Cyber Threat Intelligence as Socio-Technical Practice in Organizations: A Systematic Literature Review

Patrick Shirazi[1,*]

[1] University of Skövde, Högskolevägen 3, 541 45 Skövde, Sweden

Abstract

Cyber Threat Intelligence (CTI) is often framed as a technical capability centered on threat data, platforms, standards, automation, and information sharing. However, its organizational value also depends on analyst expertise, leadership, trust, governance, business alignment, and cross-functional collaboration. This study addresses this imbalance through a systematic literature review of 66 peer-reviewed studies published between 2014 and 2026. Grounded in socio-technical systems theory, the review organizes the literature into three interconnected dimensions: social-system factors, including human capabilities and organizational conditions; technical-system factors, including data quality, interoperability, and automation; and socio-technical interaction factors, including strategic alignment, business translation, governance, and workflow integration. The synthesis reveals critical tensions between automated speed and analyst interpretation, technical standardization and local organizational context, and intelligence sharing and data sovereignty. The findings indicate that these tensions cannot be resolved through technical improvement alone. Sustainable CTI practice requires automation that augments human interpretation, standards adapted to local work practices, sharing mechanisms coupled with trust and governance controls, and intelligence outputs integrated into organizational decision-making workflows. By reframing CTI as an integrated socio-technical practice rather than a siloed technical function, the study provides a structured basis for future empirical research and actionable design priorities for managers seeking to develop sustainable, context-sensitive, and human-centered CTI capabilities.

Keywords

Cyber Threat Intelligence, CTI practice, Socio-technical systems, Organization [1]

1. Introduction

Cyber Threat Intelligence (CTI) encompasses both actionable threat knowledge relevant to a specific organization [1] and the organizational process through which threat-related data and information are directed, collected, processed, analyzed, and disseminated to support decision-making [2, 3]. By reducing the knowledge asymmetry between attackers and defenders, CTI can help decision-makers reduce uncertainty, improve situational awareness, and evaluate possible courses of action at operational, tactical, and strategic levels [1, 2, 4, 5]. In this study, CTI practice refers to the coordinated organizational work through which these intelligence

STPIS2026: Proceedings of the 12th International Conference on Socio-Technical Perspectives in IS, September 16-17th L'Aquila, Italy

* Corresponding author.

† These authors contributed equally.

patrick.shirazi@his.se (P. Shirazi);

0009-0008-9916-7439 (P. Shirazi);

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-4334/paper8.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-19

activities are performed, their outputs are interpreted and contextualized, and the resulting intelligence is embedded in security and business workflows [2, 3, 6]. In organizational settings, CTI is therefore not limited to indicators, feeds, or technical alerts. Its value depends on whether threat-related data can be transformed into contextualized intelligence that supports informed organizational action.

Existing CTI research has made important contributions to technical mechanisms, data processing, automation, sharing standards, threat intelligence platforms, and information-exchange infrastructures [2, 7, 8]. These contributions remain essential because effective CTI practice requires high-quality data, interoperability, analytical and automation capabilities, and reliable technical infrastructures. However, organizational studies of CTI suggest that technical capability alone does not explain whether CTI becomes useful in practice. This is consistent with broader socio-technical research showing that technically sound systems may fail to deliver their intended value when user capabilities, work practices, governance, stakeholder engagement, and organizational change are insufficiently considered, as demonstrated by Baxter and Sommerville (2011) [9] and Sommerville (2015) [10]. Within the CTI context, Berndt and Ophoff (2020) [11] show that CTI value and challenges differ according to organizational skills, tools, tasks, and context, while Shin and Lowry (2020) [1] emphasize the analytical, contextual, and learning capabilities required from practitioners.

Recent studies further indicate that CTI practice depends on the relationship between technical intelligence activities and organizational conditions. Kotsias et al. (2023) [6] show how integrating CTI into routine organizational processes and tailoring it to stakeholder needs can inform cybersecurity decisions and actions in a commercial organization. In a recent case study, Ainslie et al. (2026) [12] show that even a mature organization may struggle to use CTI strategically when intelligence requirements emerge from operational technology groups rather than from strategic business needs. Xin et al. (2026) [13] similarly highlight the difficulty of translating technical cyber information into business-facing risk and financial language for decision-makers. These studies suggest that CTI practice is shaped by communication, interpretation, trust, governance, leadership, organizational maturity, and business alignment, as well as by technical tools and data.

Despite this growing organizational focus, CTI research remains fragmented. Technical studies often examine data sources, standards, automation, and platform capabilities, whereas organizational studies discuss skills, management support, trust, sharing behavior, maturity, and decision-making. Because these research streams often treat social and technical factors separately, they do not provide a coherent explanation of how CTI operates as an organizational practice. This fragmentation reflects a broader concern within Information Systems research: Sarker et al. (2019) [14] argue that the socio-technical perspective can serve as an "axis of cohesion," providing a coherent foundation for examining technological capabilities together with their social and organizational contexts. Applied to CTI, this perspective exposes a gap in understanding how human expertise, organizational routines, governance arrangements, technical infrastructures, and stakeholder expectations interact to enable or constrain CTI practice. Addressing this gap is important because CTI may be technically accurate but still fail to become actionable, trusted, or strategically relevant if it is not connected to organizational decision-making processes [12, 15, 16].

Socio-technical systems theory provides a suitable lens for examining this problem. The theory views organizational performance as dependent on the joint optimization of social and

technical subsystems [17]. Baxter and Sommerville (2011) [9] explain why this joint perspective matters: systems may satisfy their technical requirements yet fail to support actual organizational work when their design overlooks the complex relationships among technologies, people, processes, and organizational context, including the workarounds and dynamic adaptations through which systems are used in practice. The social subsystem includes actors, roles, skills, communication, trust, leadership, governance, culture, and work practices. The technical subsystem includes tools, platforms, data sources, standards, automation, analytics, infrastructures, and the formally defined CTI lifecycle tasks these resources support. Applied to CTI, this perspective directs attention to how intelligence outcomes are produced through interactions among people, organizations, and technologies. For example, automated CTI processing still requires analyst interpretation; standards improve interoperability but require organizational learning; and CTI sharing depends on technical exchange mechanisms as well as trust, confidentiality, legal clarity, and reciprocity.

This study therefore conducts a systematic literature review to develop a socio-technical understanding of CTI practice in organizations. The review aims to identify the social-system factors, technical-system factors, and socio-technical interaction factors that shape CTI effectiveness, integration, and sustainability. The first two research questions examine factors located primarily within the social and technical subsystems, whereas the third focuses on their interactions because the effectiveness, integration, and sustainability of CTI depend on how these subsystems are aligned in organizational practice. Accordingly, the study is guided by the following research questions:

RQ1: What social-system factors influence CTI practice in organizations?

RQ2: What technical-system factors influence CTI practice in organizations?

RQ3: What socio-technical interaction factors influence the effectiveness, integration, and sustainability of CTI practice in organizations?

By answering these questions, the study contributes to CTI research by reframing CTI as a socio-technical organizational practice rather than only a technical capability, platform function, or information-sharing activity. The review also provides a basis for explaining why CTI may fail to become actionable or strategically useful even when organizations have access to threat data, automated tools, and intelligence-sharing mechanisms.

2. Research Methodology

This study followed Webster and Watson's (2002) [18] guidance to structure the literature review. This protocol provides a structured approach for identifying, selecting, and assessing relevant research studies and has been widely used in Information Systems research. The approach was appropriate for this study because the aim is to synthesize existing academic knowledge on CTI practice in organizations and to identify the social, technical, and interactional factors that influence its effectiveness, integration, and sustainability.

The databases were selected based on their academic rigor and coverage of peer-reviewed research in Information Systems, cybersecurity, and organizational studies. IEEE Xplore was included because of its strong coverage of technical cybersecurity research, while Scopus and Web of Science were selected because of their broad multidisciplinary coverage. Other sources, such as ACM Digital Library, were not included to avoid redundancy in technical coverage, while Google Scholar was excluded due to its inclusion of non-peer-reviewed and difficult-to-

replicate materials. The search was conducted in the title, abstract, and keyword fields of each database, with database-specific syntax adjustments where required.

To ensure that the search query reflected the socio-technical framing of the review, the search strategy was organized around three interrelated concept groups: CTI as the focal phenomenon; the technical subsystem of CTI practice, including technologies, frameworks and CTI lifecycle tasks; and the social subsystem of CTI practice, including organizational structures, decision-making and people. Unlike a narrow socio-technical keyword search, the term "socio-technical" was not made mandatory in the main query because many relevant CTI studies discuss social, technical, and organizational interactions without explicitly using socio-technical terminology. Therefore, the socio-technical systems lens was applied mainly during screening, data extraction, and synthesis. The search query is presented in **Figure 1** and was subsequently adapted for use in Scopus, Web of Science, and IEEE Xplore.

The inclusion criteria focused on academic, peer-reviewed journal articles and conference papers that explicitly addressed CTI practice, adoption, implementation, integration, value, or operationalization in organizational contexts. Only studies written in English were included. The review covered studies published from 2014 through July 2026, reflecting the period in which CTI became more visible as an academic and practitioner topic. Studies were included when they examined CTI in relation to organizations, enterprises, cybersecurity teams, Security Operations Centers (SOCs), Computer Security Incident Response Teams (CSIRTs), and Computer Emergency Response Teams (CERTs), or other organizational security functions.

Papers were excluded if they focused solely on CTI outside organizational contexts, such as purely technical algorithm development, malware classification, automated detection, or data-processing mechanisms without any discussion of organizational use or practice. Studies were also excluded if they lacked a clear CTI focus, did not discuss organizational implementation or use, were not peer-reviewed, were not written in English, or did not provide accessible full-text versions for review. Additionally, white papers, book chapters, editorials, reports, and unpublished manuscripts were excluded. This approach ensured that the final corpus was relevant to understanding CTI as an organizational and socio-technical practice rather than merely as a technical artifact.

The initial database search returned 1231 results. After removing 578 duplicates, 653 unique records remained. During the initial screening phase, titles, keywords, and abstracts were reviewed against the inclusion and exclusion criteria, leading to the exclusion of 395 papers. The remaining 258 papers underwent full-text screening, resulting in 216 additional exclusions and leaving 42 relevant articles. Forward and backward snowballing was then conducted by reviewing references and citations of the selected articles, identifying 24 additional papers. The final corpus therefore consisted of 66 articles. Appendix A, Table 5 presents the complete list of all 66 included papers. Appendix B presents the search queries used for each database. **Figure 1** illustrates the search query and paper selection process.

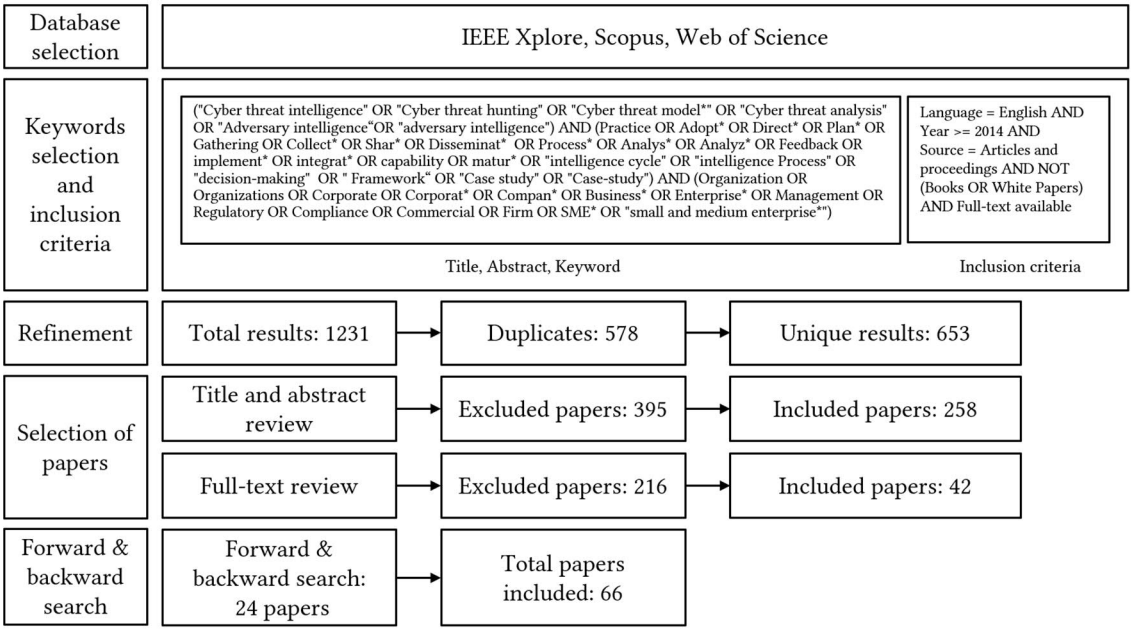


Figure 1: Paper selection process using the Webster and Watson (2002) method

Each selected article underwent a full-text review, during which findings relevant to the research questions were extracted. The extracted findings were analyzed using a hybrid deductive–inductive qualitative thematic approach, following Fereday and Muir-Cochrane (2006) [19]. The deductive component was informed by Deductive Qualitative Analysis, as outlined by Fife and Gossner (2024) [20], and supported the systematic application of socio-technical systems theory as an existing theoretical lens. The inductive component allowed the specific factors and themes to be developed from recurring concepts and relationships identified in the reviewed literature rather than being fully determined in advance.

