Trust and Trust-Building Policies to Support Cybersecurity Information Sharing: A Systematic Literature Review

Richard Posso[1] and Jörn Altmann[1,2]

[1] Technology Management, Economics and Policy Program
College of Engineering, Seoul National University, Seoul, South Korea

[2] Integrated Major in Smart City Global Convergence
Seoul National University, Seoul, South Korea

richardposso@gmail.com, jorn.altmann@acm.org

Abstract. Cybersecurity threats information (CTI) sharing protects firms and stakeholders from cyberattacks and avoid security vulnerabilities. However, despite these benefits of CTI sharing, firms are still unwilling to share due to barriers and challenges related to a lack of trust. Some studies explored the significance of trust in sharing cyber security information, but further studies are required to determine what dimensions compose trust, which processes support trust, and what trust building policies have been enacted to foster the sharing of information in cybersecurity ecosystems, which is the main purpose of this review. The deliverables from this review present 25 trust dimensions, 6 main processes supporting trust, and 30 trust government policies enacted to foster trust and sharing in cybersecurity. These outcomes enable the creation of a framework for building trust in cybersecurity ecosystems and facilitating the cyberthreat information sharing.

Keywords: trust, cybersecurity, information sharing, trust dimensions, trust processes, trust-building policies.

1 Introduction

The widespread use of technology and digital platforms worldwide expanded cyberattacks to every organization and individuals [1]. In 2022, data breaches affected around 53 million people only in USA [2] costing approximately USD $4.35 million per data breach [3]. Due to increased cyber dangers, firms cannot afford to defend themselves isolated from the threat environment. Hence, threat information exchange is essential in cybersecurity domain [4]. Cybersecurity threats information sharing (CTI) helps stakeholders anticipate and avoid security vulnerabilities [5].

1.1 Trust Role in Cybersecurity

Despite the benefits of CTI sharing, companies are still unwilling to engage in sharing due to barriers and challenges [6], such as fear to personal information leakage, risk of exploitation, reputation loss [7], privacy and civil liberties (citizens' trust in governments), loss of customer trust [6], socio-cultural (trust and confidence), technological, legal and regulatory, operational [8], confidentiality, trust management, trust on information, risk assessments [9], legal, technological (lack of interoperability), collaborative (trust between firms), and organizational cost [10]. Among these challenges and barriers, lack of trust is one of the major ones [6] because of its fragility [11]. Previous studies explored the significance of trust in sharing prediction information [12], but further studies are needed to determine what parameters, processes, and trust building policies influence trust in cybersecurity. Conventional classification to study trust suggests two categories: service requesters (trustees) and service providers (trustors) [13, 14]. When addressing CTI, an alternative approach suggests three types: trust of partner to platform (TPP) [15–20], trust between partners (TBP) [15–18, 21], and trust of partner to information (TPI) [15, 17, 22]. This classification gives a thorough review of trust and suggests dimensions and correlations between and within trust kinds that must be explored.

1.2 Stakeholders and Trust Types in Cybersecurity Ecosystems

The key cybersecurity players in trust building and information exchange are service providers, insurance providers, security groups, security administrators, government, data source providers, information providers, standardization organizations, and end users. A stakeholder can play more than one role depending on the ecosystem's foundations. For this study, cybersecurity stakeholders are categorized as platform, partner, or information provider.

Trust of partners to platform. Trusting the platform provider enhances partner collaboration, because platform security supports cyber community participation [17]. Stakeholders with roles for this category are service providers or insurance providers.

Trust between partners. This trust type is essential for CTI sharing because of its sensitivity [17]. Therefore, only the most trusted partners will receive secret information. Partners' trust and motivation to share falls, if free riders are included in the ecosystem. To improve dependability and incentivize CTI sharing between partners, reputation systems are suggested [17] [15]. Stakeholders belonging to this category are cybersecurity groups, administrators, government, and end users.

Trust of partners to information. Partners' trust in CTI is a major factor affecting the ecosystem. Cybersecurity teams must trust information to face threats. Thus, cybersecurity memberships require strong trust in CTI [17]. Stakeholders fitting into this category are data providers, information providers, and standardization organizations.

