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) 2020 guidelines to ensure a systematic and structured approach for the evidence synthesis and reporting (Page et al., 2021).

The primary *information sources* for the articles reviewed are Scopus and Web of Science, two well-regarded academic databases, which also index relevant publications within the cybersecurity domain. The *search strategy* involved searching for key terms in all published documents across the two databases. The focus of the search is on CTI and therefore this had to be the main subject of the articles and expressed in the title. Further the framing of the research is about CTI sharing across different domains, including trust and security domains, and so this formed the second search element, resulting in the following database query string:

> **TITLE** ("cyber threat intelligence" OR "CTI" OR "threat intelligence") AND
>
> **TITLE-ABS-KEY** (("cybersecurity" OR "cyber security" OR "cyber resilience" OR "information security" OR "network security") AND ("trust" OR "sharing" OR "trust domain" OR "security domain" OR "cross-domain" OR "cross domain")) AND

PUBYEAR > 2018 AND **PUBYEAR** < 2025

The *eligibility criteria* for the review were for peer-reviewed academic studies published between 2019 and 2025. The constraint on the publication period is to accommodate the rapid changes and recent advancements within the cybersecurity domain and therefore to keep the evidence synthesis relevant. Further, only English-language papers in the public domain and accessible to the researchers were considered for the review.

The *selection process* for the articles included in the review is depicted in Figure 2 and unfolded as follows. A total of 87 (WoS: 22 and Scopus:65) relevant records were identified. From these, 16 duplicates were removed, which left 71 studies for screening. The screening, based on detailed reading and review of the titles, abstracts, and keywords led to 12 studies being excluded for lack of direct relevance to the focus of this review. The remaining 59 studies were further reviewed in detail and assessed for eligibility based on the inclusion and exclusion criteria. The main *inclusion criterion* was for studies focused on aspects of CTI sharing with a particular interest in CTI sharing in broad societal contexts, for example, beyond single organizational boundaries. In terms of the *exclusion criteria*, articles that primarily focused on CTI technical solutions not related to sharing were excluded, as well as articles in which CTI sharing was tangential. At the end of this screening process, 26 studies, including 2 that were identified through citation snowballing, were selected for inclusion in the final review.