This qualitative orientation is consistent with the established tradition of qualitative inquiry in Information Systems, which examines how computing systems are developed and used by individuals, teams, and organizations within particular organizational and institutional contexts [21]. Qualitative analysis was appropriate because the research questions concerned how human capabilities, organizational practices, governance arrangements, technical elements, and the relationships among them were conceptualized across the reviewed studies. The purpose was therefore to interpret and synthesize these factors and relationships rather than to assess their importance solely according to their frequency of occurrence. This approach enabled the analysis to capture contextual meanings, organizational practices, and socio-technical dependencies that could not be adequately represented through a quantitative count of factors alone.

The initial analytical structure was derived deductively from socio-technical systems theory, which views organizational performance as dependent on the interaction and joint optimization of social and technical subsystems [17]. Accordingly, social-system factors, technical-system factors, and socio-technical interaction factors constituted the predefined analytical dimensions. Within the social-system dimension, the distinction between people and organizational elements was theoretically informed, while the technical-system dimension was

structured around technological artifacts and tasks. These overarching categories guided the analysis, but the specific factors and interaction themes presented in Tables 1–4 were not predetermined.

The extracted findings were organized in a concept matrix to support systematic comparison within and across the reviewed studies. This procedure followed the concept-centric approach to literature synthesis advocated by Webster and Watson (2002) [18], in which studies are organized according to the concepts they address rather than being summarized individually or chronologically. Findings were initially assigned to the theoretically derived analytical dimensions. Within each dimension, conceptually related findings were then compared, grouped, and refined iteratively. Through this process, the detailed factors and themes were developed inductively and assigned labels representing the underlying concepts identified across the literature. The supporting studies were subsequently mapped to each factor to maintain a transparent connection between the analytical synthesis and the reviewed evidence. The analysis was therefore deductive at the level of its overarching theoretical structure and inductive at the level of detailed factors and theme development.

Social-system factors refer to human and organizational elements such as skills, expertise, roles, leadership, governance, trust, communication, collaboration, culture, maturity, and stakeholder engagement. Technical-system factors encompass technological artifacts, including tools, platforms, data sources, standards, automation, interoperability mechanisms, analytics, threat intelligence feeds, and technical infrastructures, as well as the formally defined tasks supported by these artifacts. Following the distinction between technology and tasks in socio-technical systems theory [17], the technical-system dimension in this study includes both the technological artifacts used for CTI and the CTI lifecycle tasks through which intelligence work is performed, including direction and planning, collection, processing, analysis, and dissemination [3, 12]. This treatment is also consistent with Alter's (2015) work-system perspective [22], which emphasizes that technologies and operational activities should be examined as interconnected elements of organizational work rather than as isolated components. Although lifecycle tasks were included within the technical-system dimension for analytical purposes, their human enactment, interpretation, and adaptation within organizational settings were captured through the social-system and socio-technical interaction dimensions.

Socio-technical interaction factors capture the alignments, dependencies, and tensions between the social and technical systems. These include the fit between CTI outputs and business needs, integration with organizational workflows, trust in automated intelligence, human interpretation of machine-generated outputs, feedback between intelligence producers and consumers, and the balance between standardization and local organizational context.

This analytical approach enabled the review to move beyond a factor-based classification and examine CTI as a socio-technical organizational practice. It also provided a direct basis for answering the research questions by identifying the social-system factors influencing CTI practice, the technical-system factors enabling or constraining it, and the ways in which interactions between the social and technical systems affect CTI effectiveness, integration, and sustainability.

3. Results

3.1. Social-system: People factors

From a social-system perspective, CTI practice is shaped by human capabilities and organizational conditions. Table 1 provides a summary of the reviewed literature that explores the role of people within an organization in advancing an effective CTI practice. CTI relies on analysts' skills and cross-domain knowledge to interpret threat data and transform it into actionable intelligence. User satisfaction, perceived trust, and willingness to engage with new processes are crucial for effective CTI implementation. Each factor is explored in further detail below.

Table 1
Social-system: People factors

Factor	Description	References
Analyst skills and competence	CTI practice depends on analysts' ability to interpret threat data, apply contextual knowledge, conduct rigorous analysis, and transform raw information into actionable intelligence. Gaps in cybersecurity, data analytics, intelligence analysis, or CTI standards can reduce the practical value of CTI outputs.	[1, 5, 15, 23, 24, 25]
Analyst tradecraft and human interpretation	CTI requires more than technical data processing. Analysts must apply tradecraft, intuition, analytical rigor, and contextual interpretation to distinguish relevant threats from noise and make intelligence meaningful for organizational action.	[1, 5, 15]
Cross-domain knowledge	CTI work often requires knowledge across cybersecurity, intelligence analysis, data analytics, business risk, and organizational context. Knowledge gaps between these domains can hinder the identification, interpretation, and use of relevant CTI.	[2, 24, 26, 27, 28]
User satisfaction and perceived trust	CTI platforms and processes are more likely to be used when they meet the needs of diverse users, including operational staff, analysts, managers, and decision-makers. Perceived trust, content quality, system quality, and service quality influence engagement with CTI systems.	[29]
Willingness to engage with new CTI processes	Resistance to new CTI processes, platforms, and workflows can delay or weaken CTI practice. User willingness depends on perceived usefulness, usability, trust, organizational support, and fit with existing work routines.	[6, 29]

Analyst skills and competence. The literature emphasizes the importance of analyst skills and training in determining the value and effectiveness of CTI practice. Well-trained analysts improve organizations' ability to use shared threat intelligence effectively [1, 15, 24, 25]. Shin and Lowry (2020) [1] conceptualize CTI analytical capability as a combination of discovery, analysis, and learning capabilities. Their model suggests that effective CTI depends heavily on

practitioners' knowledge of organizational and threat environments, their analytical skills in transforming raw data into actionable intelligence, and their ability to continuously acquire and apply new knowledge.

Analyst tradecraft and human interpretation. Abraham et al. (2025) [15] similarly emphasize that CTI effectiveness depends on analyst tradecraft and analytical rigor in interpreting threat information within its organizational context. In this view, threat data only becomes intelligence when skilled analysts apply expertise and context to make it meaningful for action. Oosthoek and Doerr (2021) [5] argue that CTI needs stronger analytical methodology and tradecraft informed by intelligence studies, rather than continued reliance on technological solutions alone.

Cross-domain knowledge. Knowledge gaps are repeatedly identified as barriers to CTI practice. Miazi et al. (2017) [24] note that security experts may lack proficiency in data analytics, while data analytics professionals may lack cybersecurity expertise. This gap is linked to the limited integration of threat hunting and CTI-related practices into cybersecurity education. Alkalabi et al. (2021) [23] similarly identify a lack of employee expertise in handling threat intelligence as an operational barrier to CTI sharing. Other studies highlight knowledge gaps as barriers to identifying relevant CTI [28], as well as contributors to the disconnect between technologists and intelligence specialists [2]. These issues are particularly pronounced among small and medium-sized enterprises (SMEs), which often have limited cybersecurity knowledge, staffing, and resources [27]. Aldasoro et al. (2024) [26] show that this cross-domain skills issue is becoming more important as Artificial Intelligence (AI) is introduced into cybersecurity work because organizations require personnel who understand both cybersecurity and AI methods.

User satisfaction and perceived trust. The literature also shows that CTI practice depends on user satisfaction and perceived trust. Zibak et al. (2021) [29] propose a success model for CTI management platforms in which user satisfaction depends on content quality, system quality, service quality, and perceived trust. Because CTI users may range from operational security staff to managers and decision-makers, CTI platforms and outputs must satisfy different information needs. User engagement can also be strengthened by security measures and compliance with regulatory requirements such as the General Data Protection Regulation (GDPR).

Willingness to engage with new CTI processes. Kotsias et al. (2023) [6] show that reluctance to engage with new CTI processes can become a barrier, particularly when CTI tools or workflows do not fit existing routines or stakeholder expectations. Taken together, these findings reveal a socio-technical dependency: trust, satisfaction, and willingness to engage with CTI do not arise from platform functionality alone, but from the fit between the platform, the quality and relevance of its content, users' needs, and established organizational routines [6, 29].

3.2. Social-system: Organizational factors

The second dimension of a social system is its organizational factors, as summarized in

Table 2. The reviewed literature emphasizes that effective CTI practice requires shared terminology, organizational maturity, leadership support, adaptability, resource allocation, and internal capability for interpreting and managing outsourced services.

Table 2
Social-system: Organizational factors

Factor	Description	References
Shared terminology and conceptual clarity	CTI practice is constrained by the lack of common definitions, terminology, and vocabulary. Inconsistent understandings of CTI concepts can create communication difficulties among analysts, managers, business stakeholders, and external sharing partners.	[2, 5, 23, 30, 31, 32, 33, 34]
Organizational maturity	Mature CTI practice requires established processes, internal capabilities, appropriate technologies, defined roles, and sustained investment. Immature processes and limited organizational readiness can reduce the ability to use CTI effectively.	[30, 35, 36]
Leadership endorsement and management support	Senior management support is necessary for prioritizing CTI, allocating resources, legitimizing CTI activities, and integrating CTI into organizational security strategies and decision-making structures.	[2, 6, 37]
Institutional innovation and organizational adaptability	CTI practice is strengthened when organizations introduce or adapt policies, procedures, governance structures, and management routines in response to changing threats and intelligence needs. CTI value depends not only on technology but also on the organization's ability to institutionalize new practices.	[37]
Resource allocation and financial constraints	CTI solutions, platforms, analysts, training, and integration work require financial and human resources. Limited budgets and staffing shortages can restrict the development of sustainable CTI capabilities, especially in SMEs.	[2, 6, 13, 23, 27, 30, 37]
In-house capability and outsourcing management	Organizations need sufficient internal knowledge to interpret CTI, evaluate outsourced services, and align external intelligence with internal risks. Outsourcing may support resource-constrained organizations, but it does not remove the need for internal capability and governance.	[5, 6, 13, 35]

Shared terminology and conceptual clarity. A primary social-system barrier is the lack of consensus on CTI definitions, key terms, and vocabulary [2, 23, 30, 31, 32, 33, 34]. Inconsistent terminology can weaken communication among analysts, business stakeholders, technical teams, and external sharing partners. This problem is not merely semantic: unclear terminology can affect the interpretation of intelligence requirements, the classification of threat information, and the coordination of CTI activities across organizational boundaries. From a

socio-technical perspective, semantic fragmentation can also undermine technical interoperability because the effective use of standards such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) depends not only on compatible formats and protocols but also on a shared human interpretation of threat concepts and classifications [32, 34].

Organizational maturity. Organizational maturity is another critical factor influencing CTI practice. Maturity-model evaluation research supports the need to assess CTI capability development systematically [36]. Maturity has been examined in relation to established processes, technological infrastructure, sustained investment, and internal capability development [35]. For example, Zibak and Simpson (2019) [30] found that a large proportion of respondents considered their organization's information-sharing program immature, indicating a broader gap in organizational readiness.

Leadership endorsement and management support. Executive endorsement is essential because senior management support and financial backing are needed to prioritize, legitimize, develop, and sustain CTI capabilities [2, 6].

Institutional innovation and organizational adaptability. Chang and Hsu (2026) [37] reinforce the importance of organizational and managerial resources in CTI practice. Their study identifies top management support, institutional innovation, financial resources, and CTI response capability as central factors in successful CTI implementation, while technological innovation is ranked lower than these organizational and human capabilities. This suggests that CTI practice depends not only on acquiring advanced technologies but also on executive commitment, resource allocation, institutional adaptability, and the development of internal analytical and response capabilities.

Resource allocation and financial constraints. Financial constraints and resource limitations also shape CTI practice. CTI platforms, services, analysts, training, and integration activities require sustained investment. Excessive costs may be reduced through long-term CTI arrangements and collaborative intelligence sharing, which can distribute costs across organizations [23]. Aligning security investments with business continuity planning can also support more sustainable allocation of financial resources [23, 30].

In-house capability and outsourcing management. Developing in-house competence is important for reducing dependence on fully outsourced services or isolated CTI specialists [6, 35]. Internal expertise enables organizations to interpret intelligence, evaluate external services, and align CTI with internal risks and priorities. This requirement becomes particularly important when resource-constrained organizations depend on external security services. Xin et al. (2026) [13] show that limited cybersecurity budgets and insufficient technical expertise can make it difficult for organizations to assess outsourced services. From a socio-technical perspective, outsourcing therefore creates an interorganizational boundary at which the provider's platforms, processes, and expertise must be aligned with the client organization's internal knowledge, governance arrangements, risk priorities, and decision-making routines [6, 13]. Outsourcing may reduce the burden of building an internal CTI platform, but it does not eliminate the need for internal competence, governance, and evaluation capability.