2 Methodology

2.1 Methodology Overview

This study adopted Okoli's (2015) standalone systematic literature review (SLR) methodology, to guarantee explicit and reproducible research. Fig. 1 shows the process to carry out the SLR in 9 steps. Claiming SLR's main goal is conducted by identifying a broad research gap (step 1). The next step involves finding and evaluating review papers (step 2). This step supports research questions formulation and originality (step 3). The next step defines keywords to gather all the relevant papers (step 4). Four databases (Scopus, Web of Science, ACM Digital Library, IEEE Xplore) were chosen for the search, and customized search queries for each database were formulated (step 5). An initial number of 4790 articles were collected. By screening these articles and applying the inclusion and exclusion criteria (step 6), the number could be reduced to 490 articles. Quality appraisal of the article reduced the number to 87 articles (step 7). Data extraction is performed using Zotero version 6 (step 8), on which the analysis is performed (step 9).

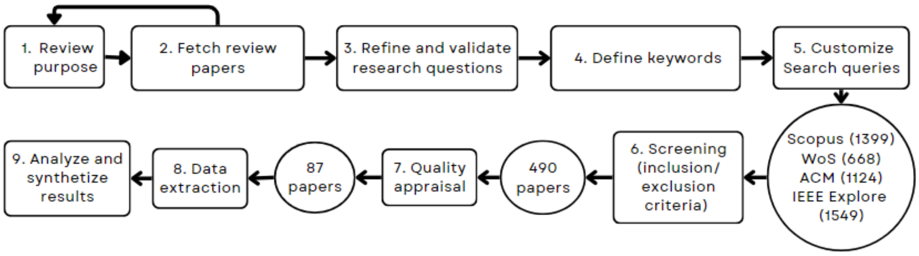

Fig. 1. Systematic literature review steps.

Review Papers. This step supports research gap and review relevance. Table presents the different topics that trust in cybersecurity review papers have addressed. Trust in data networks includes IoT [23, 24], wireless [25], mobile [26–29], P2P [30], and cloud computing [25, 31, 32]. Reviews also studied trust taxonomy [23, 24, 31, 32], trust management [25, 27, 28, 30], and trust evaluation [26, 29, 33]. In addition, researchers studied some trust dimensions such as similarity, timeliness [27], decentralization, privacy [28], asymmetry, sensitivity [24], and reputation [30].

Research gap. Despite these efforts to disclose trust dimensions, more work is needed to describe how trust types in cybersecurity ecosystems are linked to trust dimensions and what interrelationships exist between them. Table 1 shows that some reviews studied processes such dissemination [25], maintenance [29], or transference [33], but no connection between them was researched. Trust management includes some processes, but it is unclear which processes maintain, build, or disseminate trust in cybersecurity ecosystems. Thus, additional studies are needed to unveil the processes that promote trust in cybersecurity. Moreover, reviews studied trust security policies [32] but focused only on internal security policies, excluding external regulations. Thus, studies of trust government policies and their interaction are needed.

Research Relevance. Table 1 also shows that no systematic evaluation has examined trust dimensions and their relationships, trust processes, and trust-building policies to leverage CTI. Understanding current research and emerging trust challenges and trends for these topics in cybersecurity ecosystems is relevant to face growing concerns about cyber threats and boost cybersecurity information sharing.

Research Questions. The literature reviews include trust taxonomy, management, and evaluation, but the relationship between cybersecurity trust dimensions remains unknown. So, RQ1 was formulated. What are the dimensions of trust required for building trust in cybersecurity information sharing ecosystems? Table 1 also illustrates that most review papers present trust processes scattered in different areas. Thus, RQ2 was formulated. What processes have been implemented to increase trust in cybersecurity information sharing ecosystem? Table 1 also shows that trust regulations in cybersecurity ecosystem are understudied. Thus, RQ3 is proposed. What government policies have been enacted to support trust and increase information sharing in cybersecurity ecosystems?

Research Keywords. As seen in Fig. 1, step 4 shows keyword sets created to find all relevant papers: trust* AND (“cybersecurity” OR "network security" OR "cyber-security" OR "security of data" OR "cyber security" OR "information security" OR "security of information") AND ("information" OR "data") AND (“sharing”). All these strings used cybersecurity, information, and the asterisk (*).

Table 1. Comparison of review articles on trust in cybersecurity.

Study	Focus of review	Trust for Security of Data Networks					Trust Taxonomy	Trust Management	Trust Evaluation	Trust Dimensions	Trust Processes	Trust Policies
		IoT	Wireless	Mobile	Peer to Peer	Cloud Computing						
[32]	Trust Architecture					●	●					◖
[23]	Remote attestation (IoT)	●					●					
[27]	Trust Factors (IoV)			●				●		◖		
[25]	Models (WSN, IoT)		●			●		●			◖	
[28]	Trust Models (VANET)			●				●		◖		
[24]	Trust Classification (IoT)	●					●			◖		
[29]	Trust models (MANET)			●					●		◖	
[31]	Network Topology					●	●					
[30]	Reputation Issues (P2P)				●			●		◖		
[33]	Trust Factors								●		◖	
[26]	Trust Initialization (MAS)			●					●			
This Study	Sharing Information, Policies									● RQ1	● RQ2	● RQ3

● Covered ◖ Partially covered

Research Queries. Step 6 presents the research queries. As shown in Table 2, the search queries are adjusted to the syntax of the each databases to get relevant results and avoid missing important articles. Scopus, Web of Science (WoS), ACM Digital Library, and IEEE Xplore were chosen, since they are key sources for citation scientific data in multidisciplinary domains, a strength for this study.