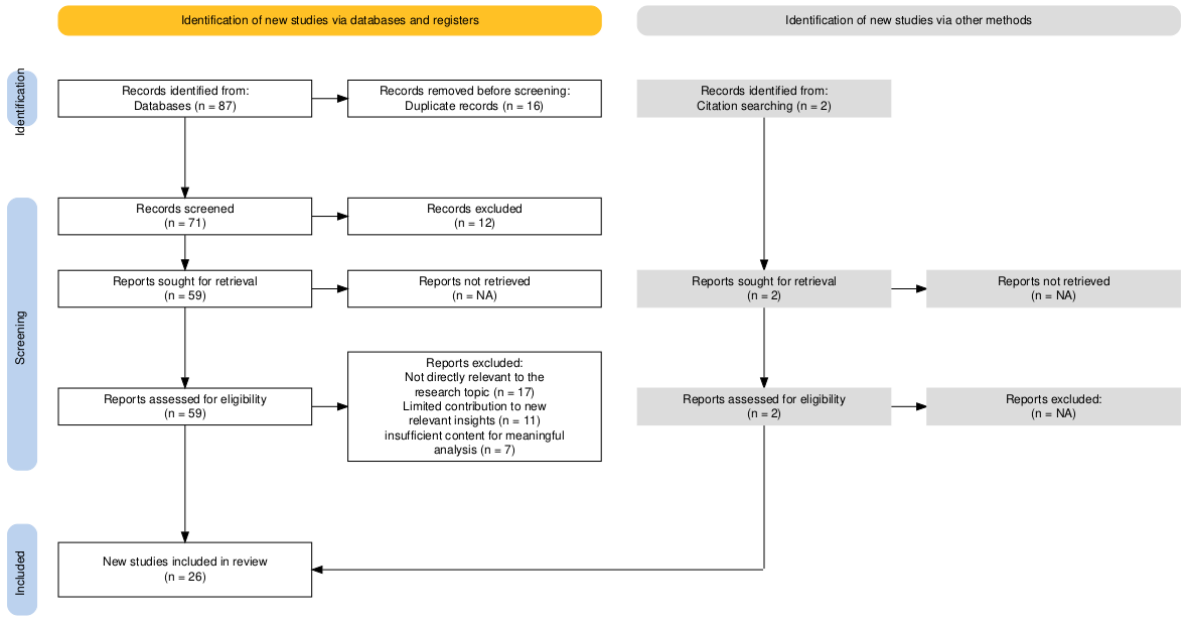

Figure 2: Identification of studies included in the review

The selected articles were imported into the NVivo qualitative data analysis tool for subsequent narrative analysis. The narrative analysis adopts a template analysis methodology, which augments grounded theory methods used in this analysis, i.e., open and axial coding, with a priori codes informed by literature and the inquiry in this research (Corbin and Strauss, 1990; King and Brooks, 2016). As such, the analysis started with the broad codes of "challenges of CTI sharing" and "opportunities of CTI sharing" and used open coding to fill in the details. A qualitative synthesis, presented hereafter, was undertaken to highlight current knowledge, emerging trends, and future research directions in CTI-sharing. Overall, this approach ensures that the study captures a comprehensive, evidence-based view of CTI-sharing in cross-domain contexts towards strengthening whole-of-society cyber resilience.

3. Challenges of Cross-Domain CTI Sharing

Despite the benefits of CTI sharing in enhancing collective cyber resilience, various challenges hinder its adoption and effectiveness. The following are the key challenges that have been identified from the literature review.

Cost

Financial limitations remain a critical barrier to CTI sharing, especially for small and mid-sized enterprises (SMEs) that struggle to allocate resources for dedicated threat intelligence programs. Establishing and maintaining CTI-sharing platforms demands significant investments in infrastructure, personnel, and ongoing operational costs, making participation difficult for organizations with constrained budgets (Dykstra et al., 2023).

Human resources challenges

Many organizations lack the necessary technical and human resources to effectively utilize and integrate CTI into their cybersecurity operations (Alaeifar et al., 2024). Many organizations lack the budget to recruit and retain in-house analysts, which weakens their ability to interpret shared intelligence effectively and respond to threats in real-time (Piazza et al., 2023). This talent gap limits participation in intelligence-sharing networks and reduces the overall effectiveness of collaborative cybersecurity efforts (Wagner et al., 2019) .

Workforce fatigue and skills shortages further complicate intelligence-sharing efforts. Security analysts are often overburdened with operational tasks, leading to burnout and high turnover rates, which disrupt the continuity of intelligence-sharing programs (Stojkovski et al., 2021). Additionally, CTI sharing relies heavily on tacit knowledge, which is often lost when experienced analysts leave an organization, creating gaps in intelligence analysis and dissemination (Jesus et al., 2024).

perational challenges

Another challenge is the sheer volume of shared intelligence. Security teams receive large amounts of data but lack efficient ways to filter and prioritize what is truly useful (Jesus et al., 2024). Without real-time feedback between intelligence providers and consumers, refining and verifying shared data becomes difficult, reducing its reliability in stopping threats before they spread (Valdés Ríos et al., 2024). Delays in updating intelligence also create blind spots, leaving organizations exposed to emerging cyber threats (Du et al., 2020).

Return on investment

For many organizations, the return on investment (ROI) for participation in CTI sharing is unclear, making it hard to justify the costs of subscription-based CTI sharing platforms or investments in automation and analytics tools. While government-funded cybersecurity initiatives, open-source intelligence-sharing platforms, and subsidized cybersecurity training programs exist, they often fail to cover the full range of expenses needed for effective intelligence-sharing adoption (Dykstra et al., 2023).

Financial liabilities

Concerns over potential financial liabilities further discourage participation in CTI sharing networks. Organizations fear penalties if shared intelligence is incomplete or misleading, making them hesitant to contribute to CTI-sharing networks (Sauerwein et al., 2024).

Reputational risks

The fear of exposing vulnerabilities discourages companies from fully engaging in intelligence-sharing networks, particularly when incidents could attract negative publicity (Piazza et al., 2023). In some cases, organizations practice "circumstantial sharing", selectively sharing threat intelligence only when it aligns with internal priorities or regulatory pressures rather than as a continuous practice (Nainna et al., 2024).