3.3. Technical-system factors

The reviewed literature identifies several technical-system factors that enable or constrain CTI practice. As summarized in Table 3, the effectiveness of CTI depends on data quality, feed

timeliness and coverage, interoperability, platform capabilities, data-processing and analytical functions, and automation and orchestration. These technical capabilities provide essential support for CTI work, but their organizational value depends on their reliability, integration, and suitability for the intelligence tasks they are intended to support.

Table 3
Technical-system factors

Factor	Description	References
Data quality	CTI effectiveness is constrained by incomplete, imprecise, inconsistent, biased, outdated, manipulated, or unverified data. False positives, unstructured formats, and insufficient contextual information can limit the usefulness of CTI feeds and repositories.	[5, 23, 28, 38, 39, 40, 41, 42, 43]
Feed timeliness and coverage	Delays in feed updates reduce the value of CTI for proactive threat mitigation. Geographic bias, reliance on repackaged feeds, and limited originality can also affect the relevance and reliability of threat intelligence.	[7, 39, 44]
Interoperability and standards	CTI exchange depends on common standards, formats, taxonomies, and protocols. STIX, TAXII, MISP, and related mechanisms can support structured exchange, but differences in implementation and data representation can create compatibility problems.	[6, 7, 23, 27, 29, 32, 34, 42, 43, 45, 46, 47]
Threat Intelligence Platform (TIP) capabilities	TIPs support CTI aggregation, management, processing, and sharing but may be limited by weak filtering, restricted customization, limited stream aggregation, basic search functions, and insufficient integration capabilities.	[27, 29, 38, 39, 43, 48, 49, 50]
Data processing and analytics	CTI practice requires tools for collecting, filtering, enriching, normalizing, linking, and analyzing large volumes of heterogeneous data. Machine learning, Natural Language Processing (NLP), text mining, and visualization can support these activities and reduce manual effort.	[41, 51, 52, 53, 54, 55, 56, 57]
Automation and orchestration	Automation can improve the speed, scale, and consistency of CTI processing and sharing. However, it requires appropriate service architectures, synchronization, orchestration, and integration with existing security systems.	[25, 35, 49, 50, 58]

Data quality. Data quality is a central technical challenge in CTI practice. CTI-feed evaluation requires mechanisms for assessing feed efficacy, yet many traditional CTI models provide limited support for such evaluation [42]. The absence of centralized exchange systems, standardized formats, shared taxonomies, and secure communication channels can further reduce the quality and consistency of shared intelligence [23]. Multiple representations of the

same CTI data and flexible enrichment practices may also create inconsistencies for organizations consuming shared intelligence [43]. Public sources vary in information type, integrability, timeliness, originality, and trustworthiness [39], and may contain unstructured, vague, incomplete, manipulated, or unverified information [28, 39, 40]. Normalization, consolidation, data linkage, and advanced analytics can help address these inconsistencies [41].

Feed timeliness and coverage. Delays in updating CTI feeds reduce their usefulness for proactive mitigation. Indicators of compromise may appear in feeds only after a substantial delay, limiting their operational value [44]. Tounsi and Rais (2018) [7] similarly emphasize timeliness while explaining that faster sharing of indicators alone is insufficient against targeted attacks, where attackers may use indicators only once. Feed quality can also be weakened by geographic bias and limited originality when sources rely on aggregation, curation, or repackaging rather than original intelligence production [39, 44]. CTI systems therefore require not only large volumes of data but also timely, original, relevant, and reliable sources.

Interoperability and standards. Technical interoperability is another major factor influencing CTI practice. The continuing lack of consistently implemented cyber-intelligence standards has motivated the development of standards-based CTI frameworks [42]. STIX, TAXII, the Malware Information Sharing Platform (MISP), and related mechanisms can support structured exchange, relationship modeling, documentation, data restrictions, and interoperability [6, 27, 29, 32, 34, 45, 46, 47]. However, differences in implementation, data notation, and representation can create compatibility problems [46].

Threat Intelligence Platform (TIP) capabilities. Platform limitations can include restricted customization, weak filtering, stream-aggregation challenges, basic search functionality, and insufficiently developed Application Programming Interfaces (APIs) [27, 38, 39, 43, 49]. The absence of clear technical requirements and specifications can also hinder platform implementation, as demonstrated in the implementation of CTI feeds for Industrial Control Systems and Operational Technology (ICS/OT) networks [48].

Data processing and analytics. Analytical capabilities are increasingly important because organizations must process large volumes of heterogeneous threat data. Behavioral indicators concerning threat actors, attacks, and assets can be transformed into measurable features and maintained within a CTI knowledge base [53]. However, behavioral parameters may vary across domains and therefore need to be adapted to domain-specific and organization-specific settings. Custom crawlers and machine-learning models can improve data collection and filtering [52], while AI, NLP, text mining, and big-data technologies can support the extraction of CTI from human-readable sources and reduce manual workload [51, 54, 55, 56, 57]. Visualization techniques can also support the analysis of diverse CTI datasets and improve situational awareness [41]. These capabilities nevertheless require integration architectures that connect CTI sources, repositories, platforms, and organizational security systems.

Automation and orchestration. A recurring technical constraint is the continued reliance on manual processes. Many threat-modeling processes remain manual and provide limited validation mechanisms [31]. Similarly, CTI platforms may lack effective filtering based on organizational relevance and risk priority, increasing the effort required to identify useful intelligence [27, 43, 49]. The manual selection of relevant security feeds can extend response times and increase the risk of missing opportunities for mitigation [52]. Automation can reduce

manual error, accelerate processing, and improve the efficiency and consistency of intelligence exchange [25, 35, 58]. However, developing sustainable automation requires appropriate resources, synchronization, service architectures, orchestration, and integration with existing systems [49, 50].

3.4. Socio-technical interaction factors

Findings show that CTI value emerges through the alignment of people, organizational structures, governance arrangements, and technical infrastructures. CTI practice is effective when technical systems provide timely and reliable threat information, when analysts can interpret and contextualize this information, when governance mechanisms support trust and accountability, and when decision-makers can use CTI outputs in strategic and operational decisions. Table 4 summarizes the socio-technical interaction factors identified in the reviewed literature.

Table 4
Socio-technical interaction factors

Factor	Description	References
Strategic alignment and direction	CTI practice depends on alignment among organizational strategy, intelligence requirements, technical collection, and security operations. When CTI is directed mainly by technical teams, intelligence may be accurate but strategically irrelevant.	[12, 59, 60, 61]
Translation of CTI into business value	CTI must be translated from technical indicators, vulnerabilities, and threat descriptions into business-relevant risk, financial, operational, and strategic implications. Without this translation, CTI may not support executive decision-making.	[4, 6, 12, 13, 16, 27, 49, 62, 63]
Human interpretation of technical outputs	CTI platforms, automation, AI, and feeds do not automatically produce actionable intelligence. Analysts must interpret, validate, contextualize, and operationalize technical outputs before they can support action.	[1, 5, 15, 16, 27, 43, 49, 64]
Automation versus analyst interpretation	Automation increases speed and scale, but excessive reliance on automated outputs can reduce contextual understanding. Effective CTI practice requires a balance between machine processing and human interpretation.	[15, 16, 26, 27, 43, 49, 64]
Standardization versus local context	Standards improve interoperability and structured exchange, but their value depends on organizational compatibility, learning capacity, terminology comprehension, and adaptation to local CTI practices.	[6, 32, 34, 43, 45, 46]
Sharing versus confidentiality and data sovereignty	CTI sharing depends on technical exchange mechanisms and organizational willingness to disclose sensitive information. Confidentiality, privacy, liability, reputation, data sovereignty, and control over shared intelligence shape participation.	[7, 23, 50, 55, 58, 65, 66, 67, 68, 69, 70, 71, 72, 73]

Factor	Description	References
Trust, governance, and auditability	CTI output and sharing mechanisms must be trusted. Trust depends on governance, evidence traceability, auditability, reproducibility, policy enforcement, data protection, and accountability.	[7, 13, 29, 39, 40, 65, 67, 74]
Incentive alignment in CTI ecosystems	Interorganizational CTI sharing depends on incentives, reciprocity, trust, investment, and participation. Platforms are valuable only when organizations have reasons to contribute, consume, and act on shared intelligence.	[7, 15, 23, 72, 75, 76]
Workflow integration and feedback	CTI becomes useful when embedded in incident response, risk management, SOC and security information and event management (SIEM) environments, board-level reporting, and feedback loops between intelligence producers and consumers.	[5, 13, 27, 39, 40, 77, 78]

The literature indicates that CTI practice is shaped not only by social-system or technical-system factors in isolation but also by the relationships between them. These interactions determine whether technical threat data can be transformed into intelligence that is relevant, trusted, contextualized, and usable in organizational decision-making. The factors presented in Table 4 therefore explain how the alignment or misalignment of social and technical elements influences the effectiveness, integration, and sustainability of CTI practice.

Strategic alignment and direction. CTI effectiveness depends on aligning technical intelligence activities with organizational strategy. Strategic CTI can provide senior leadership with a broader situational picture of relevant cyber threats, although intelligence direction and strategic interpretation continue to require human involvement [61]. When strategic leaders do not participate in defining intelligence requirements, CTI teams may generate requirements internally based primarily on operational and technical concerns. The resulting intelligence products may be technically accurate but fail to address business priorities or strategic decisions [12]. This misalignment can also encourage leaders to rely on informal networks and personal contacts for actionable insight, further weakening formal CTI processes. Structured direction and planning provide a means of addressing this problem. Research in the Brazilian financial sector demonstrates how strategic priorities, threat mapping, priority intelligence requirements, requests for information, and collection plans can guide CTI before collection begins [60]. Gontijo et al. (2025) [59] illustrate this translation through a conceptual case study using OpenCTI, in which intelligence requirements inform lexical, contextual, and sectoral filtering. The example shows how organizational priorities can guide platform configuration to reduce informational noise and improve contextual relevance. CTI relevance is therefore shaped upstream through the translation of organizational priorities into intelligence requirements, collection plans, and platform-level filtering mechanisms.

Translation of CTI into business value. CTI outputs frequently contain technical indicators, vulnerabilities, adversary behaviors, and platform-generated summaries, but these outputs do not automatically support business-level decisions. Effective CTI practice requires intelligence to be accessible, reliable, contextually enriched, and relevant to the organization's

business environment. CTI must therefore be connected to board-level agendas, business processes, risk assessment, and organizational planning rather than remaining confined to operational security functions [4, 6, 27, 63].

The translation of CTI into business value also creates an evaluation challenge. Organizations may find it difficult to demonstrate CTI value through tangible measures such as return on investment [2, 6, 25]. Risk-oriented evaluations may instead consider sensitivity, organizational impact, and the consequences of sharing or withholding intelligence [66, 67], while technical evaluations emphasize properties such as timeliness, originality, coverage, and accuracy [44]. A socio-technical evaluation must therefore consider not only whether intelligence is technically accurate but also whether it improves risk prioritization, decision-making, and organizational response.

Organization-wide risk-management research identifies a persistent communication boundary between cybersecurity specialists and business stakeholders. Technical terminology and differences in professional knowledge can hinder timely cyber-risk assessment and strategic decision-making [13]. Translating threat information into financial exposure, organizational risk, and decision-relevant metrics can make CTI more actionable and support collaboration between cybersecurity, finance, and executive functions. Board-level engagement also depends on concise executive reporting, automated data integration, and transparent connections between technical threats and potential organizational consequences [13]. When formal CTI products fail to provide such business-relevant insight, leadership may instead rely on informal networks [12]. Translation should therefore not be treated as a final reporting activity after technical analysis; it is an embedded socio-technical process through which intelligence is connected to stakeholder responsibilities, governance, investment, and organizational action.

The business relevance of CTI also depends on continuous adaptation to changes in the organizational environment. CTI collection, filtering, and reporting must be tailored to the organization's business context and changing information requirements [49, 62]. Although CTI may deliver operational and tactical benefits, it can still lack strategic value when it does not reach executive decision-makers or is treated as a technical necessity rather than a business priority [6]. Technical intelligence may therefore exist without becoming organizationally valuable if it is not connected to decision-makers, changing business priorities, and trusted organizational routines.

Human interpretation of technical outputs. The translation problem reflects a broader knowledge boundary between business and technical groups. Business stakeholders may struggle to formulate intelligence requirements, while CTI practitioners may struggle to convert technical threat information into business-relevant insight [12]. Analyst tradecraft and contextual interpretation are therefore necessary for determining whether technical outputs are relevant to particular assets, risks, and organizational priorities [15]. Organizational learning is similarly required to transform intelligence into actionable security practices [16]. Human interpretation is consequently not an activity performed only after technical processing; it is the mechanism through which platform outputs are validated, contextualized, and connected across technical, operational, and strategic domains.