Table 2. Strings queries used in databases.

Database	Query	No.
SCOPUS	TITLE-ABS-KEY (trust* AND (cybersecurity OR cyber-security OR cyber security OR network security OR security of data OR security of information OR information security) AND (information OR data) AND (sharing))	1399
WoS	trust* AND (cybersecurity OR cyber-security OR cyber security OR network security OR security of data OR security of information" OR "information security") AND (information OR data) AND (sharing)	668
ACM Digital Library	AllField:(trust*) AND AllField:(cybersecurity OR "cyber-security" OR "cyber security" OR "network security" OR "security of data" OR "security of information" OR "information security") AND AllField:("information" OR "data ") AND AllField:(sharing)	1124
IEEE Explore	trust* AND(cybersecurity OR"cyber-security" OR"cyber security"OR "network security" OR"security of data"OR "security of information" OR "information security")AND(informationORdata) AND(sharing)	1549
Total Number of Papers		4740

Screening. Step 6 involves screening and applying inclusion and exclusion criteria. Through this stage, 4740 articles were reduced to 490. Fig.2 summarizes this stage, which describes the technical and content criteria applied.

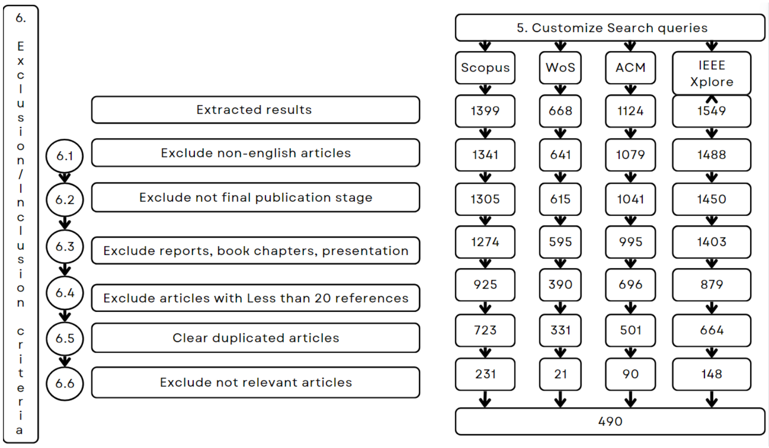

Fig. 2. Inclusion and exclusion criteria applied.

Quality Appraisal. Step 7 comprises the quality appraisal, to identify the most relevant and important papers. The criteria are based on a set of questions proposed by [34, 35] and a tool suggested by [36]. The questions are: Is the paper a research or a discussion based on expert opinion? Is there a clear statement of the research aims? Is there an adequate description of context, in which the research was carried out? Was the research method appropriate to address the aims of the research? Was the data analysis sufficiently rigorous? Is there a clear statement of findings? Is there a clear statement of limitations? Is the study of value for this research?

Data Extraction. The quality rating yields 87 research papers for data extraction (step 8). Zotero version 6 is used to arrange the retrieved study citations.

Analysis of Results. This stage of the systematic literature review is detailed in the next section.

3 Research Results

3.1 Descriptive Analysis

The descriptive analysis includes a keyword co-occurrence of the 87 articles using VOSViewer (version 1.6.18). Fig.3(a) shows 46 keywords in the selected articles that occurred at least three times, generating 3 clusters using Van Eck and Waltman's clustering algorithm [37, 38]. The 3 clusters represent trust dimensions (cybersecurity trust characteristics), trust processes, and trust policies in cybersecurity ecosystems. Additional analysis also included the top occurrences and the keyword link strength. The link strength is the number of articles with identical keywords [38]. Fig.3(b) shows that the top 13 co-occurring terms and their link strength. The terms are trust, information sharing, cyber security, cybersecurity policy, and data secrecy policy. It reveals the significance of these terms in cybersecurity information sharing ecosystems.