Legal challenges and Data privacy

Depending on the legal frameworks applicable in different jurisdictions, some organizations might not be inclined to share information about their cybersecurity posture and experiences which could expose them to legal scrutiny (Piazza et al., 2023). Further, some organizations struggle with interpreting and understanding legal obligations with regards to disclosures and CTI sharing in different relevant jurisdictions. For example, the General Data Protection Regulation (GDPR) and similar frameworks introduce additional restrictions, requiring firms to comply with stringent data protection rules before sharing intelligence (Ali et al., 2021).

Jurisdictional compliance

Differences in cybersecurity laws, compliance requirements, and data privacy policies make it difficult for organizations to share intelligence across borders. These challenges slow down collaboration and limit how much threat intelligence can be exchanged to improve global cybersecurity (Ali et al., 2022). Conflicting laws and regulations create uncertainty in CTI sharing. Different countries impose varied regulations, making it difficult for organizations to exchange threat data without legal risks (Alaeifar et al., 2024); (Sauerwein et al., 2024). Regulatory uncertainty further complicates the issue. Many organizations fear non-compliance with regional cybersecurity laws, making cross-border intelligence sharing difficult (Alaeifar et al., 2024).

Adversarial risks

Cybercriminals have been known to infiltrate intelligence-sharing networks to study detection techniques, identify weaknesses, and refine their attack methods (Jesus et al., 2024). If intelligence-sharing platforms lack robust verification and security controls, they can become a goldmine for threat actors, who exploit these insights to evade defences and launch more sophisticated attacks (Ma et al., 2023). At the same time, adversaries can exploit disclosed intelligence to refine attack strategies, increasing the risks associated with open information exchange (Jesus et al., 2024).

Competitive risks

Concerns about competition make many organizations hesitant to share CTI. Some fear that instead of strengthening collective security, their shared intelligence could be leveraged by competitors for strategic or financial gain, reducing their own security advantage (Piazza et al., 2023). This hesitation is especially strong in sectors where cybersecurity is seen as a competitive differentiator, making organizations reluctant to disclose insights that could expose their own security postures (Dykstra et al., 2023).

Free-riding and Lack of incentives to contribute

Another major challenge is free riding, where organizations consume shared intelligence but do not contribute back. This imbalance weakens CTI networks, leading to a lack of reciprocity and discouraging active participation (Dykstra et al., 2023). Without incentives to contribute and mechanisms to ensure fair contributions, intelligence-sharing platforms risk becoming one-sided, benefiting only those who extract value without adding to the collective pool of knowledge (Jesus et al., 2024).

Lack of trust

One of the biggest hurdles in CTI sharing is lack of trust. Many organizations hesitate to participate because they worry about data security, competition risks, and potential legal issues (Sauerwein et al., 2024). Sharing threat intelligence can feel risky, as revealing vulnerabilities might expose weaknesses that adversaries or competitors could exploit (Jesus et al., 2024).

Governance challenges

Decentralized intelligence-sharing models offer greater transparency and trust, but governance and control issues make them difficult to manage (Zhang et al., 2022). Organizations struggle to balance control and accessibility, ensuring that sensitive intelligence remains protected while still enabling effective collaboration. Without strong governance structures, the risks of misuse, unauthorized access, and data leaks increase, leading some organizations to hesitate in adopting decentralized models.

Technology interoperability and Standard incompatibility

Without standardized data formats, automated threat processing becomes difficult, forcing security teams to rely on manual methods that are slow and error-prone (Jesus et al., 2024). While structured formats like STIX and TAXII help streamline sharing, in general, standards and technology differences in make it hard for organizations to exchange intelligence seamlessly (Alaeifar et al., 2024).

Organizational barriers

Differences in security maturity, trust issues, and system compatibility make smooth collaboration difficult (Jesus et al., 2024).

Socio-cultural differences

Cultural and language differences also impact collaboration. Since CTI sharing spans multiple sectors and geographic regions, misunderstandings and inconsistent threat interpretations can hinder cooperation (Stojkovski et al., 2021). Some organizations struggle with English-based intelligence-sharing platforms, while others have differing perceptions of cyber threats based on regional security environments.