Automation versus analyst interpretation. Automation, AI, NLP, and CTI platforms can improve the speed, scale, and consistency of data processing. Generative AI may support

detection, response, and routine-task automation, but its effective use still requires specialist expertise, human supervision, and governance controls [26]. The reviewed literature emphasizes analysts' contextual knowledge, tradecraft, and analytical rigor in transforming threat data into actionable intelligence [15]. Platform limitations further reinforce this dependency because practitioners frequently need to correct, evaluate, prioritize, and contextualize automated outputs before they become actionable [27, 43, 49, 64]. Technical systems therefore create the greatest value when they augment human interpretation rather than merely increasing the volume or speed of indicator processing.

The organizational value of combined human and automated capabilities depends on their institutionalization across governance, processes, and personnel. Governance structures must assign responsibility for CTI activities and support sustained investment. Operational processes must establish procedures for intelligence analysis, incident response, feedback, and organizational learning. Human-resource practices must support the continuing development of analytical and response capabilities [16]. CTI should therefore be treated as an organizational capability embedded across routines and responsibilities rather than as an isolated platform function.

Standardization versus local context. Standards such as STIX and TAXII can improve structured exchange and technical interoperability, but their practical value depends on organizational compatibility, terminology comprehension, staff learning, and integration into local CTI routines [34]. Standardization does not eliminate the need for local interpretation and adaptation. Instead, standards become operationally useful when organizational actors understand their concepts, configure them for local requirements, and incorporate standardized information into existing security and decision-making practices.

Sharing versus confidentiality and data sovereignty. CTI sharing depends on the interaction among technical interoperability, organizational trust, shared terminology, and legal-governance conditions. Shared intelligence may contain personally identifiable information, sensitive operational details, proprietary business information, or indicators that expose internal security weaknesses. Privacy and regulatory concerns are therefore prominent barriers to participation [23, 58, 69, 71]. Risk-focused studies additionally identify legal liability and loss of control over disseminated intelligence [67], while supply-chain and collective-defense research highlights reputational and competitive concerns [66, 72]. Privacy and antitrust uncertainty may further discourage cross-organizational exchange [73]. GDPR can both constrain and enable business-to-business CTI sharing, depending on how the legal basis and public interest in cybersecurity are interpreted [58]. Technical deidentification can reduce privacy exposure, but it may also remove contextual detail and reduce operational utility [40]. Automated exchange additionally requires synchronization and orchestration across organizational and technical processes [49]. Effective sharing therefore requires the joint design of legal governance, data protection, interoperability, automation, and operational usefulness.

Trust, governance, and auditability. Sustainable CTI sharing requires governance architectures that connect technical exchange with organizational control and accountability [65, 74]. Governance should not operate solely as an external policy layer: organizational requirements can be embedded into sharing architecture through policy enforcement, certification, usage control, and federated data spaces. These mechanisms can operationalize requirements concerning compliance, ownership, collaboration, and data sovereignty while

allowing organizations to retain control over how intelligence is accessed and used [65]. Technical transparency also influences social trust. When decision-makers receive highly summarized intelligence without traceable evidence, transparent assumptions, or reproducible analytical paths, their ability and willingness to rely on the resulting assessments may be limited [13]. Trusted CTI practice therefore depends on both information quality and defensible processes that make intelligence production and use auditable.

Incentive alignment in CTI ecosystems. Interorganizational CTI sharing depends on networks of trust, reciprocal value, governance, and sustained participation. Tounsi and Rais (2018) [7] emphasize that sharing communities require attention to members' business processes, organizational stability, and cooperation policies, alongside trust and anonymity mechanisms that reduce concerns about sensitive-information disclosure. Technical standards and platforms can transfer threat data, but they do not automatically create willingness to contribute or use it. Participation depends on perceived usefulness, reciprocity, organizational maturity, and confidence that other participants will handle intelligence responsibly [15]. Cross-domain sharing also requires legal alignment, resource capacity, analyst expertise, automation, feedback, and incentives across organizational and jurisdictional boundaries [76]. Where these institutional and capability conditions are absent, technically functional platforms may remain underused. CTI-sharing platforms create collective value only when participating organizations have incentives to invest in cyber readiness, contribute intelligence, and act on shared knowledge [75]. CTI sharing should therefore be understood as a socio-technical ecosystem sustained by reciprocal relationships rather than as a platform-centered transfer of data.

Workflow integration and feedback. CTI becomes useful when it is embedded in organizational workflows and supported by feedback between intelligence producers and consumers. The availability of shared CTI does not ensure its operational use: Oosthoek and Doerr (2021) [5] discuss instances in which previously shared indicators were not acted upon. CTI, cyber-threat monitoring, and cyber-threat hunting form interdependent elements of the broader Cyber Threat Monitoring and Analysis domain: CTI supports management-level decisions, monitoring provides system-level visibility, and threat hunting uses CTI evidence and monitoring data to conduct hypothesis-driven investigations [78]. Fragmented tools, weak APIs, manual exchanges, and limited feedback reduce the timeliness and sustainability of these relationships. Even where platforms such as MISP are available, regional CTI may continue to be exchanged manually through email and chat, creating delays and inaccuracies [77]. Interface limitations can also prevent CTI from being embedded in incident response, risk management, Security Operations Center (SOC), and Security Information and Event Management (SIEM) workflows [39]. Feedback mechanisms such as reliability scoring connect users' evaluations to technical data quality and allow intelligence to be validated over time [39, 40]. Organizational contextualization remains essential because technically valid indicators may not be relevant to local assets, risks, or priorities [27]. Sustainable board-level use similarly requires continuous updates, automated imports, integration with SOC and SIEM environments, and reduced dependence on repeated manual explanation [13]. CTI integration therefore depends on the alignment of platforms, workflows, analyst interpretation, feedback, and organizational decision routines.

4. Discussion

This systematic literature review identifies and synthesizes the social-system, technical-system, and socio-technical interaction factors that shape CTI practice in organizations. While previous CTI reviews have often emphasized technical mechanisms, information-sharing standards, automation, platforms, and data quality [7, 8, 68], the findings of this review show that CTI practice cannot be fully understood as a technical capability alone. These earlier reviews also recognize organizational barriers, including trust and reluctance to share [7]; the present review brings such findings together through an explicit socio-technical systems framework. CTI becomes valuable when technical threat information is interpreted by skilled analysts, aligned with organizational priorities, embedded into governance and operational processes, and translated into forms that support decision-making. This finding is consistent with prior research that emphasizes the need to connect cybersecurity initiatives with organizational goals and security decision-making [2, 3, 6], but this review extends that work by explicitly framing CTI as a socio-technical organizational practice.

The social-system findings show that human expertise remains central to CTI practice. Analyst skills, tradecraft, contextual understanding, and learning capabilities are repeatedly identified as necessary for transforming threat data into actionable intelligence [1, 15]. These findings challenge tool-centric views of CTI, where intelligence value is assumed to result mainly from feeds, platforms, or automated processing. Instead, the literature suggests that CTI outputs require interpretation, validation, prioritization, and contextualization before they can support organizational action. This is particularly important because CTI often involves incomplete, uncertain, or heterogeneous information. Therefore, analyst competence is not a secondary support factor, but a core condition for effective CTI practice.

The findings also show that CTI practice depends on organizational and managerial conditions. Leadership endorsement, financial resources, organizational maturity, institutional innovation, and in-house capability development shape whether CTI can be sustained beyond isolated technical activities. This is especially visible in studies that identify top management support, institutional innovation, and CTI response capability as key enablers of CTI implementation, sometimes ranking these organizational and human resources above technological innovation itself [37]. These findings suggest that CTI practice requires more than investment in platforms. It also requires executive commitment, clear responsibilities, sustained resourcing, training, process development, and organizational readiness to use intelligence in security and business decision-making.

The technical-system findings confirm that data, platforms, standards, automation, and analytics remain important foundations of CTI practice. Data quality issues, including incompleteness, inconsistency, false positives, delayed indicators, lack of originality, and limited contextual information, continue to reduce the usefulness of CTI outputs [38, 39, 44]. Similarly, Threat Intelligence Platforms, APIs, standards, and automated exchange mechanisms can support CTI processing and sharing, but they may also introduce limitations when they lack filtering, customization, integration, or orchestration capabilities. These findings are consistent with technical CTI literature, but the socio-technical synthesis shows that technical

improvement alone is insufficient if organizations lack the capacity to interpret, trust, govern, and act on CTI outputs.

The most important contribution of this review lies in showing that CTI practice is shaped by socio-technical interaction factors rather than by social or technical factors independently. The findings suggest that CTI should be understood as a configuration of people, organizational routines, governance arrangements, technical infrastructures, and intelligence lifecycle tasks. For example, strategic alignment depends on the ability of leadership and business stakeholders to define intelligence requirements that can guide technical collection and analysis. When CTI requirements are generated mainly within technical teams, intelligence products may be technically accurate but strategically irrelevant [12]. Similarly, the translation of CTI into business, financial, and risk-related language should be understood not merely as a communication activity but as a socio-technical alignment mechanism. Research on organization-wide cyber-risk management demonstrates the communication boundary between cybersecurity specialists and business stakeholders [13], while the present review extends that insight by showing that CTI translation is connected to intelligence requirements, analyst interpretation, workflow integration, executive engagement, trust in CTI outputs, and feedback between intelligence producers and consumers. This challenge parallels the broader information-security problem identified by Bednar and Sadok (2024) [79], whose findings indicate that employees may perceive security as an additional layer imposed on their existing responsibilities rather than as an integral part of their work. When CTI is similarly treated as the exclusive responsibility of security specialists, strategic stakeholders, risk owners, operational teams, and decision-makers may remain detached from defining, contextualizing, and acting on intelligence. CTI translation should therefore not be treated as a final reporting step following technical analysis, but as a continuous organization-wide process through which technical intelligence is connected to stakeholder responsibilities and made actionable.

Previous organizational CTI studies provide important foundations for understanding how intelligence is implemented in practice, although they have approached the phenomenon through different theoretical and methodological perspectives. For example, Kotsias et al. (2023) [6] use clinical research as a form of action research to explain the adoption and integration of CTI in a commercial organization. Ainslie et al. (2026) [12] explicitly examine CTI within a socio-technical organizational environment while drawing on intelligence doctrine and the intelligence cycle as their formal theoretical lens. These approaches are well suited to their respective research objectives and provide valuable empirical explanations of CTI activities, stakeholders, intelligence flows, and organizational integration. The present review builds on these contributions by applying socio-technical systems theory explicitly across a broader body of CTI literature. Its contribution is therefore complementary: it integrates findings that have previously been examined through different theoretical perspectives and organizes their relationships around the social system, technical system, and the mechanisms through which the two are aligned. Rather than revealing simple empirical contradictions, this diversity points to competing emphases and unresolved tensions concerning automation and human interpretation, standardization and local adaptation, and intelligence sharing and organizational control, which are examined below.

The synthesis suggests that the traditional socio-technical principle of jointly optimizing social and technical systems [17] remains relevant to CTI but must be applied under conditions that distinguish CTI from many other organizational information systems. Socio-technical alignment in CTI cannot be treated as a one-time design objective because threat actors, vulnerabilities, intelligence sources, regulatory requirements, and organizational priorities change continuously. CTI also operates under adversarial information conditions in which external actors may conceal their activities, manipulate signals, or deliberately disseminate misleading information. Furthermore, CTI frequently extends beyond the boundaries of a single organization to include intelligence providers, sharing communities, technology vendors, managed-security services, regulators, and partner organizations. Sharing across these boundaries may improve collective intelligence while simultaneously increasing confidentiality, legal, reputational, and data-sovereignty risks. The review therefore contextualizes socio-technical alignment for CTI by emphasizing the continuous coordination of social and technical capabilities across organizational boundaries under conditions of uncertainty, time pressure, and adversarial change.

Figure 2 integrates the findings into a conceptual framework of socio-technical alignment in organizational CTI practice. The framework proposes that social-system capabilities, including expertise, leadership, trust, and learning, and technical-system capabilities, including data, platforms, standards, automation, and CTI lifecycle tasks, enable or constrain the interaction mechanisms through which CTI is operationalized. These mechanisms include strategic direction, business translation, human involvement in automated analysis, workflow integration, and sharing governance. For clarity, the figure groups the detailed interaction factors in Table 4 into broader mechanisms. Their configuration influences CTI effectiveness, organizational integration, and sustainability. These outcomes subsequently contribute to reduced uncertainty, risk-informed decision-making, resilience, and business continuity. The relationships are conditioned by adversarial change, regulation, available resources, the threat and risk landscape, local workflows, and organizational maturity. CTI outcomes also generate feedback through learning and reconfiguration, enabling organizations to adjust their social and technical capabilities over time. The framework therefore moves beyond presenting factors as separate categories by proposing how their alignment may produce CTI and organizational outcomes. Because these relationships are derived analytically from the reviewed literature, the framework should be understood as a conceptual synthesis rather than an empirically validated causal model.