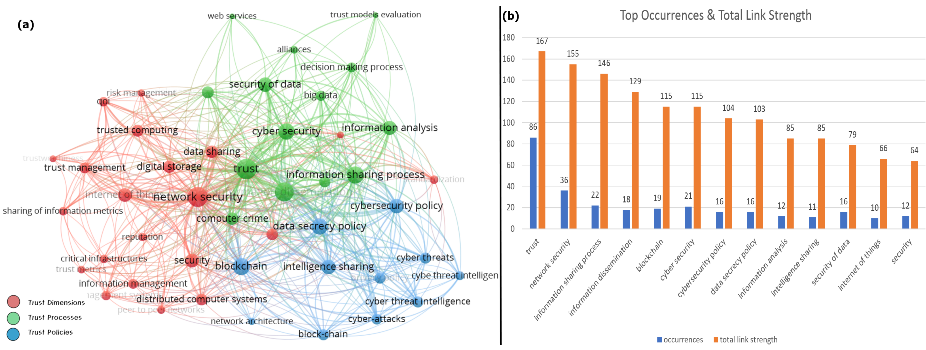

Fig.3. (a) Keyword co-occurrence relationships; **(b)** Top occurrence and keyword link strength.

3.2 Trust Dimensions in Cybersecurity Information Sharing Ecosystems

As seen in Fig.4(a), the research identified 25 trust dimensions that influence the three trust types and motivate CTI sharing.

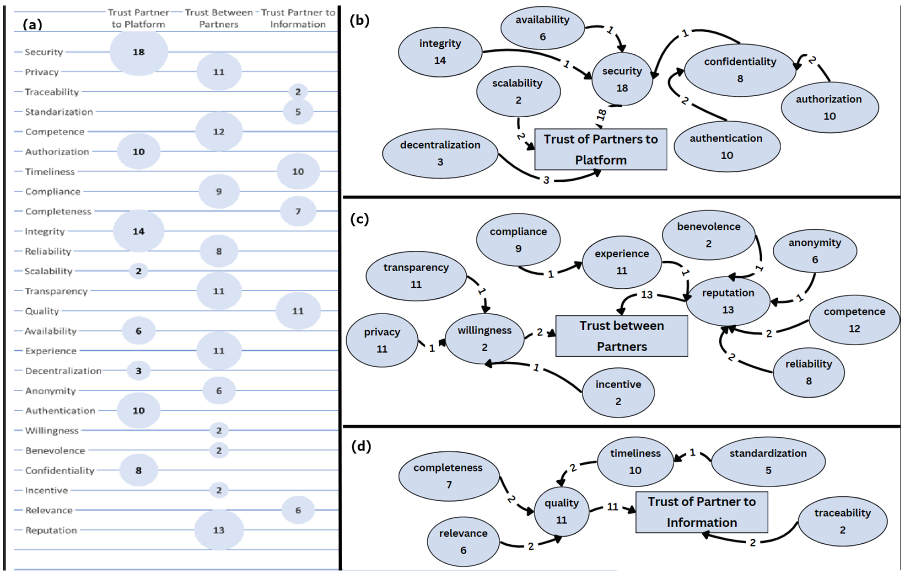

Fig.4. (a) Trust dimensions by trust types; **(b)** TPP; **(c)** TBP; and **(d)** TPI relationships.

Trust of partner to platform (TPP). Fig.4(a) shows that in TPP the most influential trust dimensions are security [17, 39–50] [51–55], integrity [17, 40, 46, 48, 50, 52, 56–63],authorization [15, 17, 20, 48, 50, 51, 61, 64–66], and authentication [15, 20, 22, 45, 48, 50, 56, 61, 66, 67]. The analysis also reveals that confidentiality [7, 17, 47, 48, 50, 59, 68, 69],availability [48, 50, 52, 62, 70, 71], decentralization [44, 65, 72], and scalability [18, 52] play a secondary role in the research of TPP (Fig.4(b)). Some dimensions are influenced by others: integrity, authentication, authorizathion impact security [50]; also impacts security [50]; confidentiality impacts security [68]; authorization [48] and authentication [45] impact confidentiality.

