CTI Sharing Practices and MISP Adoption in Finland's Critical Infrastructure Protection

Katja Henttonen[1,2] and Jyri Rajamäki[1]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]University of Jyväskylä, Jyväskylä, Finland

katja.henttonen@laurea.fi
katja.m.henttonen@student.jyu.fi
jyri.rajamaki@laurea.fi

Abstract: Cyber Threat Intelligence (CTI) sharing is crucial for safeguarding organisations and securing national critical infrastructure. This study delves into the CTI-sharing practices of large, safety-critical Finnish organisations, with a specific interest in the deployment and potential of the Malware Information Sharing Platform (MISP). We gathered insights through qualitative interviews with cybersecurity experts from key sectors: energy, healthcare, and transportation. Our findings reveal that a significant proportion of regional CTI data is still shared through manual methods such as email and chat. While these systems are generally viewed positively, they are also understood to be prone to delays and inaccuracies. The interest in utilising MISP is rising in Finland, yet its implementation is still in the nascent stages. Organisations are looking towards the National Cyber Security Center to lead the establishment of a national MISP instance. The benefits of adopting a national MISP framework could be further amplified by organisations joining Europewide industry specific MISP instances or leveraging MISP to share threat intelligence with their supply chain partners. However, challenges remain, particularly in balancing threat data sharing with European data protection laws, motivating community contributions, and standardising CTI-sharing tools and practices within a country.

Keywords: Cyber Threat Intelligence, CTI Sharing, Critical Infrastructure, MISP, Finland

1. Introduction

In cybersecurity, sharing Cyber Threat Intelligence (CTI) is key to protecting organisations and national infrastructures. While global CTI repositories are widely used, the specific security needs of countries, shaped by their unique geopolitical, regulatory, and industry-related factors, call for a closer look at how CTI sharing works on a local level. This is especially true in Finland, where the dynamics of CTI sharing within critical sectors like energy, healthcare, and transportation remain largely unexplored despite their critical importance to the country's security and resilience.

This study contributes to the field by examining the state of CTI sharing in Finland's critical infrastructure, focusing on the Malware Information Sharing Platform (MISP). While the transformative potential of MISP in revolutionising national-scale CTI sharing is acknowledged, its practical deployment and efficacy within the unique Finnish context have not yet been systematically studied. To address this knowledge gap, our research is driven by two main questions:

1. How do critical infrastructure organisations in Finland receive and share Cyber Threat Intelligence (CTI)?
2. What are the current MISP deployment status and potential usage scenarios in these organisations?

Employing a qualitative research approach, this inquiry involved engaging cybersecurity experts from key sectors through six in-depth interviews. These conversations, supplemented by document analysis, provide insights into the complexities of CTI sharing in Finland, especially the usage and potential of MISP.

The structure of the paper is as follows. The second section provides background information, introduces key terms, and reviews CTI sharing and MISP literature. The third section elaborates on this study's data collection and analysis methodology. The fourth section presents the research results, first offering an overview of CTI-sharing practices within Finland's critical infrastructure and then delving into the status and potential of MISP adoption. Discussions and conclusions close the paper.

2. Literature Review

This section provides a concise overview of relevant literature. The first subsection covers general literature on CTI sharing. The second subsection explores the automation of CTI sharing and introduces the MISP platform.

2.1 Cyber-Threat Intelligence (CTI) Sharing

Cyber-threat intelligence (CTI) is knowledge about current or potential cyber threats, encompassing aspects like malicious actors, attack methods, vulnerabilities, and their impacts. Li et al. (2017) offer a more detailed definition, describing CTI as evidence-based knowledge that includes context, mechanisms, indicators, implications, and actionable advice about existing or emerging threats. Abu (2018) highlights that the core objective of CTI is to empower organisations to tackle cyber threats strategically, operationally, and tactically.