A key tension identified in the literature concerns automation and analyst interpretation. Automation, AI, NLP, and platform-based processing can improve the speed, scalability, and consistency of CTI activities, particularly when organizations face large volumes of heterogeneous threat data [15, 26]. Nevertheless, CTI derives its value from combining data with human insight [15], and CTI capabilities contribute to cybersecurity performance only when organizations can interpret, internalize, and operationalize the resulting intelligence [16]. Automation should therefore be understood as complementing and reconfiguring analysts' work rather than simply replacing their expertise. This conclusion is consistent with Mumford's (1999) examination of decision-making in complex socio-technical environments [80], which provides a theoretical warning against marginalizing human agency in high-risk technical

systems. It also reflects Nissen's (2012) critique of treating knowledge primarily as an object to be managed [81]. From this perspective, investment in feeds, platforms, and automated processing cannot substitute for supporting the analysts who provide contextual interpretation and convert threat data into organizational knowledge. Advances in generative AI may shift the boundary between automated processing and human analysis, but the reviewed evidence does not establish whether advanced language models can achieve parity with human analysts in contextual interpretation, source evaluation, accountability, or resistance to adversarial manipulation. Future research should therefore compare human-led, AI-assisted, and highly automated CTI configurations and examine their effects on intelligence quality, analyst interpretation, organizational learning, trust, and decision outcomes.

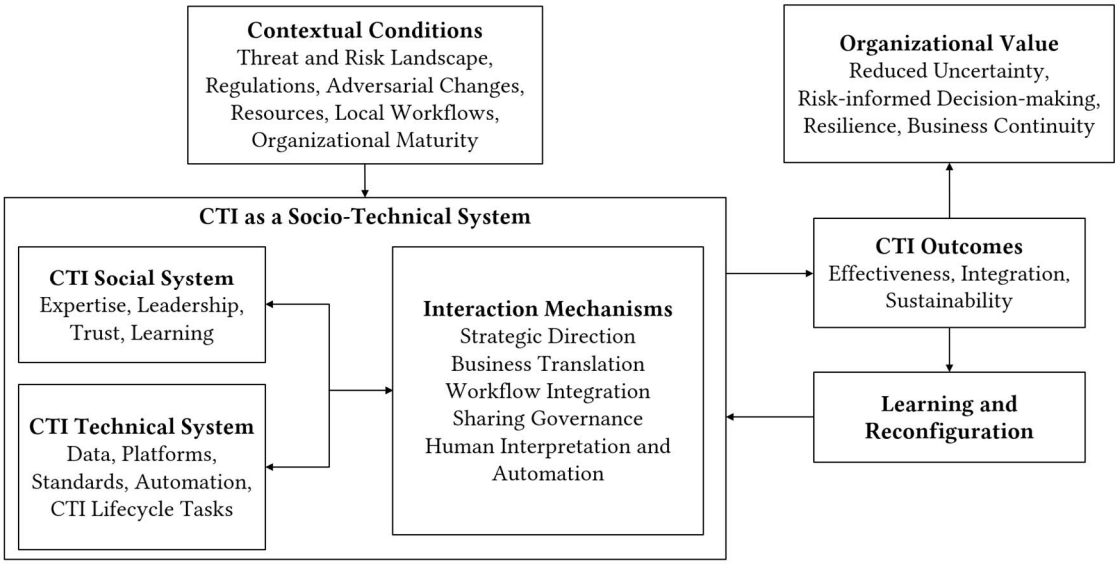


Figure 2: Conceptual framework of socio-technical alignment in organizational CTI practice

Note: Arrows represent theoretically proposed enabling, constraining, and feedback relationships synthesized from the reviewed literature; they do not represent empirically validated causal effects.

Another important tension concerns standardization and organizational context. Standards and protocols such as STIX and TAXII, together with sharing platforms such as MISP, can improve interoperability, structured exchange, and automation. However, their practical value depends on organizational compatibility, staff learning capacity, terminology comprehension, and integration into local CTI routines [34]. This dependency is consistent with Bednar's (2000) contextual perspective on Information Systems, according to which information acquires meaning through individual sensemaking shaped by prior knowledge, while individual and organizational learning remain closely intertwined [82]. Standardized technical representations therefore cannot, by themselves, ensure a common interpretation or effective organizational use of threat information. They become operationally valuable when personnel understand their terminology, adapt them to local requirements, and embed them in existing security practices through training, communication, and organizational learning. Organizations should

therefore regard standards as enabling mechanisms rather than automatic solutions to CTI sharing and integration problems.

Trust, governance, auditability, and data sovereignty also appear as central socio-technical concerns. CTI sharing is often constrained by confidentiality, privacy, regulatory uncertainty, legal liability, reputational risk, and concerns over control of shared intelligence. Technical mechanisms such as policy enforcement, certification, usage control, federated data spaces, and deidentification can support sharing, but they must be connected to governance arrangements that provide accountability and trust [65]. Similarly, auditability and reproducibility are important because decision-makers may hesitate to rely on summarized intelligence if they cannot understand how risk conclusions were produced [13]. These findings suggest that trusted CTI practice depends not only on accurate information, but also on transparent processes, traceable evidence, and governance mechanisms that make intelligence use defensible.

The review further shows that CTI sharing should be understood as a socio-technical ecosystem practice. Interorganizational sharing depends on platforms and standards, but also on trust, reciprocity, incentives, legal alignment, resource capacity, and community participation [15, 76]. Arisian et al. (2025) [75] extend this argument by showing that CTI-sharing platforms gain value only when organizations have incentives to invest in cyber readiness, contribute intelligence, and participate in collective resilience mechanisms. This indicates that CTI sharing cannot be reduced to the movement of threat data between organizations. It also requires economic, institutional, legal, and relational conditions that make sharing safe, useful, and sustainable.

These findings imply that improving CTI practice should be approached as the design of an integrated socio-technical work system rather than primarily as a technology-acquisition problem. This orientation is consistent with Alter's (2019) work-system perspective, which adapts socio-technical thinking to contemporary agile, lean, and data-driven knowledge-work environments [83]. Organizations should therefore begin by defining their intelligence requirements and decision-making needs, involving strategic stakeholders in CTI direction and planning, and designing workflows that connect intelligence producers, analysts, security operations, and organizational decision-makers. These workflows should incorporate feedback mechanisms and translate technical outputs into business-relevant risk and decision information. Organizations must also invest in analyst development, maintain sufficient internal capability to assess outsourced CTI services, and establish governance mechanisms supporting trust, auditability, accountability, and data protection. Technical improvements in data quality, automation, interoperability, and platform integration should subsequently be selected and configured according to these organizational requirements and use cases. CTI capability should therefore be evaluated not simply by the number of feeds acquired or the volume of data processed, but by how effectively the combined configuration of people, processes, tasks, and technologies supports organizational decisions and responses. In practice, the conceptual framework can guide a joint review by analysts, managers, and intelligence users to identify where requirements, tools, responsibilities, and workflows are misaligned and to agree on improvements. Progress can then be assessed through the relevance and timeliness of

intelligence for specific decisions, its use in organizational responses, and its effects on analyst workload and opportunities for learning.

This review also has implications for CTI research. Future studies should empirically examine the relationships proposed in **Figure 2** and determine how contextual conditions, including organizational maturity, regulation, resource availability, sourcing arrangements, and threat intensity, shape these relationships. Rather than continuing to present isolated factor lists, research should investigate how CTI work is enacted across technical, operational, managerial, and strategic levels. Particular attention should be given to the interaction between CTI platforms and analyst interpretation, especially in contexts involving AI, automation, and decision support. Further research is also needed to explain how technical intelligence is translated into business value, financial risk, and strategic decisions. Studies of SMEs and other resource-constrained organizations could clarify how outsourcing, limited expertise, and budget constraints produce distinct socio-technical configurations and challenges. Interorganizational CTI sharing should similarly be examined as an ecosystem phenomenon in which trust, incentives, governance, legal constraints, resource differences, and technical interoperability jointly influence participation and sustainability.

This study has limitations. The review was limited to selected academic databases and English-language peer-reviewed literature, which may have excluded relevant practitioner reports, industry frameworks, or regional CTI practices. In addition, the socio-technical interaction factors and the relationships represented in the conceptual framework were synthesized from existing literature and have not yet been empirically validated through practitioner interviews, organizational case studies, or other empirical methods. Future research could therefore use qualitative case studies, surveys, design science research, and longitudinal methods to examine how these factors interact in practice and how CTI capabilities evolve over time. Despite these limitations, the review provides a structured basis for understanding CTI as a socio-technical practice shaped by the joint configuration of people, organizations, governance arrangements, and technical infrastructures.

5. Conclusion

This systematic literature review examined CTI practice in organizations through a socio-technical systems lens. The review identified three groups of factors shaping CTI practice: social-system factors, technical-system factors, and socio-technical interaction factors. The findings show that CTI practice depends on analyst expertise, leadership support, organizational maturity, governance, resources, data quality, automation, platforms, standards, and interoperability. However, the main contribution of this review is the finding that these factors do not operate independently. CTI becomes valuable when social and technical systems are aligned.

The review shows that effective CTI practice requires the translation of technical threat information into organizationally meaningful intelligence. Technical CTI outputs must be connected to business priorities, risk assessment, decision-making, and operational workflows. Skilled analysts are needed to interpret and contextualize intelligence, while governance mechanisms are needed to support trust, auditability, accountability, and responsible sharing. Similarly, CTI-sharing platforms and standards are useful only when supported by incentives,

trust, legal clarity, organizational capability, and shared practices. These findings indicate that CTI should not be viewed merely as a technical artifact, a platform function, or an information-sharing mechanism, but as a socio-technical organizational practice. Aligning these elements can support risk-informed decision-making, organizational resilience, and business continuity.

Declaration on Generative AI

During the preparation of this work, the author used ChatGPT (OpenAI) in order to check grammar and spelling. After using the tool, the author critically reviewed and edited the outputs and takes full responsibility for the publication's content.

References

[1] B. Shin, P. B. Lowry, A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished, Comput. Secur. 92 (2020) 101761. doi:10.1016/j.cose.2020.101761.

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

[3] M. Lundgren, A. Padyab, A Review of Cyber Threat (Artificial) Intelligence in Security Management, in: T. Sipola, T. Kokkonen, M. Karjalainen (Eds.), Artificial Intelligence and Cybersecurity: Theory and Applications, Springer International Publishing, Cham, 2023, pp. 29–45. URL: https://doi.org/10.1007/978-3-031-15030-2_2. doi:10.1007/978-3-031-15030-2_2.

[4] A. Aliyu, Y. He, I. Yevseyeva, C. Luo, Cyber Security Decision Making Informed by Cyber Threat Intelligence (CYDETI): IEEE CNS 20 Poster, in: 2020 IEEE Conference on Communications and Network Security (CNS), 2020 IEEE Conference on Communications and Network Security (CNS), 2020, pp. 1–2. URL: https://ieeexplore.ieee.org/abstract/document/9162162. doi:10.1109/CNS48642.2020.9162162.

[5] K. Oosthoek, C. Doerr, Cyber Threat Intelligence: A Product Without a Process?, Int. J. Intell. CounterIntelligence 34 (2021) 300–315. doi:10.1080/08850607.2020.1780062.

[6] J. Kotsias, A. Ahmad, R. Scheepers, Adopting and integrating cyber-threat intelligence in a commercial organisation, Eur. J. Inf. Syst. 32 (2023) 35–51. doi:10.1080/0960085X.2022.2088414.

[7] W. Tounsi, H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, Comput. Secur. 72 (2018) 212–233. doi:10.1016/j.cose.2017.09.001.

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

[9] G. Baxter, I. Sommerville, Socio-technical systems: From design methods to systems engineering, Interact. Comput. 23 (2011) 4–17. doi:10.1016/j.intcom.2010.07.003.

[10] I. Sommerville, Designing software for a million users – It's not about the technology (Keynote), in: Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS 2015), 2015, pp. 1–4.

[11] A. Berndt, J. Ophoff, Exploring the Value of a Cyber Threat Intelligence Function in an Organization, in: L. Drevin, S. Von Solms, M. Theocharidou (Eds.), Information Security Education. Information Security in Action, Springer International Publishing, Cham, 2020, pp. 96–109. doi:10.1007/978-3-030-59291-2_7.