Trust between partners (TBP). Fig.4(a) also reveals that TBP is mostly influenced by dimensions such as reputation [18, 22, 30, 57, 63, 75–78], competence [18, 22, 52, 56, 78, 80], experience [18, 22, 30, 50, 53, 60, 71, 75, 81–83], transparency [17, 21, 30, 42, 47, 49, 61, 64, 81, 84, 85], and privacy [17, 20, 46, 51, 52, 55, 62, 64, 86–88]. Moreover, the analysis also shows secondary dimensions such as compliance [40, 49, 51, 52, 57, 65, 79, 89], reliability [17, 18, 44, 45, 52, 54, 75, 81], and anonymity [17, 18, 41, 51, 67, 72], incentive [40, 74], benevolence [13, 40], and willingness [18, 55]. Fig.4(c) summarizes the different relationships that exist in TBP. First, incentive [65], privacy [87], and transparency [64] have an impact on willingness to trust and share information. Compliance [71] impact experience; experience influences reputation [75], and benevolence [13], competence [75, 76], reliability [17, 75], and anonymity [41] impacts on reputation.

Trust of partner to information. TPI dimensions such as quality [17, 18, 46, 52, 58, 64, 71, 80, 88, 90, 91], and timeliness [17, 18, 52, 53, 75, 90–94] influence trust of partners to information (Fig.4(a)). In addition, completeness [17, 60, 81, 90–93], relevance [17, 41, 54, 90, 92, 93], standardization [39, 52, 60, 89, 95], and traceability [61, 93] constituting secondary influences. As additional analysis shows (Fig.4(d)), TPI quality is impacted by relevance [17, 90], timeliness [17, 90], completeness [17, 90], whereas standardization impacts on timeliness [44].

3.3 Processes to Increase Trust in Cybersecurity Ecosystems

Six processes and their subprocesses, which increase trust in cybersecurity ecosystems, have been identified (Fig.5):

Trust setup process. This phase establishes trust connections for exchanging and transmission of threat information [86] (Fig.5). The setup process is divided into three subprocesses, namely user registration [7, 65, 86], source validation [17, 56, 78, 80, 87, 91, 93], and building trust structure [42, 57, 86, 93, 95–97].

Trust gathering process. The gathered data is used to compute trust by qualitative or quantitative approach [75]. Gathering process is divided into four subprocesses named encryption [7, 17, 42, 86, 87, 98], authentication [14, 17, 20, 56, 59, 65, 69, 86, 87, 97], authorization [7, 20, 41, 44, 51, 61, 66, 69, 71, 94, 95, 99–101], and collection [14, 61, 75, 78, 82, 83].

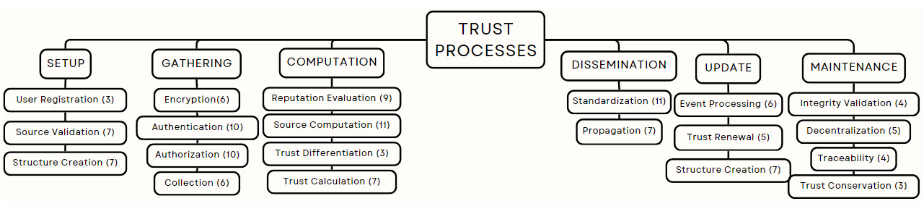

Fig. 5. Trust processes and subprocesses.

Trust computation process. Statistical, probabilistic, or machine learning methods are used during computing [75]. The findings suggest dividing trust computation into four subprocesses: reputation evaluation [42, 44, 71, 76, 86, 90, 91, 95, 96], source computation [7, 17, 41, 46, 48, 65, 85, 87, 91, 93, 102], trust differentiation [44, 89, 93], and trust calculation [16, 44, 52, 56, 61, 75, 76].

Trust dissemination process. This process distributes the computed trust values to partners [7, 95]. Depending on the cybersecurity ecosystem, suitable trust scenarios will implement a centralized or distributed scheme for the dissemination [75]. This process should be divided in two subprocesses: standardization [44, 64, 67, 87, 93, 94, 97, 99, 101, 103, 104], and propagation [7, 83, 95] [52, 56, 75].

Trust update process. It is required to identify the events that trigger a trust update estimation process [75]. The result of this review suggest to partition into two distinct subprocesses: event processing [17, 52, 56, 57, 61, 71], and trust renewal [52, 71, 75, 76, 96].

Trust maintenance process. It not only determines how often trust information needs to be revised [75, 93] but also indicates how often to verify the information source [93]. The process should be partitioned into four distinct subprocesses: integrity validation [17, 46, 61, 87], decentralization [17, 41, 48, 61, 65], traceability [17, 61, 86, 87], and trust conservation [44, 75, 93].

3.4 Trust and Sharing Policies in Cybersecurity

As presented in Fig.6, 30 government initiatives were discovered in primary papers to improve trust or information sharing. These policies also safeguard government, public, and private sector from growing cyberthreats [105].