Actionable CTI refers to cyber threat information that provides specific details for effectively detecting, preventing, or responding to threats (Wagner et al., 2019). Several criteria for actionable CTI have been proposed (ibid). Influential criteria outlined by the European Union Agency for Cybersecurity (Pawlinski et al., 2015) include relevance (ensuring the CTI directly applies to the system at risk), timeliness (sharing current information promptly), accuracy (informing stakeholders on vulnerabilities post-analysis), completeness (covering all threat aspects for adequate response), and ingestibility (the organisation's ability to integrate and apply CTI within its systems). The criteria help ensure that CTI is informative and practical, enabling organisations to mitigate and respond to cyber threats effectively.

Cyber-threat intelligence sharing (CTIS) is the process of exchanging CTI among different entities, such as security teams, business partners, vendors, customers, regulators, and industry peers (Jonsson et al., 2016). Following Vazquez et al. (2011), Wagner et al. (2019) outline three CTI sharing models: Peer-to-Peer, where organisations share CTI directly without intermediaries; Peer-to-Hub, involving a central hub that collects, processes, and disseminates CTI to stakeholders; and a Hybrid model that blends direct sharing between entities with the centralised management and broad reach of a hub.

CTI sharing has demonstrated its efficacy in mitigating cyber-attacks, preventing potential ones, and quickly pinpointing attackers and their tactics (Tounsi, 2019). Its benefits, including cost savings and improved cybersecurity quality, are widely acknowledged in different contexts (Skopik et al., 2017; Zibak & Simpson, 2019). This recognition has led to a growing trend among organisations to participate actively in CTI sharing (Wagner et al., 2019).

While there is an increase in global and industry-specific CTI-sharing initiatives, national CTI-sharing remains prevalent (Wagner et al., 2019). CTI-sharing landscapes can differ markedly across countries due to their unique geopolitical dynamics, local regulations, and industry-specific contexts (Fransen & Kerkdijk, 2017). However, research focusing on national CTI-sharing ecosystems remains sparse, with only a few case studies (e.g., Fransen & Kerkdijk, 2017; Amanowicz, 2020) addressing this area.

2.2 CTI Sharing Automation and Malware Information Sharing Platform (MISP)

With the increasing volume of threat data, automating Cyber Threat Intelligence (CTI) sharing is becoming critical (Haque & Krishnan, 2021; Wagner, 2019). Traditional methods like email are inefficient, leading to delays and information overload (Kampanakis, 2014). Despite the recognised importance of automated CTI sharing (Piotr & Pawliński, 2014; Wagner, 2019; Haque & Krishnan, 2021), challenges persist in ensuring data accuracy and algorithm sophistication, which is necessary to avoid false positives or missed threats (Wagner, 2019). Additionally, concerns about privacy legislation are significant (Schwartz et al., 2016; Sullivan, 2017).

Various platforms have been developed to improve threat intelligence sharing through automation and standardisation (Stojkovski et al., 2021). These platforms, while varying in capabilities, are essential for efficient Cyber Threat Intelligence (CTI) sharing among organisations and have been widely adopted due to their demonstrated benefits (Dandurand & Serrano, 2023; Bauer et al., 2020; De Melo e Silva et al., 2020). Notable platforms include MISP, OTX (Open Threat Exchange), OpenCTI, and ThreadQ, each offering unique features and strengths (Bauer et al. 2020, De Melo e Silva et al. 2020).

Evolving from its initial purpose of malware information sharing within military circles, MISP has expanded its scope to encompass a wide range of cybersecurity intelligence (Wagner et al., 2016; Stojkovski et al., 2021) and even other domains like dissemination of COVID information (Ramallo-Gonzále, 2021). With the backing of the Computer Incident Response Center Luxembourg (CIRCL) and the European Union (MISP 2024), MISP operates as an open-source collaborative platform, serving a diverse user base ranging from NATO agencies to private sector entities (Stojkovski et al., 2021). Organisations can join established MISP communities or establish their own MISP instances, which function as centralised or decentralised servers within a network to enable efficient CTI exchange (Stojkovski et al., 2021).

3. Methodology

We opted for a fully qualitative research approach involving content analysis of semi-structured interviews and relevant business documents. This approach allows for a comprehensive exploration of the multifaceted nature of CTI sharing and is well-suited to this study's exploratory nature.