Technical developments and emerging technologies

Automation gaps in CTI processing and sharing create inefficiencies. Without automated threat processing, organizations rely on manual workflows, which take time and increase the risk of human error (Valdés Ríos et al., 2024). The need for real-time analysis is growing, but many current systems lack the capability to integrate shared intelligence quickly and accurately (Du et al., 2020).

Data classification and sensitivity

CTI sharing in high security contexts, such as those involving national security and military stakeholders, must ensure that classified or sensitive data reaches only authorized personnel while preventing leaks or misuse (Przybyszewski et al., 2024). Strong security measures, trust mechanisms, and controlled access policies are necessary to maintain both security and operational efficiency. Finding the right balance between collaboration and secrecy can be a challenge.

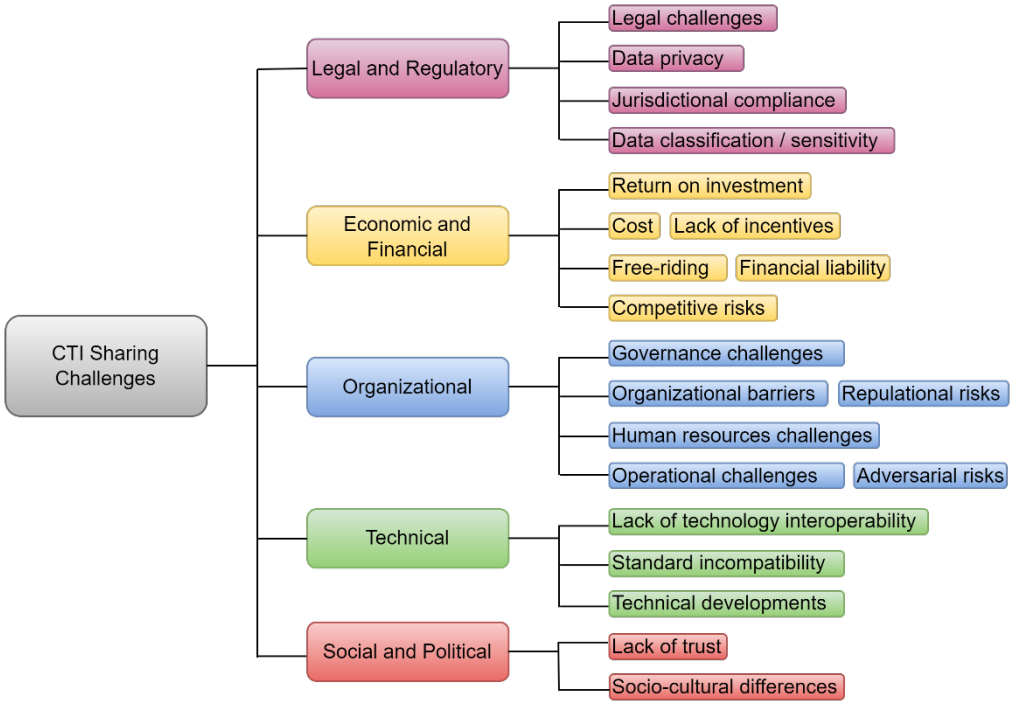

Figure 3: Initial taxonomy of (cross-domain) CTI sharing challenges

An initial taxonomy (Figure 3) of the challenges of cross-domain CTI sharing has been formulated based on the high-level classification into legal and regulatory, economic and financial, organizational, technical, and social and political challenges. While these are clustered into distinct categories, some of these co-occur across categories and can be closely linked. For example, the human resource challenges under organizational challenges are closely related to and interact with the cost challenges under the economic and financial category.

These challenges identified above continue to hinder the effectiveness of cross-domain CTI sharing and to hamper efforts towards whole-of-society cyber resilience. However, efforts to improve collaboration and coordination within the cybersecurity ecosystem, including through improved CTI sharing, continue to advance around the world. Further, despite these challenges, opportunities for enhancing cross-domain CTI sharing remain.

4. Discussion and Opportunities for Cross-Domain CTI Sharing

One of the underlying challenges in cross-domain CTI sharing is that of lack of trust between different participating stakeholders. To tackle this, experts suggest trust-building methods like cryptographic assurance models and federated risk assessments. These help make data sharing more secure and reliable (Zhang et al., 2022). Another approach is reputation-based verification, where shared intelligence is rated for accuracy and reliability before being widely distributed (Piazza et al., 2023). While these strategies help, building trust remains a slow process and it is not just about security; it also requires a shift in people's thinking patterns, where organizations see intelligence sharing as a collective defence strategy rather than a risk (Piazza et al., 2023).