[12] S. Ainslie, A. Ahmad, D. Thompson, S. Maynard, The practice of cyber-threat intelligence in organizations: A socio-technical case study of a mature financial organization, Comput. Secur. 168 (2026) 104930. doi:10.1016/j.cose.2026.104930.
[13] T. Xin, Y. He, E. D. Zamani, M. Evans, C. Luo, A cyber risk economics model for organization-wide risk management (CYREM-ORM), Comput. Secur. 165 (2026) 104873. doi:10.1016/j.cose.2026.104873.
[14] S. Sarker, S. Chatterjee, X. Xiao, A. Elbanna, The Sociotechnical Axis of Cohesion for the is Discipline: Its Historical Legacy and its Continued Relevance1, MIS Q. 43 (2019) 695–719. doi:10.25300/MISQ/2019/13747.
[15] C. Abraham, F. Bélanger, S. Daultrey, Promoting research on cyber threat intelligence sharing in ecosystems, J. Cybersecurity 11 (2025) tyaf016. doi:10.1093/cybsec/tyaf016.
[16] T.-S. Chang, Z.-L. Chao, Cybersecurity performance: the impact of integrative cyber threat intelligence capability and information security innovation management capability, Inf. Comput. Secur. ahead-of-print (2026) 1–24. doi:10.1108/ICS-08-2025-0335.
[17] R. P. Bostrom, J. S. Heinen, MIS Problems and Failures: A Socio-Technical Perspective, MIS Q. 1 (1977) 17–32. doi:10.2307/248710.
[18] J. Webster, R. T. Watson, Analyzing the Past to Prepare for the Future: Writing a Literature Review, MIS Q. 26 (2002) xiii–xxiii.
[19] J. Fereday, E. Muir-Cochrane, Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development, Int. J. Qual. Methods 5 (2006) 80–92. doi:10.1177/160940690600500107.
[20] S. T. Fife, J. D. Gossner, Deductive Qualitative Analysis: Evaluating, Expanding, and Refining Theory, Int. J. Qual. Methods 23 (2024) 16094069241244856. doi:10.1177/16094069241244856.
[21] E. Wynn, H. Vallo Hult, Qualitative and Critical Research in Information Systems and Human Computer Interaction: Divergent and Convergent Paths, Found. Trends® Inf. Syst. 3 (2019) 1–233. doi:10.1561/2900000014.
[22] S. Alter, Sociotechnical systems through a work system lens: A possible path for reconciling system conceptualizations, business realities, and humanist values in IS development, in: Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS 2015), CEUR Workshop, 2015, pp. 32–39. URL: https://ceur-ws.org/Vol-1374/paper3.pdf.
[23] W. Alkalabi, L. Simpson, H. Morarji, Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia, in: Proceedings of the 2021 Australasian Computer Science Week Multiconference, Association for Computing Machinery, New York, NY, USA, 2021, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3437378.3437391. doi:10.1145/3437378.3437391.
[24] M. N. S. Miazi, M. M. A. Pritom, M. Shehab, B. Chu, J. Wei, The Design of Cyber Threat Hunting Games: A Case Study, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1–6. URL: https://ieeexplore.ieee.org/document/8038527. doi:10.1109/ICCCN.2017.8038527.
[25] A. Zibak, A. Simpson, Can We Evaluate the Impact of Cyber Security Information Sharing?, in: 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2018, pp. 1–2. URL: https://ieeexplore.ieee.org/document/8551462. doi:10.1109/CyberSA.2018.8551462.
[26] I. Aldasoro, S. Doerr, L. Gambacorta, S. Notra, T. Oliviero, D. Whyte, Generative Artificial Intelligence and Cyber Security in Central Banking, J. Financ. Regul. (2024) fjae008. doi:10.1093/jfr/fjae008.

[27] M. van Haastrecht, G. Golpur, G. Tzismadia, R. Kab, C. Priboi, D. David, A. Răcătăian, L. Baumgartner, S. Fricker, J. F. Ruiz, E. Armas, M. Brinkhuis, M. Spruit, A Shared Cyber Threat Intelligence Solution for SMEs, Electronics 10 (2021) 2913. doi:10.3390/electronics10232913.

[28] Y. Xu, Y. Yang, Y. He, A Representation of Business Oriented Cyber Threat Intelligence and the Objects Assembly, in: 2020 10th International Conference on Information Science and Technology (ICIST), 2020 10th International Conference on Information Science and Technology (ICIST), 2020, pp. 105–113. URL: https://ieeexplore.ieee.org/document/9202271. doi:10.1109/ICIST49303.2020.9202271.

[29] A. Zibak, C. Sauerwein, A. Simpson, A success model for cyber threat intelligence management platforms, Comput. Secur. 111 (2021) 102466. doi:10.1016/j.cose.2021.102466.

[30] A. Zibak, A. Simpson, Towards Better Understanding of Cyber Security Information Sharing, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019, pp. 1–8. URL: https://ieeexplore.ieee.org/document/8899697. doi:10.1109/CyberSA.2019.8899697.

[31] W. Xiong, R. Lagerström, Threat modeling – A systematic literature review, Comput. Secur. 84 (2019) 53–69. doi:10.1016/j.cose.2019.03.010.

[32] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, L. J. García Villalba, A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence, Future Internet 12 (2020) 108. doi:10.3390/fi12060108.

[33] M. S. Abu, S. R. Selamat, A. Ariffin, R. Yusof, Cyber Threat Intelligence – Issue and Challenges, Indones. J. Electr. Eng. Comput. Sci. 10 (2018) 371–379. doi:10.11591/ijeecs.v10.i1.pp371-379.

[34] N. Gong, Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study, in: K. Arai, S. Kapoor, R. Bhatia (Eds.), Intelligent Computing, Springer International Publishing, Cham, 2019, pp. 666–684. doi:10.1007/978-3-030-01177-2_49.

[35] G. Amato, S. Ciccarone, P. Digregorio, G. Natalucci, A Service Architecture for an Enhanced Cyber Threat Intelligence Capability, in: A. Armando, M. Colajanni (Eds.), Proceedings of the Italian Conference on Cybersecurity (ITASEC 2021), volume 2940 of CEUR Workshop Proceedings, CEUR, 2021, pp. 436–446. URL: https://ceur-ws.org/Vol-2940/#paper37.

[36] H. D. Pambudhi, R. F. Aji, Evaluation of Cyber Threat Intelligence Maturity Models: A Comparison Based on Maturity Model Design Principles, in: 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), 2022, pp. 105–110. URL: https://ieeexplore.ieee.org/document/10038112. doi:10.1109/ICICyTA57421.2022.10038112.

[37] T.-S. Chang, H.-Y. Hsu, Critical Resource Factors for Cyber Threat Intelligence Implementation in Enterprises, IEEE Trans. Eng. Manag. 73 (2026) 432–447. doi:10.1109/TEM.2025.3639939.

[38] C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, Association for Computing Machinery, New York, NY, USA, 2016, pp. 65–70. URL: https://dl.acm.org/doi/10.1145/2994539.2994546. doi:10.1145/2994539.2994546.

[39] C. Sauerwein, I. Pekaric, M. Felderer, R. Breu, An analysis and classification of public information security data sources used in research and practice, Comput. Secur. 82 (2019) 140–155. doi:10.1016/j.cose.2018.12.011.

[40] S. Gong, C. Lee, BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance, Electronics 9 (2020) 521. doi:10.3390/electronics9030521.
[41] S. Brown, J. Gommers, O. Serrano, From Cyber Security Information Sharing to Threat Management, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, Association for Computing Machinery, New York, NY, USA, 2015, pp. 43–49. URL: https://dl.acm.org/doi/10.1145/2808128.2808133. doi:10.1145/2808128.2808133.
[42] Y. Keim, A. K. Mohapatra, Cyber threat intelligence framework using advanced malware forensics, Int. J. Inf. Technol. 14 (2022) 521–530. doi:10.1007/s41870-019-00280-3.
[43] S. Bromander, M. Swimmer, L. P. Muller, A. Jøsang, M. Eian, G. Skjøtskift, F. Borg, Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange, Digit. Threats 3 (2021) 6:1-6:22. doi:10.1145/3458027.
[44] H. Griffioen, T. Booij, C. Doerr, Quality Evaluation of Cyber Threat Intelligence Feeds, in: M. Conti, J. Zhou, E. Casalicchio, A. Spognardi (Eds.), Applied Cryptography and Network Security, Springer International Publishing, Cham, 2020, pp. 277–296. doi:10.1007/978-3-030-57878-7_14.
[45] C. Wagner, A. Dulaunoy, G. Wagener, A. Iklody, 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, Association for Computing Machinery, New York, NY, USA, 2016, pp. 49–56. URL: https://dl.acm.org/doi/10.1145/2994539.2994542. doi:10.1145/2994539.2994542.
[46] A. Ramsdale, S. Shiaeles, N. Kolokotronis, A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages, Electronics 9 (2020) 824. doi:10.3390/electronics9050824.
[47] M. Mundt, H. Baier, Towards Mitigation of Data Exfiltration Techniques Using the MITRE ATT&CK Framework, in: P. Gladyshev, S. Goel, J. James, G. Markowsky, D. Johnson (Eds.), Digital Forensics and Cyber Crime, Springer International Publishing, Cham, 2022, pp. 139–158. doi:10.1007/978-3-031-06365-7_9.
[48] C. Krasznay, G. Gyebnár, Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems, in: 2021 13th International Conference on Cyber Conflict (CyCon), 2021 13th International Conference on Cyber Conflict (CyCon), 2021, pp. 171–188. URL: https://ieeexplore.ieee.org/document/9468289. doi:10.23919/CyCon51939.2021.9468289.
[49] T. D. Wagner, E. Palomar, K. Mahbub, A. E. Abdallah, Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper), in: J. K. Liu, P. Samarati (Eds.), Information Security Practice and Experience, Springer International Publishing, Cham, 2017, pp. 576–586. doi:10.1007/978-3-319-72359-4_35.
[50] T. Chantzios, P. Koloveas, S. Skiadopoulos, N. Kolokotronis, C. Tryfonopoulos, V.-G. Bilali, D. Kavallieros, The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform:, in: Proceedings of the 8th International Conference on Data Science, Technology and Applications, 8th International Conference on Data Science, Technology and Applications, SCITEPRESS - Science and Technology Publications, Prague, Czech Republic, 2019, pp. 369–376. URL: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0007978103690376. doi:10.5220/0007978103690376.
[51] L. Sadlek, P. Čeleda, D. Tovarňák, Current Challenges of Cyber Threat and Vulnerability Identification Using Public Enumerations, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA, 2022, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3538969.3544458. doi:10.1145/3538969.3544458.

[52] D. R. Arikkat, V. P., R. R. K.a., S. Nicolazzo, A. Nocera, G. Timpau, M. Conti, OSTIS: A novel Organization-Specific Threat Intelligence System, Comput. Secur. 145 (2024) 103990. doi:10.1016/j.cose.2024.103990.

[53] R. Puranam, S. Sharma, S. Das, Role of Behavioural Factors in Cyber Threat Intelligence, in: TENCON 2022 - 2022 IEEE Region 10 Conference (TENCON), TENCON 2022 - 2022 IEEE Region 10 Conference (TENCON), 2022, pp. 1–6. URL: https://ieeexplore.ieee.org/document/9978135. doi:10.1109/TENCON55691.2022.9978135.

[54] R. R. Ramnani, K. Shivaram, S. Sengupta, A. K. M., Semi-Automated Information Extraction from Unstructured Threat Advisories, in: Proceedings of the 10th Innovations in Software Engineering Conference, Association for Computing Machinery, New York, NY, USA, 2017, pp. 181–187. URL: https://dl.acm.org/doi/10.1145/3021460.3021482. doi:10.1145/3021460.3021482.

[55] C. B. Basha, S. Aggarwal, N. Esanmurodova, H. Alabdeli, A. Tiwari, G. Sathi, S. Ritwika, Fostering Effective Cyber Threat Intelligence Sharing: Overcoming Challenges and Implementing Best Practices, in: 2023 International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD), 2023 International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD), 2023, pp. 177–182. URL: https://ieeexplore.ieee.org/document/10585133. doi:10.1109/ICTEASD57136.2023.10585133.

[56] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, X. Niu, TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources, in: Proceedings of the 33rd Annual Computer Security Applications Conference, Association for Computing Machinery, New York, NY, USA, 2017, pp. 103–115. URL: https://dl.acm.org/doi/10.1145/3134600.3134646. doi:10.1145/3134600.3134646.

[57] M. R. Rahman, R. Mahdavi-Hezaveh, L. Williams, What are the attackers doing now? Automating cyber threat intelligence extraction from text on pace with the changing threat landscape: A survey, ACM Comput. Surv. 55 (2023) 1–36. doi:10.1145/3571726.

[58] C. Sullivan, E. Burger, "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence, Comput. Law Secur. Rev. 33 (2017) 14–29. doi:10.1016/j.clsr.2016.11.015.

[59] P. H. S. Gontijo, R. de Oliveira Albuquerque, J. J. C. Gondim, Operationalizing Structured Direction and Planning for Cyber Threat Intelligence: A Practical Implementation for the Brazilian Financial System, in: 2025 IEEE International Conference on Big Data (BigData), 2025 IEEE International Conference on Big Data (BigData), 2025, pp. 6847–6852. ISSN: 2573-2978. URL: https://ieeexplore.ieee.org/document/11401892. doi:10.1109/BigData66926.2025.11401892.