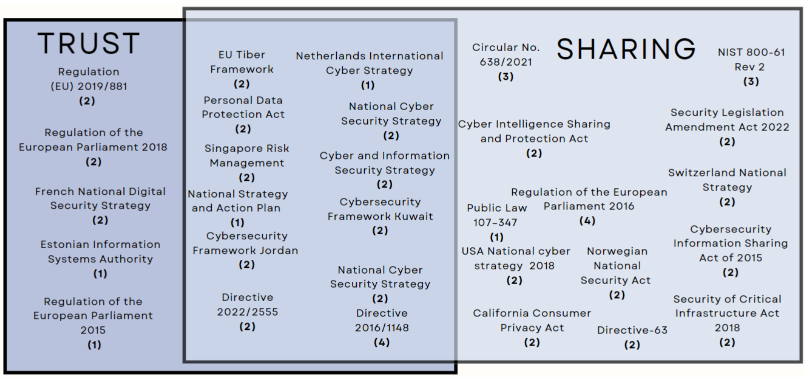

Fig. 6. Trust and sharing policies.

4 Discussion

4.1 Opportunities

This research outlines opportunities to create trustful cybersecurity information sharing ecosystems by identifying trust dimensions, trust processes, and trust policies. So, every stakeholder participating in the ecosystem can get a common trust overview, and collaboration becomes easier with other members. The findings contribute to create a comprehensive cybersecurity information sharing ecosystems, where stakeholders, trust types, trust dimensions, trust processes, and trust policies can be measured to evaluate real trust impact on the ecosystem.

It is an opportunity to standardize and evaluate best practices for trust processes in cybersecurity. These processes can be used for the implementation, testing, and comparison of performance and efficiency between ecosystems. Trust and sharing policies not only provide an outlook about governments' regulations and efforts to promote trust but also frame the trust types relationships under legal boundaries and support trust dimensions enhancement. The results could disrupt traditional approaches for leveraging trust in cybersecurity and improve best practices and policies.

There is also opportunity to overcome trust barriers in cybersecurity ecosystems. Barriers demonstrate current flaws that impede collaboration and trust emerging in cybersecurity ecosystems. Thus, strategies may incorporate dimensions, processes, and policies to overcome barriers. For example, if the aim is to reduce the barrier of ambiguity in regulations, it requires standardization of concepts and clarification about what dimensions should be measured and how to measure them.

Technological solutions can increase the willingness and participation of partners in the proposed framework for trust in cybersecurity ecosystems. Therefore, there is research opportunity to analyze the relationship between incentives, rewards and incorporate the diversity of technologies, to evaluate which solution creates better trusted ecosystem involving trust dimensions, trust processes, and policies compliance. There is also an opportunity to analyze how digital transformation complies with regulations and with trust dimensions. So, the willingness of stakeholders to share information may be strengthened in cybersecurity ecosystems.

4.2 Challenges

One of the main challenges is addressing legal requirements, because regulations are different for each cybersecurity ecosystem. It is vital to adhere to local regulation, to standardize trust concepts, and to establish trust processes for facilitating trust in cybersecurity information sharing ecosystems. Another challenge to achieve the opportunities is to find appropriate real testing environments, in which trust dimensions, processes, and policies can be adjusted, to determine acceptable levels of performance and sustainable ecosystems that can be implemented. A permanent challenge is the gathering of reliable information, to support and validate the different hypothesis in the area. It is recommended to ask the experts in cybersecurity communities, to evaluate how accurate the information obtained from research is applicable to real scenarios.

5 Limitations and Future Research

Despite the systematic literature review and primary study selection, relevant papers or articles may not have been included. These articles may have affected the review's conclusions and comprehensiveness. It also focuses on trust dimensions, processes, and policies that directly affect cybersecurity ecosystem information exchange. This study ignored other cybersecurity aspects. However, evaluating dimensions, processes, and policies in a single setting might provide significant cybersecurity trust outcomes. Generalization may be difficult, since further study and verification may be needed to strengthen the evidence. Outcomes from a single element must be evaluated in numerous contexts, and further scenarios with distinct characteristics must be addressed.

Acknowledgments. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government, Ministry of Science and ICT (MSIT), with project No. NRF-2022R1A2C1092077, NRF-RS-2023-00302083 (as part of the EC-funded Swarmchestrate Project), and BK21 FOUR (Fostering Outstanding Universities for Research) funded by Korea's Ministry of Education (MOE) and the NRF of Korea.