Organizations need more confidence that shared intelligence is accurate, useful, and won't be misused. New methods and policies are still needed to address these concerns and encourage broader participation in CTI sharing. Some of the approaches that can support the safe, secure, and trusted sharing of CTI data include privacy-preserving technologies, using social network analysis approaches to understand intelligence flows, developing scalable and flexible sharing models that enforce strong cybersecurity at every level and maintaining

the right balance between security, accessibility, and collaboration (Piazza et al., 2023; Sleem and Elhenawy, 2022).

To improve operational efficiency, organizations need better automation and standardization in CTI-sharing platforms. Adopting consistent formats across different systems to help reduce compatibility issues (Alaeifar et al., 2024). Machine learning tools can also help process intelligence faster, filtering out noise and highlighting the most critical threats (Jesus et al., 2024). Blockchain-based verification methods add another layer of trust, ensuring that shared intelligence remains accurate and tamper-proof (El-Kosairy et al, 2024). With these improvements, organizations can make CTI-sharing more reliable, actionable, and effective in strengthening cybersecurity.

Addressing the economic and financial challenges, cost-sharing models and industry collaboration could help SMEs access intelligence-sharing networks without bearing the full financial burden. Establishing public-private partnerships, financial incentives, and pooled cybersecurity resources would support broader participation while ensuring that smaller organizations can still benefit from shared intelligence without excessive upfront costs (Alaeifar et al., 2024). Additionally, developing targeted subsidized training programs for cybersecurity professionals would help bridge the talent gap and enable more effective use of shared intelligence within the industry (Piazza et al., 2023). Besides these formalized partnership and collaborations models, decentralized models for CTI sharing are gaining attention to further address the trust and security concerns (Zhang et al., 2022). By decentralizing CTI-sharing, organizations reduce reliance on central authorities and lower the risks of data monopolies or single points of failure (Alaeifar et al., 2024). Despite these benefits, decentralized CTI-sharing models are not without challenges, including delays in real-time intelligence sharing, and legal uncertainties which make widespread adoption difficult (Ainslie et al., 2023). To address these issues, researchers are exploring hybrid models that combine the benefits of decentralized systems with faster and more efficient verification methods (Wen et al., 2024).

Another collaboration approach is through open-source and community-driven CTI platforms, which provide an affordable way for organizations with limited cybersecurity resources to participate in intelligence sharing. These platforms lower the barriers for smaller entities to access valuable threat information, fostering a broader and more inclusive defence network (Jesus et al., 2024). However, the reliability of shared intelligence remains a major concern. Without proper validation, incorrect or misleading threat data can weaken security efforts rather than strengthen them. To address this, reputation-based verification models help assess the credibility of shared intelligence before organizations act on it. Blockchain-based incentivized participation frameworks can also encourage fair, more accurate, and responsible contributions to intelligence-sharing initiatives while discouraging free-riding (Nguyen et al., 2022). While these solutions improve trust and accuracy, maintaining high-quality intelligence in an open-sharing environment still presents ongoing challenges.

Around the world some of these solutions are being adopted to address the challenges of cross-domain CTI sharing. It is imperative that effective collaboration and partnership frameworks are established, interoperable standards and technologies are developed, and initiatives established to enable participation of broad sectors of society towards collective cyber resilience.

5. Conclusion

This research undertook an extensive systematic literature review to examine the challenges of cross-domain CTI sharing and why it remains a difficult challenge despite its importance in strengthening collective cyber resilience. The research found that factors, such as trust concerns, differences in organizational policies and regulations, and interoperability gaps, which can be clustered into legal and regulatory, economic and financial, organizational, technical, and social and political factors, continue to hamper effective and seamless collaboration. A taxonomy that classifies and characterises these cross-domain CTI sharing challenges, has been proposed to help researchers and practitioners better understand these challenges and develop relevant solutions.