[60] P. H. S. Gontijo, F. B. de Oliveira, R. de Oliveira Albuquerque, J. J. C. Gondim, Structured Direction and Planning for Cyber Threat Intelligence in the Brazilian Financial System, in: 2025 Workshop on Communication Networks and Power Systems (WCNPS), 2025 Workshop on Communication Networks and Power Systems (WCNPS), 2025, pp. 1–7. ISSN: 2768-0045. URL: https://ieeexplore.ieee.org/document/11295925. doi:10.1109/WCNPS69127.2025.11295925.

[61] J. Voutilainen, M. Kari, Strategic Cyber Threat Intelligence: Building the Situational Picture with Emerging Technologies, in: Proceedings of the 19th European Conference on Cyber Warfare, The 19th European Conference on Cyber Warfare, ACPI, 2020. URL: https://www.academic-conferences.org/wp-content/uploads/dlm_uploads/2020/07/ECCWS-abstract-booklet-FINAL.pdf#page=101. doi:10.34190/EWS.20.030.

[62] Y. Xu, Y. Yang, Y. He, A Business Process Oriented Dynamic Cyber Threat Intelligence Model, in: 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2019, pp. 648–653. URL: https://ieeexplore.ieee.org/document/9060169. doi:10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00147.

[63] C. Sauerwein, C. Sillaber, R. Breu, Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes, in: MKWI, Multikonferenz Wirtschaftsinformatik (MKWI) 2018, 2018, pp. 1333–1344. URL: https://api.semanticscholar.org/CorpusID:54573968.

[64] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, B.-T. Chu, Data-driven analytics for cyber-threat intelligence and information sharing, Comput. Secur. 67 (2017) 35–58. doi:10.1016/j.cose.2017.02.005.

[65] M. A. Gurabi, Ö. Sen, N. Rahimidanesh, A. Ulbig, S. Decker, Enhancing Cyber Threat Intelligence Sharing through Data Spaces in Critical Infrastructures, in: 2025 IEEE International Conference on Cyber Security and Resilience (CSR), 2025 IEEE International Conference on Cyber Security and Resilience (CSR), 2025, pp. 83–90. URL: https://ieeexplore.ieee.org/document/11130001. doi:10.1109/CSR64739.2025.11130001.

[66] R. Lewis, P. Louvieris, P. Abbott, N. Clewley, K. Jones, Cybersecurity information sharing: A framework for information security management in UK SME supply chains, in: 2014. Accepted: 2015-01-28T10:27:36Z. URL: http://bura.brunel.ac.uk/handle/2438/9977.

[67] A. Albakri, E. Boiten, R. Smith, Risk Assessment of Sharing Cyber Threat Intelligence, in: I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, A. Sasse (Eds.), Computer Security, Springer International Publishing, Cham, 2020, pp. 92–113. doi:10.1007/978-3-030-66504-3_6.

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

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

[70] O. Serrano, L. Dandurand, S. Brown, On the Design of a Cyber Security Data Sharing System, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, Association for Computing Machinery, New York, NY, USA, 2014, pp. 61–69. URL: https://dl.acm.org/doi/10.1145/2663876.2663882. doi:10.1145/2663876.2663882.

[71] A. Albakri, E. Boiten, R. De Lemos, Risks of Sharing Cyber Incident Information, in: Proceedings of the 13th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA, 2018, pp. 1–10. URL: https://dl.acm.org/doi/10.1145/3230833.3233284. doi:10.1145/3230833.3233284.

[72] F. Skopik, G. Settanni, R. Fiedler, A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing, Comput. Secur. 60 (2016) 154–176. doi:10.1016/j.cose.2016.04.003.

[73] A. Zibak, A. Simpson, Cyber Threat Information Sharing: Perceived Benefits and Barriers, in: Proceedings of the 14th International Conference on Availability, Reliability and

Security, Association for Computing Machinery, New York, NY, USA, 2019, pp. 1–9. URL: https://dl.acm.org/doi/10.1145/3339252.3340528. doi:10.1145/3339252.3340528.
[74] J. Rajamäki, A. Feyesa, A. Nepal, E-EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector, Eur. Conf. Cyber Warf. Secur. 23 (2024) 398–406. doi:10.34190/eccws.23.1.2073.
[75] S. Arisian, K. Halat, A. Hafezalkotob, R. Maskey, Coopetitive Resilience: Integrating Cyber Threat Intelligence Platforms in Critical Supply Chains, Transp. Res. Part E Logist. Transp. Rev. 197 (2025) 104043. doi:10.1016/j.tre.2025.104043.
[76] B. Dissanayake, M. Thinyane, Challenges and Opportunities for Cross-Domain Cyber Threat Intelligence Sharing Towards Whole-of-Society Resilience, Eur. Conf. Cyber Warf. Secur. 24 (2025) 753–761. doi:10.34190/eccws.24.1.3570.
[77] K. Henttonen, J. Rajamäki, CTI Sharing Practices and MISP Adoption in Finland's Critical Infrastructure Protection, Eur. Conf. Cyber Warf. Secur. 23 (2024). URL: https://papers.academic-conferences.org/index.php/eccws/article/view/2352. doi:10.34190/eccws.23.1.2352.
[78] N. Ntingi, P. Duvenage, J. du Toit, S. von Solms, Effective Cyber Threat Hunting: Where and how does it fit?, Eur. Conf. Cyber Warf. Secur. 21 (2022) 206–213. doi:10.34190/eccws.21.1.240.
[79] P. Bednar, M. Sadok, Information Security: Still Not my Job!, in: R. Agrifoglio, A. Lazazzara, S. Za (Eds.), Navigating Digital Transformation: Organizational Change, Digital Work, and Individual Behavior, Springer Nature Switzerland, Cham, 2024, pp. 63–74. URL: https://doi.org/10.1007/978-3-031-76970-2_5. doi:10.1007/978-3-031-76970-2_5.
[80] E. Mumford, Dangerous Decisions: Problem Solving in Tomorrow's World, Springer US, Boston, MA, 1999. URL: http://link.springer.com/10.1007/b102291. doi:10.1007/b102291.
[81] H.-E. Nissen, What or whom do knowledge-managers manage?, in: Proc. Eur. Conf. Knowl. Manage., ECKM, Proceedings of the European Conference on Knowledge Management, ECKM, 2012, pp. 839–847. journalAbbreviation: Proc. Eur. Conf. Knowl. Manage., ECKM.
[82] P. M. Bednar, A Contextual Integration of Individual and Organizational Learning Perspectives as Part of IS Analysis, Informing Sci. Int. J. Emerg. Transdiscipl. 3 145–156.
[83] S. Alter, Applying Socio-technical Thinking in the Competitive, Agile, Lean, Data-Driven World of Knowledge Work and Smart, Service-Oriented, Customer-Centric Value Creation Ecosystems, Complex Syst. Inform. Model. Q. (2019) 1–22. doi:10.7250/csimq.2019-18.01.

A. Included studies

Table 5 contains all papers included in the results.

Table 5
List of included papers

ID	Article
A1	Y. Xu, Y. Yang, Y. He, A Business Process Oriented Dynamic Cyber Threat Intelligence Model, in: 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2019, pp. 648–653. doi:10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00147.
A2	A. Ramsdale, S. Shiaeles, N. Kolokotronis, A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages, Electronics 9 (2020) 824. doi:10.3390/electronics9050824.
A3	T. Xin, Y. He, E. D. Zamani, M. Evans, C. Luo, A cyber risk economics model for organization-wide risk management (CYREM-ORM), Comput. Secur. 165 (2026) 104873. doi:10.1016/j.cose.2026.104873.
A4	A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, L. J. García Villalba, A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence, Future Internet 12 (2020) 108. doi:10.3390/fi12060108.
A5	F. Skopik, G. Settanni, R. Fiedler, A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing, Comput. Secur. 60 (2016) 154–176. doi:10.1016/j.cose.2016.04.003.
A6	Y. Xu, Y. Yang, Y. He, A Representation of Business Oriented Cyber Threat Intelligence and the Objects Assembly, in: 2020 10th International Conference on Information Science and Technology (ICIST), 2020, pp. 105–113. doi:10.1109/ICIST49303.2020.9202271.
A7	B. Shin, P. B. Lowry, A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished, Comput. Secur. 92 (2020) 101761. doi:10.1016/j.cose.2020.101761.
A8	G. Amato, S. Ciccarone, P. Digregorio, G. Natalucci, A Service Architecture for an Enhanced Cyber Threat Intelligence Capability, in: A. Armando, M. Colajanni (Eds.), Proceedings of the Italian Conference on Cybersecurity (ITASEC 2021), volume 2940 of CEUR Workshop Proceedings, CEUR, 2021, pp. 436–446. URL: https://ceur-ws.org/Vol-2940/#paper37.
A9	M. van Haastrecht, G. Golpur, G. Tzismadia, R. Kab, C. Priboi, D. David, A. Răcătăian, L. Baumgartner, S. Fricker, J. F. Ruiz, E. Armas, M. Brinkhuis, M. Spruit, A Shared Cyber Threat Intelligence Solution for SMEs, Electronics 10 (2021) 2913. doi:10.3390/electronics10232913.

ID	Article
A10	A. Zibak, C. Sauerwein, A. Simpson, A success model for cyber threat intelligence management platforms, Comput. Secur. 111 (2021) 102466. doi:10.1016/j.cose.2021.102466.
A11	W. Tounsi, H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, Comput. Secur. 72 (2018) 212–233. doi:10.1016/j.cose.2017.09.001.
A12	J. Kotsias, A. Ahmad, R. Scheepers, Adopting and integrating cyber-threat intelligence in a commercial organisation, Eur. J. Inf. Syst. 32 (2023) 35–51. doi:10.1080/0960085X.2022.2088414.
A13	C. Sauerwein, I. Pekaric, M. Felderer, R. Breu, An analysis and classification of public information security data sources used in research and practice, Comput. Secur. 82 (2019) 140–155. doi:10.1016/j.cose.2018.12.011.
A14	W. Alkalabi, L. Simpson, H. Morarji, Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia, in: Proceedings of the 2021 Australasian Computer Science Week Multiconference, Association for Computing Machinery, New York, NY, USA, 2021, pp. 1–8. doi:10.1145/3437378.3437391.
A15	N. Gong, Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study, in: K. Arai, S. Kapoor, R. Bhatia (Eds.), Intelligent Computing, Springer International Publishing, Cham, 2019, pp. 666–684. doi:10.1007/978-3-030-01177-2_49.
A16	S. Gong, C. Lee, BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance, Electronics 9 (2020) 521. doi:10.3390/electronics9030521.
A17	A. Zibak, A. Simpson, Can We Evaluate the Impact of Cyber Security Information Sharing?, in: 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2018, pp. 1–2. doi:10.1109/CyberSA.2018.8551462.
A18	B. Dissanayake, M. Thinyane, Challenges and Opportunities for Cross-Domain Cyber Threat Intelligence Sharing Towards Whole-of-Society Resilience, Eur. Conf. Cyber Warf. Secur. 24 (2025) 753–761. doi:10.34190/eccws.24.1.3570.
A19	P. H. S. Gontijo, R. de Oliveira Albuquerque, J. J. C. Gondim, Operationalizing Structured Direction and Planning for Cyber Threat Intelligence: A Practical Implementation for the Brazilian Financial System, in: 2025 IEEE International Conference on Big Data (BigData), 2025, pp. 6847–6852. doi:10.1109/BigData66926.2025.11401892.
A20	S. Arisian, K. Halat, A. Hafezalkotob, R. Maskey, Coopetitive Resilience: Integrating Cyber Threat Intelligence Platforms in Critical Supply Chains, Transp. Res. Part E Logist. Transp. Rev. 197 (2025) 104043. doi:10.1016/j.tre.2025.104043.
A21	T.-S. Chang, H.-Y. Hsu, Critical Resource Factors for Cyber Threat Intelligence Implementation in Enterprises, IEEE Trans. Eng. Manag. 73 (2026) 432–447. doi:10.1109/TEM.2025.3639939.