References

1. Takahashi T, Kadobayashi Y (2015) Reference Ontology for Cybersecurity Operational Information. Comput J 58:2297–2312. https://doi.org/10.1093/comjnl/bxu101
2. Statista (2022a) Data breaches and individuals impacted U.S. 2022. In: Statista. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. Accessed 3 Oct 2022
3. IBM (2022) Cost data breach 2022. https://www.ibm.com/reports/data-breach. Access 3 Oct 2022
4. Ali H, Papadopoulos P, Ahmad J, Pitropakis N, Jaroucheh Z, Buchanan WJ (2021) Privacy-Preserving and Trusted Threat Intelligence Sharing Using Distributed Ledgers. 14th Int Conf on (SIN). https://doi.org/10.1109/SIN54109.2021.9699366
5. Rashid Z, Noor U, Altmann J (2021) Economic Model for Evaluating Value Creation Through Information Sharing within the Cybersecurity Information Sharing Ecosystem. https://doi.org/10.1016/j.future.2021.05.033
6. Pala A, Zhuang J (2019) Inf Sharing in Cybersecurity: A Review. https://doi.org/10.1287/deca.2018.0387
7. Vakilinia I, Tosh DK, Sengupta S (2017) Attribute based Sharing in Cybersecurity Information Exchange Framework. In: 2017 International Symposium (SPECTS). IEEE, Seattle, WA, USA, pp 1–6
8. Alkalabi W, Simpson L, Morarji H (2021) Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia. https://doi.org/10.1145/3437378.3437391
9. Bernabe JB, Skarmeta A (2019) Challenges in Cybersecurity and Privacy: The European Research Landscape. River Publishers https://doi.org/10.1201/9781003337492
10. Koepke P (2017) Cybersecurity Information Sharing Incentives and Barriers. MIT, Working Paper CISL# 2017-13
11. Höök K (2000) Steps to Take Before Intelligent User Interfaces Become Real. Interact Comput 12:409–426. https://doi.org/10.1016/S0953-5438(99)00006-5
12. Özer Ö, Zheng Y, Chen K-Y (2011) Trust in Forecast Information Sharing. Manag Sci 57:1111–1137. https://doi.org/10.1287/mnsc.1110.1334
13. Deljoo A, van Engers T, Gommans L, de Laat C (2018) Social Computational Trust Model (SCTM): A Framework to Facilitate Selection of Partners.2018 IEEE/ACM (INDIS). Dallas, TX, USA, pp 45–54

14. Wu Z (2009) A Semantic Approach for Trust Information Exchange in Federation Systems. In: 2009 International Conference on Advanced Information Networking and Applications Workshops. IEEE, Bradford, United Kingdom, pp 25–30

15. Latvala O, Emanuilov I, Niskanen T, Raitio, Salonen, Santos, Yordanova (2022) Proof-of-Concept for a Granular Incident Mngmt Inf Sharing Scheme. In: 2022 IEEE World AI IoT Congress. IEEE, Seattle, WA

16. Qin X, Zhang C, Lei Q, Guo Y (2012) A Trust Model for Data-Sharing in Virtual Communities. In: 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE). IEEE,

17. Wu Y, Qiao Y, Ye Y, Lee B (2019) Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. In: 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS). IEEE, Granada, Spain, pp 474–481

18. Vance A, Benjamin Lowry P, Wilson DW (2017) Using Trust and Anonymity to Expand the use of anonymizing systems that improve security across organizations. https://doi.org/10.1057/sj.2015.22

19. Ud Din I, Bano A, Awan KA, Almogren, Altameem, Guizani (2023) LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things. https://doi.org/10.1109/JIOT.2021.3081422

20. Song H, Yin F, Han X, Luo T, Li J (2022) MPDS-RCA: Multi-level Privacy-Preserving Data Sharing for Resisting Collusion Attacks Based on an Integration of CP-ABE and LDP. Comput Secur 112:102523. https://doi.org/10.1016/j.cose.2021.102523

21. Chen P-K, He Q-R, Chu S (2022) Influence of Blockchain and Smart Contracts on Partners' Trust, Visibility, Competitiveness, and Environmental Performance. https://doi.org/10.3846/jbem.2022.16431

22. Gao Y, Li X, Li J, Gao Y, Yu P (2019) Info-Trust: A Multi-Criteria and Adaptive Trustworthiness Calculation Mechanism for Information Sources. https://doi.org/10.1109/ACCESS.2019.2893657

23. Johnson WA, Ghafoor S, Prowell S (2021) A Taxonomy and Review of Remote Attestation Schemes in Embedded Systems. IEEE Access 9:142390–142410. https://doi.org/10.1109/ACCESS.2021.3119220

24. Ahmed A, Ab Hamid SH, Gani A, Khan S, Khan M (2019) Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. https://doi.org/10.1016/j.jnca.2019.102409