Organizations hesitate to share intelligence, fearing misuse or exposure, while country-specific policies complicate the process. Even with frameworks like STIX and TAXII improving standardization, technical barriers persist, limiting real-time intelligence exchange. Without effective CTI sharing with accuracy in quality and timelines, its potential impact weakens at organizational levels. To make sharing work, trust must grow, regulatory alignment must improve, and technology needs to keep up with evolving threats.

As future work, stakeholders from public and private sectors could be interviewed to gather insights that support the development of a framework for cross-domain CTI sharing aimed at enhancing whole-of-society resilience.

This framework could then be further developed and validated through engagement with stakeholders and other participants to assess its relevance and inform practices that strengthen cyber resilience across society.

AI Declaration: The writing, analysis, and development of this paper were carried out entirely by the author(s) without the use of AI tools.

Ethics Declaration: This research did not involve human participants, personal data collection, or any activities requiring ethical review. As a result, no ethical clearance was necessary, and none was sought.

References

Ainslie, S., Thompson, D., Maynard, S., Ahmad, A., 2023. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Comput. Secur. 132, 103352. https://doi.org/10.1016/j.cose.2023.103352

Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., Foo, E., 2024. Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. J. Inf. Secur. Appl. 83, 103786. https://doi.org/10.1016/j.jisa.2024.103786

Ali, H., Ahmad, J., Jaroucheh, Z., Papadopoulos, P., Pitropakis, N., Lo, O., Abramson, W., Buchanan, W.J., 2022. Trusted Threat Intelligence Sharing in Practice and Performance Benchmarking through the Hyperledger Fabric Platform. Entropy 24, 1379. https://doi.org/10.3390/e24101379

Ali, H., Papadopoulos, P., Ahmad, J., Pitropakis, N., Jaroucheh, Z., Buchanan, W.J., 2021. Privacy-preserving and Trusted Threat Intelligence Sharing using Distributed Ledgers. https://doi.org/10.48550/arXiv.2112.10092

Arachchilage, N.A.G., Namiluko, C., Martin, A., 2013. A taxonomy for securely sharing information among others in a trust domain, in: 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). pp. 296–304. https://doi.org/10.1109/ICITST.2013.6750210

Chalkias, I., Yucel, C., Mallis, D., Rajamaki, J., De Vecchis, F., Hagstrom, P., Katos, V., 2024. An Empirical Evaluation of Cyber Threat Intelligence Sharing in the ECHO Early Warning System, in: Tagarev, T., Stoianov, N. (Eds.), Digital Transformation, Cyber Security and Resilience. Springer Nature Switzerland, Cham, pp. 23–40. https://doi.org/10.1007/978-3-031-44440-1_3

Corbin, J.M., Strauss, A., 1990. Grounded theory research: Procedures, canons, and evaluative criteria. Qual. Sociol. 13, 3–21. https://doi.org/10.1007/BF00988593

Du, L., Fan, Y., Zhang, L., Wang, L., Sun, T., 2020. A Summary of the Development of Cyber Security Threat Intelligence Sharing. Int. J. Digit. Crime Forensics IJDCF 12, 54–67. https://doi.org/10.4018/IJDCF.2020100105

Dykstra, J., Gordon, L.A., Loeb, M.P., Zhou, L., 2023. Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments. J. Cybersecurity 9, tyad003. https://doi.org/10.1093/cybsec/tyad003

El-Kosairy et al, 2024. Transforming Cybersecurity: Leveraging Blockchain for Enhanced Threat Intelligence Sharing | Request PDF. ResearchGate. https://doi.org/10.18280/ijsse.140412

Jesus, V., Bains, B., Chang, V., 2024. Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence. IEEE Trans. Eng. Manag. 71, 6854–6873. https://doi.org/10.1109/TEM.2023.3279274

King, N., Brooks, J., 2016. Template Analysis for Business and Management Students 1–120.