We initially reached out to 12 organisations meeting specific criteria: operating in Finland's energy, healthcare, or logistics/transport sectors, ranking among the country's largest in their respective fields, headquartered in Finland, and identified by the Finnish National Emergency Supply Agency as critical for national supply security. Eventually, cybersecurity directors or managers from six critical infrastructure organisations agreed to participate. Please refer to **Table 1** for a summary of the informants and their organisations. Following our commitment to confidentiality, we maintain the anonymity of the interviewees and their organisations.

Table 1: Summary of interviewees

Abbreviation	Sector	Position	Time of interview
Interviewee A	Energy	Executive Level	December 2023
Interviewee B	Energy	Executive Level	December 2023
Interviewee C	Transportation/Logistics	Executive Level	December 2023
Interviewee D	Transportation/Logistics	Managerial Level	September 2023
Interviewee E	Healthcare	Managerial Level	November 2023
Interviewee F	Energy	Managerial Level	November 2023

The semi-structured interviews covered the following themes: current CTI sharing practices and their effectiveness, existing and potential use cases of MISP, and the perceived benefits and challenges in MISP adoption. The discussions aimed to capture insights not only from the organisational perspective but also in the broader national context. All interviews were conducted remotely and took about 45 minutes on average. Most were recorded and subsequently transcribed for analysis. In two cases, we relied on detailed notes due to the interviewees' preference not to record or automatically transcribe their responses. We corroborated and cross-referenced the evidence collected during interviews by examining relevant business documents related to CTI sharing in the studied organisations or their respective industries. These documents were provided to us by our informants.

Conventional content analysis (Hsieh & Shannon, 2005) was used to approach the interpretation of data. It is particularly effective in research where theoretical knowledge is limited, as it allows themes to emerge from the data instead of being imposed by existing theories. Template Analysis (King 2012) was employed as a practical technique to analyse the interview transcripts and the business documents. It involves developing a coding 'template' that represents themes identified in the data. The process begins with initial codes, which are then refined and organised into higher-order themes as the analytic process proceeds (King, 2012). This method is flexible and allows for modifying the template as new data is incorporated, making it particularly suitable for data-driven research where themes evolve during the analysis.

4. Results

This section presents out findings in two main parts. First, we examine how CTI is shared among Finland's critical infrastructure organisations. Then, we explore how MISP is being adopted and its potential benefits and challenges for the future.

4.1 Current CTI Sharing Practices in Finnish Critical Infrastructure

Finnish critical infrastructure follows a hybrid CTI sharing model involving centralised information exchange through a hub, the National Cyber Security Centre Finland (NCSC-FI), and direct organisational exchanges. Information happens formally and informally, using various traditional tools like email, instant messaging, and meetings. Figure 1 gives an overview of the CTI sharing network by Finnish critical infrastructure organisations (CIOs), as outlined by the informants. The details of these exchanges are described in the following sections.