ID	Article
A22	K. Henttonen, J. Rajamäki, CTI Sharing Practices and MISP Adoption in Finland's Critical Infrastructure Protection, Eur. Conf. Cyber Warf. Secur. 23 (2024). doi:10.34190/eccws.23.1.2352.
A23	P. Alaeifar, S. Pal, Z. Jadidi, M. Hussain, E. Foo, Current approaches and future directions for Cyber Threat Intelligence sharing: A survey, J. Inf. Secur. Appl. 83 (2024) 103786. doi:10.1016/j.jisa.2024.103786.
A24	L. Sadlek, P. Čeleda, D. Tovarňák, Current Challenges of Cyber Threat and Vulnerability Identification Using Public Enumerations, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA, 2022, pp. 1–8. doi:10.1145/3538969.3544458.
A25	A. Aliyu, Y. He, I. Yevseyeva, C. Luo, Cyber Security Decision Making Informed by Cyber Threat Intelligence (CYDETI): IEEE CNS 20 Poster, in: 2020 IEEE Conference on Communications and Network Security (CNS), 2020, pp. 1–2. doi:10.1109/CNS48642.2020.9162162.
A26	A. Zibak, A. Simpson, Cyber Threat Information Sharing: Perceived Benefits and Barriers, in: Proceedings of the 14th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA, 2019, pp. 1–9. doi:10.1145/3339252.3340528.
A27	M. S. Abu, S. R. Selamat, A. Ariffin, R. Yusof, Cyber Threat Intelligence – Issue and Challenges, Indones. J. Electr. Eng. Comput. Sci. 10 (2018) 371–379. doi:10.11591/ijeecs.v10.i1.pp371-379.
A28	Y. Keim, A. K. Mohapatra, Cyber threat intelligence framework using advanced malware forensics, Int. J. Inf. Technol. 14 (2022) 521–530. doi:10.1007/s41870-019-00280-3.
A29	K. Oosthoek, C. Doerr, Cyber Threat Intelligence: A Product Without a Process?, Int. J. Intell. CounterIntelligence 34 (2021) 300–315. doi:10.1080/08850607.2020.1780062.
A30	S. Ainslie, D. Thompson, S. Maynard, A. Ahmad, Cyber-threat intelligence for security decision-making: A review and research agenda for practice, Comput. Secur. 132 (2023) 103352. doi:10.1016/j.cose.2023.103352.
A31	R. Lewis, P. Louvieris, P. Abbott, N. Clewley, K. Jones, Cybersecurity information sharing: A framework for sustainable information security management in UK SME supply chains, in: Proceedings of the European Conference on Information Systems (ECIS 2014), 2014. URL: https://aisel.aisnet.org/ecis2014/proceedings/track14/4/.
A32	T.-S. Chang, Z.-L. Chao, Cybersecurity performance: the impact of integrative cyber threat intelligence capability and information security innovation management capability, Inf. Comput. Secur. ahead-of-print (2026) 1–24. doi:10.1108/ICS-08-2025-0335.
A33	C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and

ID	Article
	Collaborative Security, Association for Computing Machinery, New York, NY, USA, 2016, pp. 65–70. doi:10.1145/2994539.2994546.
A34	S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, B.-T. Chu, Data-driven analytics for cyber-threat intelligence and information sharing, Comput. Secur. 67 (2017) 35–58. doi:10.1016/j.cose.2017.02.005.
A35	J. Rajamäki, A. Feyesa, A. Nepal, E-EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector, Eur. Conf. Cyber Warf. Secur. 23 (2024) 398–406. doi:10.34190/eccws.23.1.2073.
A36	N. Ntingi, P. Duvenage, J. du Toit, S. von Solms, Effective Cyber Threat Hunting: Where and how does it fit?, Eur. Conf. Cyber Warf. Secur. 21 (2022) 206–213. doi:10.34190/eccws.21.1.240.
A37	M. A. Gurabi, Ö. Sen, N. Rahimidanesh, A. Ulbig, S. Decker, Enhancing Cyber Threat Intelligence Sharing through Data Spaces in Critical Infrastructures, in: 2025 IEEE International Conference on Cyber Security and Resilience (CSR), 2025, pp. 83–90. doi:10.1109/CSR64739.2025.11130001.
A38	H. D. Pambudhi, R. F. Aji, Evaluation of Cyber Threat Intelligence Maturity Models: A Comparison Based on Maturity Model Design Principles, in: 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), 2022, pp. 105–110. doi:10.1109/ICICyTA57421.2022.10038112.
A39	C. B. Basha, S. Aggarwal, N. Esanmurodova, H. Alabdeli, A. Tiwari, G. Sathi, S. Ritwika, Fostering Effective Cyber Threat Intelligence Sharing: Overcoming Challenges and Implementing Best Practices, in: 2023 International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD), 2023, pp. 177–182. doi:10.1109/ICTEASD57136.2023.10585133.
A40	S. Brown, J. Gommers, O. Serrano, From Cyber Security Information Sharing to Threat Management, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, Association for Computing Machinery, New York, NY, USA, 2015, pp. 43–49. doi:10.1145/2808128.2808133.
A41	I. Aldasoro, S. Doerr, L. Gambacorta, S. Notra, T. Oliviero, D. Whyte, Generative Artificial Intelligence and Cyber Security in Central Banking, J. Financ. Regul. (2024) fjae008. doi:10.1093/jfr/fjae008.
A42	C. Sullivan, E. Burger, "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence, Comput. Law Secur. Rev. 33 (2017) 14–29. doi:10.1016/j.clsr.2016.11.015.
A43	S. Bromander, M. Swimmer, L. P. Muller, A. Jøsang, M. Eian, G. Skjøtskift, F. Borg, Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange, Digit. Threats 3 (2021) 6:1–6:22. doi:10.1145/3458027.
A44	C. Wagner, A. Dulaunoy, G. Wagener, A. Iklody, 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, Association for Computing Machinery, New York, NY, USA, 2016, pp. 49–56. doi:10.1145/2994539.2994542.

ID	Article
A45	O. Serrano, L. Dandurand, S. Brown, On the Design of a Cyber Security Data Sharing System, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, Association for Computing Machinery, New York, NY, USA, 2014, pp. 61–69. doi:10.1145/2663876.2663882.
A46	D. R. Arikkat, V. P., R. R. K.A., S. Nicolazzo, A. Nocera, G. Timpau, M. Conti, OSTIS: A novel Organization-Specific Threat Intelligence System, Comput. Secur. 145 (2024) 103990. doi:10.1016/j.cose.2024.103990.
A47	C. Krasznay, G. Gyebnár, Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems, in: 2021 13th International Conference on Cyber Conflict (CyCon), 2021, pp. 171–188. doi:10.23919/CyCon51939.2021.9468289.
A48	C. Abraham, F. Bélanger, S. Daultrey, Promoting research on cyber threat intelligence sharing in ecosystems, J. Cybersecurity 11 (2025) tyaf016. doi:10.1093/cybsec/tyaf016.
A49	H. Griffioen, T. Booij, C. Doerr, Quality Evaluation of Cyber Threat Intelligence Feeds, in: M. Conti, J. Zhou, E. Casalicchio, A. Spognardi (Eds.), Applied Cryptography and Network Security, Springer International Publishing, Cham, 2020, pp. 277–296. doi:10.1007/978-3-030-57878-7_14.
A50	T. D. Wagner, E. Palomar, K. Mahbub, A. E. Abdallah, Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper), in: J. K. Liu, P. Samarati (Eds.), Information Security Practice and Experience, Springer International Publishing, Cham, 2017, pp. 576–586. doi:10.1007/978-3-319-72359-4_35.
A51	A. Albakri, E. Boiten, R. Smith, Risk Assessment of Sharing Cyber Threat Intelligence, in: I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, A. Sasse (Eds.), Computer Security, Springer International Publishing, Cham, 2020, pp. 92–113. doi:10.1007/978-3-030-66504-3_6.
A52	A. Albakri, E. Boiten, R. De Lemos, Risks of Sharing Cyber Incident Information, in: Proceedings of the 13th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA, 2018, pp. 1–10. doi:10.1145/3230833.3233284.
A53	R. Puranam, S. Sharma, S. Das, Role of Behavioural Factors in Cyber Threat Intelligence, in: TENCON 2022 - 2022 IEEE Region 10 Conference (TENCON), 2022, pp. 1–6. doi:10.1109/TENCON55691.2022.9978135.
A54	R. R. Ramnani, K. Shivaram, S. Sengupta, A. K. M., Semi-Automated Information Extraction from Unstructured Threat Advisories, in: Proceedings of the 10th Innovations in Software Engineering Conference, Association for Computing Machinery, New York, NY, USA, 2017, pp. 181–187. doi:10.1145/3021460.3021482.
A55	C. Sauerwein, C. Sillaber, R. Breu, Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes, in: Multikonferenz Wirtschaftsinformatik (MKWI) 2018, 2018, pp. 1333–1344. URL: https://api.semanticscholar.org/CorpusID:54573968.

ID	Article
A56	V. Jesus, B. Bains, V. Chang, Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence, IEEE Trans. Eng. Manag. 71 (2024) 6854–6873. doi:10.1109/TEM.2023.3279274.
A57	J. Voutilainen, M. Kari, Strategic Cyber Threat Intelligence: Building the Situational Picture with Emerging Technologies, in: Proceedings of the 19th European Conference on Cyber Warfare, ACPI, 2020. doi:10.34190/EWS.20.030.
A58	P. H. S. Gontijo, F. B. de Oliveira, R. de Oliveira Albuquerque, J. J. C. Gondim, Structured Direction and Planning for Cyber Threat Intelligence in the Brazilian Financial System, in: 2025 Workshop on Communication Networks and Power Systems (WCNPS), 2025, pp. 1–7. doi:10.1109/WCNPS69127.2025.11295925.
A59	M. N. S. Miazi, M. M. A. Pritom, M. Shehab, B. Chu, J. Wei, The Design of Cyber Threat Hunting Games: A Case Study, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1–6. doi:10.1109/ICCCN.2017.8038527.
A60	S. Ainslie, A. Ahmad, D. Thompson, S. Maynard, The practice of cyber-threat intelligence in organizations: A socio-technical case study of a mature financial organization, Comput. Secur. 168 (2026) 104930. doi:10.1016/j.cose.2026.104930.
A61	T. Chantzios, P. Koloveas, S. Skiadopoulos, N. Kolokotronis, C. Tryfonopoulos, V.-G. Bilali, D. Kavallieros, The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform, in: Proceedings of the 8th International Conference on Data Science, Technology and Applications, SCITEPRESS - Science and Technology Publications, Prague, Czech Republic, 2019, pp. 369–376. doi:10.5220/0007978103690376.
A62	W. Xiong, R. Lagerström, Threat modeling – A systematic literature review, Comput. Secur. 84 (2019) 53–69. doi:10.1016/j.cose.2019.03.010.
A63	A. Zibak, A. Simpson, Towards Better Understanding of Cyber Security Information Sharing, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019, pp. 1–8. doi:10.1109/CyberSA.2019.8899697.
A64	M. Mundt, H. Baier, Towards Mitigation of Data Exfiltration Techniques Using the MITRE ATT&CK Framework, in: P. Gladyshev, S. Goel, J. James, G. Markowsky, D. Johnson (Eds.), Digital Forensics and Cyber Crime, Springer International Publishing, Cham, 2022, pp. 139–158. doi:10.1007/978-3-031-06365-7_9.
A65	G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, X. Niu, TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources, in: Proceedings of the 33rd Annual Computer Security Applications Conference, Association for Computing Machinery, New York, NY, USA, 2017, pp. 103–115. doi:10.1145/3134600.3134646.
A66	M. R. Rahman, R. Mahdavi-Hezaveh, L. Williams, What are the attackers doing now? Automating cyber threat intelligence extraction from text on pace with the changing threat landscape: A survey, ACM Comput. Surv. 55 (2023) 1–36. doi:10.1145/3571726.

B. Database search queries

The following search queries were used for Web of Science and Scopus:

Web of Science and Scopus
("Cyber threat intelligence" OR "Cyber threat hunting" OR "Cyber threat model*" OR "Cyber threat analysis" OR "Adversary intelligence" OR "adversary intelligence") AND (Practice OR Adopt* OR Direct* OR Plan* OR Gathering OR Collect* OR Shar* OR Disseminat* OR Process* OR Analys* OR Analyz* OR Feedback OR implement* OR integrat* OR capability OR matur* OR "intelligence cycle" OR "intelligence Process" OR "decision-making" OR "Framework" OR "Case study" OR "Case-study") AND (Organization OR Organizations OR Corporate OR Corporat* OR Compan* OR Business* OR Enterprise* OR Management OR Regulatory OR Compliance OR Commercial OR Firm OR SME* OR "small and medium enterprise*")

IEEE Xplore
Due to IEEE Xplore's limit of a maximum of 10 wildcard characters per query at the time the search was conducted, selected wildcard terms were replaced with explicit term variants while preserving the original search logic as closely as possible.

(("Cyber threat intelligence" OR "Cyber threat hunting" OR "Cyber threat model*" OR "Cyber threat analysis" OR "Adversary intelligence") AND (Practice OR Adopt OR Adoption OR Adopting OR Adoptation OR Direct* OR Plan* OR Gathering OR Collect OR Collecting OR Collection OR Collections OR Shar* OR Disseminat* OR Process OR Processes OR Processing OR Processor OR Processors OR Analysis OR Analys OR Analyzing OR Feedback OR implement* OR integrat* OR capability OR Mature OR Maturity OR "intelligence cycle" OR "intelligence Process" OR "decision-making" OR "Framework" OR "Case study" OR "Case-study") AND (Organization OR Organizations OR Corporate OR Corporat* OR Compan* OR Business* OR Enterprise OR Enterprises OR Management OR Regulatory OR Compliance OR Commercial OR Firm OR SME OR SMEs OR "small and medium enterprise" OR "small and medium enterprises"))