Ma, X., Yu, D., Du, Y., Li, L., Ni, W., Lv, H., 2023. A Blockchain-Based Incentive Mechanism for Sharing Cyber Threat Intelligence. Electronics 12, 2454. https://doi.org/10.3390/electronics12112454

Nainna, M.A., Bass, J.M., Speakman, L., 2024. Factors Amplifying or Inhibiting Cyber Threat Intelligence Sharing, in: Papadaki, M., Themistocleous, M., Al Marri, K., Al Zarouni, M. (Eds.), Information Systems. Springer Nature Switzerland, Cham, pp. 204–214. https://doi.org/10.1007/978-3-031-56481-9_14

Newman, M., Gough, D., 2020. Systematic Reviews in Educational Research: Methodology, Perspectives and Application, in: Zawacki-Richter, O., Kerres, M., Bedenlier, S., Bond, M., Buntins, K. (Eds.), Systematic Reviews in Educational Research: Methodology, Perspectives and Application. Springer Fachmedien, Wiesbaden, pp. 3–22. https://doi.org/10.1007/978-3-658-27602-7_1

Nguyen, K., Pal, S., Jadidi, Z., Dorri, A., Jurdak, R., 2022. A Blockchain-Enabled Incentivised Framework for Cyber Threat Intelligence Sharing in ICS. Presented at the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 261–266. https://doi.org/10.1109/PerComWorkshops53856.2022.9767226

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., Moher, D., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. https://doi.org/10.1136/bmj.n71

Piazza, A., Vasudevan, S., Carr, M., 2023. Cybersecurity in UK Universities: mapping (or managing) threat intelligence sharing within the higher education sector. J. Cybersecurity 9, tyad019. https://doi.org/10.1093/cybsec/tyad019

Przybyszewski, M., Gierszal, H., Tyczka, P., Kruszyński, A., Skoufis, C., Pure, I., Pierret, F., 2024. HERMES DXP: An Approach to Military and Non-military Cyber Threat Intelligence Sharing, in: Fujita, H., Cimler, R., Hernandez-Matamoros, A., Ali, M. (Eds.), Advances and Trends in Artificial Intelligence. Theory and Applications. Springer Nature, Singapore, pp. 68–79. https://doi.org/10.1007/978-981-97-4677-4_7

Sauerwein, C., Wenzl, C., Breu, R., 2024. Uncovering Critical Resources and Factors Influencing the Use of Threat Intelligence Sharing Platforms.

Sleem, A., Elhenawy, I., 2022. Enhancing Cyber Threat Intelligence Sharing through a Privacy-Preserving Federated Learning Approach. J. Cybersecurity Inf. Manag. 51–59. https://doi.org/10.54216/JCIM.090205

Stojkovski, B., Lenzini, G., 2021. A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). pp. 324–330. https://doi.org/10.1109/CSR51186.2021.9527903

Stojkovski, B., Lenzini, G., Koenig, V., Rivas, S., 2021. What's in a Cyber Threat Intelligence sharing platform? A mixed-methods user experience investigation of MISP, in: Proceedings of the 37th Annual Computer Security Applications Conference, ACSAC '21. Association for Computing Machinery, New York, NY, USA, pp. 385–398. https://doi.org/10.1145/3485832.3488030

Tavakolifard, M., Almeroth, K.C., 2012. A Taxonomy to Express Open Challenges in Trust and Reputation Systems. J. Commun. 7, 538–551. https://doi.org/10.4304/jcm.7.7.538-551

Valdés Ríos, V., Zaidi, F., Cavalli, A.R., Rego, A., 2024. Towards the adoption of automated cyber threat intelligence information sharing with integrated risk assessment, in: Proceedings of the 19th International Conference on Availability, Reliability and Security, ARES '24. Association for Computing Machinery, New York, NY, USA, pp. 1–9. https://doi.org/10.1145/3664476.3670444

Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E., 2019. Cyber threat intelligence sharing: Survey and research directions. Comput. Secur. 87, 101589. https://doi.org/10.1016/j.cose.2019.101589

Wagner, T.D., Palomar, E., Mahbub, K., Abdallah, A.E., 2018. A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. Secur. Commun. Netw. 2018, 9634507. https://doi.org/10.1155/2018/9634507

Wen, B., Xing, X., Wang, G., 2024. RTB-RM: A Blockchainenabled System for Reliable and Transparent CTI Sharing with Multidimensional Reputation Model, in: 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Presented at the 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 1399–1404. https://doi.org/10.1109/CSCWD61410.2024.10580557

Zhang, X., Miao, X., Xue, M., 2022. A Reputation-Based Approach Using Consortium Blockchain for Cyber Threat Intelligence Sharing. Secur. Commun. Netw. 2022, 7760509. https://doi.org/10.1155/2022/7760509