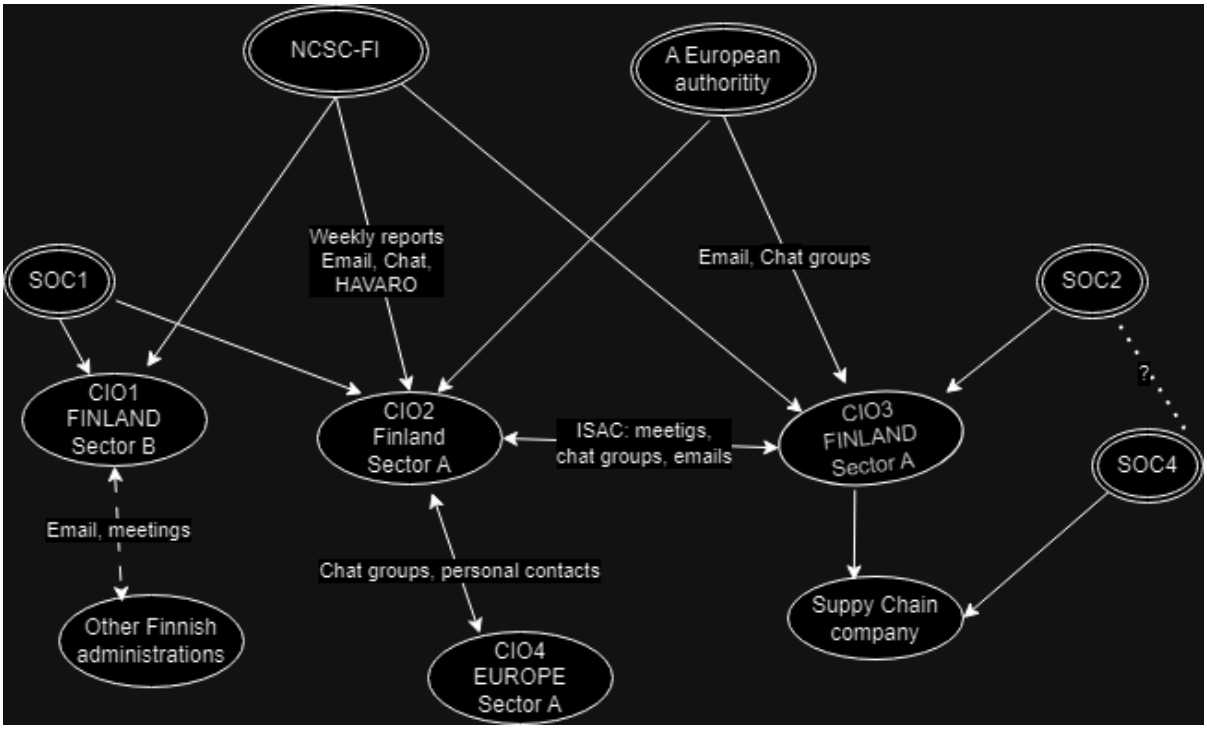

Figure 1: CTI sharing network around Finnish CIOs

4.1.1 Information Exchange with Hubs

National Cyber Security Centre Finland (NCSC-FI) operates under the Finnish Transport and Communication Agency (Traficom). It is a key information hub for critical sector organisations, disseminating cyber threat information primarily through traditional means like email and weekly reports. The CTI shared by NCSC-FI was highly appreciated due to its regional specificity. For example, interviewee A said, "*The threat information reserved by Microsoft and these other American platforms is global. From there, one can observe major trends, but it does not tell what is currently happening in the Finnish context specifically, nor is it very detailed. In that sense, the information from the National Cyber Security Centre is very important to us*.".

Some participants highlighted that while information on NCSC-FI mailings and reports was valuable, there was room for improvement in terms of specificity. They emphasized the importance of detailed and actionable threat information, stressing that it should enable a swift response, e.g., by allowing them to provide technical identifiers to their SOC (Security Operations Center) for immediate checks and actions. Informant C said: "*They [NCSC-FI] provide really good information, especially about certain vulnerabilities and others, but then it can be general."* Industry-specific European supervisory authorities served as a secondary CTI hub for Finnish critical organisations and sometimes provided more concrete alerts than the NCSC-FI. Informant C continued: "*They [a European authority] share information at a level where, for example, they notice an organisation's data being sold on a Dark Web marketplace and then warn others that such an attack is underway, or they alert about ongoing DDoS attacks at specific locations based on mentions in Telegram"*.

NCSC-FI is also the main producer of the HAVARO service, which detects serious cybersecurity threats targeting Finnish organisations and issues warnings. It is based on automatically monitoring the data traffic through sensors, but humans analyse the findings before the target organisation is contacted. Notably, while NCSC-FI collects a substantial amount of threat data, much of it is not shared directly due to data protection considerations. However, organisations can still access it through HAVARO identifiers. Informant C says: "*Currently, organisations like Traficom [=NCSC-FI] may collect a lot of threat information but do not actively share it with others [due to data protection considerations]. However, as HAVARO users, we receive their identifiers, essentially the threat information they do not share directly with us*."

Most organisations we interviewed utilise commercial Security Operations Centers (SOCs) to manage their security operations. These commercial SOCs collaborate with NCSC-FI in delivering the HAVARO service and function as a central 'hub' or repository for their respective client bases, facilitating the sharing of Cyber Threat

Intelligence (CTI) among clients. However, due to the competitive landscape among commercial SOC providers, genuine information sharing between different SOCs is reportedly not a prevalent practice.

4.1.2 Peer-to-Peer Information Sharing

Instructure critical organisations (CIOs) in Finland share CTI in so-called ISAC groups (the abbreviation stands for Information Sharing and Analysis Center), which are maintained and facilitated by NCSC-FI. The industry-specific groups include one or more ISAC groups for energy, transportation, and healthcare sectors. Within these groups, organisations share CTI in quarterly meetings, via secure email, and through instant messaging services like Signal or RocketChat when classification permits. Access to ISAC groups is limited to major critical infrastructure companies that appoint their own representatives, and informal rules of the group enforce reciprocity, saying that if you want to be a member and receive CTI, you must also share your own CTI.

Information disseminated via ISAC-related chat groups typically focuses on detected cyberattack attempts or vulnerabilities within a company, serving as alerts for others to investigate potential similar issues. These groups occasionally facilitate the sharing of solutions as well. Regarding the relevance of the shared information, informant B provided an estimate, suggesting that approximately one-fifth of the messages resulted in actionable responses. He explained, *"In about four out of five cases, we can independently determine that no action is needed. We either confirm that the situation is under control or does not pertain to us. However, in the remaining twenty percent, we conduct further reviews and may share information. On the administrative side, users are often informed on appropriate actions or precautions*."

CIOs also exchanged CTI with domestic authorities, such as the police's cybersecurity department, the border security agency, and regulatory authorities. These exchanges were generally viewed positively but were not without challenges. For example, informant B mentioned instances where the organisation had to act as an intermediary, relaying information between different authorities during cybersecurity incidents.

Additionally, interviewees mentioned the importance of providing thread intelligence to non-critical supply chain partners who lack access to CTI channels but may handle sensitive data. In addition to informing their supply chain partners independently, some organisations sought to leverage their client influence to mandate direct information sharing between their SOC provider and partner companies' SOC providers.

4.2 The Status and Potential of MISP Deployment in Finland

None of the interviewed organisations – and based on our secondary data, this also applies to all contacted organisations that declined to participate – have fully implemented the MISP platform. However, there is a notable interest in adopting MISP, with some organisations having either decided to deploy it or have already initiated the process. **Figure 2** shows the organisations represented by our informants that are placed on adopting MISP (refer to Table 1 in Section 3 for background information).

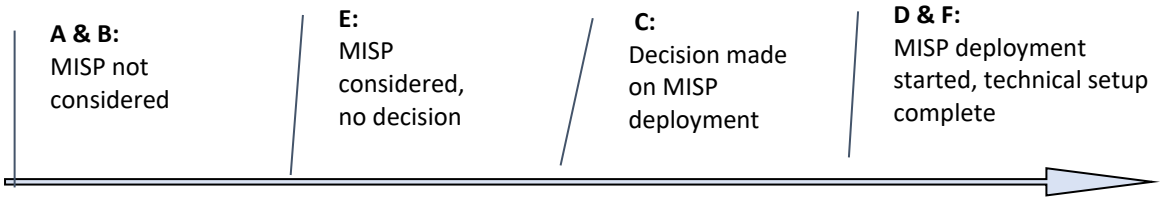

Figure 2: Status of MISP adoption in Finnish CIOs

Those informants whose organisations had considered MISP or taken steps towards deployment emphasised the advantages of the MISP system over the current email and chat-based CTI exchange systems. They emphasised MISP's capability for real-time CTI sharing, reducing delays. For example, Informant E explained:" *Whenever we start threat hunting and find something actionable, it takes time. In any case, it takes a long time before we can share it with other organisations. […] If all organisations were connected to MISP, each organisation would instantly receive the information, eliminating unnecessary delays*."

Some informants also emphasised MISP's ability to provide access to structured data, facilitating automation for prompt security updates. Informant F gave an example*: "For instance, when we receive information through MISP, we could automatically use the identification details, like updating firewall rules or other security measures. If you inform someone via email, it is manual work at every endpoint where I inform 1000 parties, and each person handles it manually. […] With MISP, the information becomes immediately actionable, and you can*

do whatever you want, even automate it". They acknowledged potential challenges in automating threat responses but stressed the importance of MISP in making it possible when appropriate.

While recognising the advantages of MISP, informants expressed strong reservations about the possibility of widespread MISP adoption in Finland without NCSC-FI assuming a leadership role. Their leadership was seen as instrumental in building trust and ensuring broader participation. Informants C and F strongly called for an approach in which NCSC-FI would serve as the central authority, administrating a MISP instance and providing it as a (preferably free) service to CIOs. Informant C said: "*If we get what everyone dreams and asks for from Traficom [NCSC-FI], then they would be a government authority that either builds or implements MISP, so then these critical sector organisations […] could join that MISP"*. No other organisation than NCSC-FI was seen as well-positioned to administrate the national MISP instance. The idea was not new, as informant F noted: "*We see that there would be much use for such a tool [MISP]. Discussions about this have been ongoing for several years, but we have not seen any concrete steps taken, for example, from Traficom*'s [NCSC-FI] *side*."

Among the organisations interviewed, the national MISP instance maintained by NCSC-FI, as described earlier, emerged as the most widely discussed and desired usage scenario. It was envisioned to have sector-specific subgroups and work in parallel with existing ISAC-group collaborations, offering more real-time and actionable threat information than email or chat. In addition to the national MISP, two other usage scenarios were discussed. Some organisations expressed interest in joining MISP instances provided as a service by European administrations within their respective industries. Furthermore, some contemplated the possibility of maintaining their own MISP groups to share threat information with their supply chain partners. These three MISP instances relevant to Finnish CIOs are summarised in **Table 2**. Global and open threat data feeds in MISP were not perceived as equally appealing. For example, informant D noted that they often contain excess information and noise, making it challenging to discern the relevant data amid the clutter.

Table 2: Envisioned and Existing MISP Instances relevant to Finnish CIOs

	Administrator	**Members**	**Focus**	**Status**
Finnish National MISP	NCSC-FI / Traficom	Critical infrastructure organisations in Finland	Sharing and collaborating on regional cybersecurity threats within Finland.	Envisioned, not yet operational
Supply Chain MISP	A Finnish infrastructure-critical organisation	Supply chain partners	Enhancing supply chain cybersecurity and sharing threat information among partners.	Envisioned, not yet implemented by interviewed companies
European Industry-Specific MISP	A relevant European administration	Large organisations in specific industries	Sharing cybersecurity threats within specific industries (e.g., electricity transfer or maritime) on a European scale	Already established in many industries.

Informants elaborated on several challenges in adopting MISP within the Finnish critical sector. To make such a solution valuable and sustainable, enough organisations in Finland must adopt MISP and actively use it to contribute thread data. Even if the service were free, effectively utilising MISP would necessitate acquiring specific skills and resources, which could prove challenging, especially for certain public sector organisations, as highlighted by informant E. Some informants stressed the importance of mechanisms to ensure active community participation, such as making reciprocal sharing a requirement for membership or enacting legislation mandating threat information sharing in specific cases.

The perceived reluctance of the National Cyber Security Centre Finland (NCSC-FI) to spearhead the implementation of MISP was attributed, in part, to concerns surrounding GDPR (General Data Protection Regulation). Classifying dynamic IP addresses as personal data subject to GDPR can create obstacles to sharing detailed and specific threat data within MISP groups. Informants also highlighted differing interpretations of GDPR across European countries, with Finland and Germany cited as examples of nations with particularly strict interpretations. Informant D emphasised that while GDPR facilitates data sharing more readily within the public sector, it poses greater challenges when sharing between the public and private sectors. Furthermore, other regulatory hurdles, particularly those pertaining to publicly traded companies, were identified as potential impediments to wider MISP use. Specifically, concerns were raised regarding classifying threat information as material non-public information under securities laws.

5. Discussion

Due to a limited number of interviews, the findings may not represent the entire spectrum of critical infrastructure organisations in Finland. The participation of only half the invited organisations introduces the possibility of selection bias, potentially favouring those more inclined towards MISP adoption or its national implementation. To counteract this, we concentrated on collecting comprehensive data during the interviews, encouraging participants to share not only specifics from their organisations but also broader trends and practices from their sectors, thus enriching the organisational focus with broader industry insights.

Interviews were limited to large, safety-critical organisations; however, concerns about resource constraints affecting MISP adoption were still raised. This leads to questions about the scalability of MISP adoption, especially for smaller organisations. The interviews highlighted the inclusion of smaller companies within their supply chains, which, while not officially categorised as critical infrastructure, can still access valuable data and should be considered in CTI collaborations. Previous research (e.g. Van Haastrecht, 2021) suggests MISP's potential for SME-sized organisations, but its practicality for the supply partners of Finnish safety-critical organisations merits examination. Further research is needed on standardising CTI-sharing tools and practices within a national context to ensure they are accessible for organisations of all sizes.

The discussions on the strict GDPR interpretations hindering MISP adoption reflect a broader concern within the cybersecurity community regarding the delicate balance between data privacy and threat intelligence sharing (see, for example, Nweke & Wolthusen, 2020; Grotto & Schallbruch, 2021). The observations made by informants regarding the varying interpretations of GDPR across European countries find support in existing research (Custers et al., 2018). These findings raise concerns about whether the stringent approaches adopted by some countries might potentially jeopardise long-term European cybersecurity efforts.

6. Conclusion

In conclusion, this study sheds light on the existing landscape of CTI sharing within Finland's critical infrastructure sectors and highlights the promising role of MISP in advancing these efforts. Notably, several critical organisations are contemplating a shift from conventional CTI sharing methods, such as email and chat groups, to MISP, attracted by its benefits like real-time sharing and the facilitation of data automation. However, the broader adoption of MISP at the national level is still hindered, with the critical infrastructure organisations waiting for the initiative from the National Cybersecurity Centre to establish a national MISP instance. Such a move was anticipated to strengthen Finland's cross-sectoral and industry-specific CTI exchanges. Implementing a national MISP framework also holds the potential to drive Finnish organisations towards engaging in Europe-wide, sector-specific MISP instances or adopting MISP as a tool for more effective threat intelligence exchange with supply chain partners. Additionally, this study draws attention to the challenges posed by data protection regulations, especially the varied interpretations of GDPR, which impact the sharing of detailed threat data across Europe. We hope this study will spark further research to deepen the understanding of CTI sharing and MISP adoption within a national framework.

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

Abu, M.S., Selamat, S.R., Ariffin, A. & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371–379.

Adam, Z. & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. ACM International Conference Proceeding Series. [Available at: https://doi.org/10.1145/3339252.334052

Amanowicz, M. (2020). Towards building national cybersecurity awareness. International Journal of Electronics and Telecommunications, 321-326.

Bauer, S., Fischer, D., Sauerwein, C., Latzel, S., Stelzer, D., and Breu, R. (2020) Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In: 53rd Hawaii International Conference on System Sciences, HICSS 2020, Maui, Hawaii, USA, January 7-10. ScholarSpace, pp. 1-10. Available at: http://hdl.handle.net/10125/63978

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative research journal, 9(2), pp 27-40, https://doi.org/10.3316/QRJ0902027

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. Computer Law & Security Review, 34(2), 234-243.

Dandurand, L. and Serrano, O.S. (2013). Towards improved cyber security information sharing. In: Cyber Conflict (CyCon), 2013 5th International Conference on. IEEE, pp. 1-16.

de Melo e Silva, A., Gondim, J.J.C., Albuquerque, R.O., García Villalba, L.J. (2020). A methodology to evaluate standards and platforms within cyber threat intelligence. Future Internet, 12(6), pp. 1–23. Available at: https://doi.org/10.3390/fi12060108

Fransen, F., & Kerkdijk, R. (2017). Cyber threat intelligence sharing through national and sector-oriented communities. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level, 187.

Grotto, A. and Schallbruch, M. (2021) Cybersecurity and the risk governance triangle: Cybersecurity governance from a comparative US–German perspective. International Cybersecurity Law Review 2(1), pp. 77-92.

Haque, M.F. and Krishnan, R. (2021). Toward automated cyber defense with secure sharing of structured cyber threat intelligence. Information Systems Frontiers 23, pp. 883–896. Available at https://doi.org/10.1007/s10796-020-10103-7

Hsieh H. and Shannon S (2005). Three approaches to qualitative content analysis. Qualitative Health Research, 15 (9) (2005), pp. 1277–1288, https://doi.org/10.1177/1049732305276687

Johnson, C.S., Badger, M.L., Waltermire, D.A., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. Technical Report NIST Special Publication (SP) 800–150. National Institute of Standards and Technology, Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.SP.800-150

Kampanakis, P. (2014). Security automation and threat information-sharing options. Security & Privacy, IEEE, 12(5), pp. 42-51.

King, N. (2012). Doing Template Analysis. In: Qualitative Organizational Research: Core Methods and Current Challenges. Sage

Kure, H. and Islam, S. (2019). Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. Journal of Universal Computer Science, 25(11), pp.1478-502.

Li, Q., Yang, Z., Liu, B., Jiang, Z.Y. (2017). Framework of Cyber Attack Attribution Based on Threat Intelligence. ICST Inst Comput Sci Soc Informatics Telecommun Eng, 2017;190:92–103.

MISP (2024)- Model of Governance.[Online] Accessed 10th of January 2025. Available at: https://www.misp-project.org/governance/

Nweke, L. and Wolthusen, S. (2020) Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. 12th International Conference on Cyber Conflict (CyCon). Vol. 1300. IEEE, 2020.

Pawlinski, P., Jaroszewski, P., Kijewski, P., Siewierski, L., Jacewicz, P., Zielony, P., Zuber, R. (2015). Actionable information for security incident response. European Union Agency for Network and Information Security, Heraklion, Greece.

Ramallo-González, A. P., González-Vidal, A., & Skarmeta, A. F. (2021). CIoTVID: Towards an open IoT platform for infective pandemic diseases such as COVID-19. Sensors, 21(2), 484.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), 7273.

Skopik, F., Settanni G., and Fiedler, R. (2017). The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats. In: Skopik, F. (Ed.), Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. Auerbach Publishers, Incorporated.

Stojkovski, B., Lenzini, G., Koenig, V., and Rivas, S. (2021). What's in a Cyber Threat Intelligence sharing platform? A mixed-methods user experience investigation of MISP. In: Annual Computer Security Applications Conference, pp. 385-398.

Sullivan, C., Burger, E. (2017). In the public interest: The privacy implications of international business-to-business sharing of cyber-threat intelligence. Computer Law & Security Review, 33(1), 14–29. ISSN 0267-3649. [Online] Available at: https://doi.org/10.1016/j.clsr.2016.11.015

Schwartz, A., Shah, S. C., MacKenzie, M. H., Thomas, S., Potashnik, T. S., & Law, B. (2016). Automatic threat sharing: how companies can best ensure liability protection when sharing cyber threat information with other companies or organizations. U. Mich. JL Reform, 50, 887.

Tounsi, W. (2019) What is Cyber Threat Intelligence and How is it Evolving? In: Cyber-Vigilance and Digital Trust. John Wiley & Sons, Ltd, Chapter 1, pp. 1–49. Available at: https://doi.org/10.1002/9781119618393.ch1

Van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Baumgartner, L., Fricker, S., Ruiz, J.F. and Armas, E., 2021. A shared cyber threat intelligence solution for smes. Electronics, 10(23), p.2913.

Vazquez, D.F., Acosta, O.P., Spirito, C., Brown, S., Reid, E. (2012). Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. In: 4th International Conference on Cyber Conflict, CyCon 2012, Tallinn, Estonia, June 5-8, pp. 1–17.

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). Misp: The design and implementation of a collaborative threat intelligence sharing platform. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 49-56.

Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.