25. Fang W, Zhang W, Chen W, Pan T, Ni , Yang (2020) Trust-Based Attack and Defense in Wireless Sensor Networks:A Survey. Wir Commun Mob Comput 2020:1–20. https://doi.org/10.1155/2020/2643546

26. Lin C, Varadharajan V (2003) Modelling and Evaluating Trust Relationships in Mobile Agents Based Systems. In: Zhou J, Yung M, Han Y (eds) Applied Cryptography and Network Security. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 176–190

27. Siddiqui SA, Mahmood A, Sheng QZ, Suzuki H, Ni W (2021) A Survey of Trust Management in the Internet of Vehicles. Electronics 10:2223. https://doi.org/10.3390/electronics10182223

28. Lu Z, Qu G, Liu Z (2019) A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy.. https://doi.org/10.1109/TITS.2018.2818888

29. Ahmed A, Abu Bakar K, Channa M, Haseeb K, Khan A (2015) A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks.. https://doi.org/10.1007/s11704-014-4212-5

30. Selvaraj C, Anand S (2012) A survey on Security Issues of Reputation Management Systems for Peer-to-Peer Networks. Comput Sci Rev 6:145–160. https://doi.org/10.1016/j.cosrev.2012.04.001
31. Xiang M, Liu W, Bai Q, Al-Anbuky A (2015) Avoiding the Opportunist: The Role of Simmelian Ties in Fostering the Trust in Sensor-Cloud Networks. https://doi.org/10.1155/2015/873941
32. He Y, Huang D, Chen L, Ni Y, Ma X, Huo Y (2022) A Survey on Zero Trust Architecture: Challenges and Future Trends. Wirel Commun Mob Comput 2022:1–13. https://doi.org/10.1155/2022/6476274
33. Luo W, Najdawi M (2004) Trust-building measures: a review of consumer health portals. Commun ACM 47:108–113. https://doi.org/10.1145/962081.962089
34. Dybå T, Dingsøyr T (2008b) Strength of Evidence in Systematic Reviews Sw Engin. pp 178–187
35. Kitchenham BA, Budgen D, Brereton P (2015) Evidence-Based Software Engineering and Systematic Reviews, 0 ed. Chapman and Hall/CRC
36. Okoli C (2015) A Guide to Conducting a Standalone Systematic Literature Review. Commun Assoc Inf Syst 37:. https://doi.org/10.17705/1CAIS.03743
37. Waltman L, Van Eck NJ, Noyons ECM (2010) A Unified Approach to Mapping and Clustering of Bibliometric Networks. J Informetr 4:629–635. https://doi.org/10.1016/j.joi.2010.07.002
38. Van Eck NJ, Waltman L (2023) VOSviewer. https://www.vosviewer.com/features/highlights.
39. Sun N, Li C, Chan H, Dung B, Islam M, Zhang (2022) Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges. https://doi.org/10.1109/ACCESS.2022.3168716
40. Deljoo A, VanEngers T, Koning R, Gommans L, DeLaat C (2018) Towards Trustworthy Information Sharing by Creating Cyber Security Alliances.
41. Lorchat J, Pelsser C, Fontugne R (2014) Collaborative Repository for Cybersecurity Data and Threat Information. In: 2014 Third International Workshop on (BADGERS). IEEE, Wroclaw, pp 83–87
42. Wang K, Dong J, Wang Y, Yin H (2019) Securing Data With Blockchain and AI. IEEE Access 7:77981–77989. https://doi.org/10.1109/ACCESS.2019.2921555
43. Hellwig O, Quirchmay G, Huber E, Golch, Vock, Pospisil (2016) Challenges in Structuring and Institutionalizing CERT-Communication. In: 2016 11th Int Conf. (ARES). IEEE, Salzburg, Austria, pp661–667
44. Steinberger J, Kuhnert B, Sperotto A, Baier H, Pras A (2016) In Whom Do We Trust - Sharing Security Events. In: Badonnel R, Koch R, Pras A, Management and Security in the Age of Hyperconnectivity. Springer International Publishing, Cham, pp 111–124
45. Wachter S (2018) Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR.. https://doi.org/10.1016/j.clsr.2018.02.002
46. Li W, Tan J, Wang Y (2020) A Framework of Blockchain-Based Collaborative Intrusion Detection in Software Defined Networking. In: Kutyłowski M, Zhang J, Chen C (eds) Network and System Security. Springer International Publishing, Cham, pp 261–276
47. Sayed AIE, Aziz MA, Azeem MHA (2020) Blockchain Decentralized IoT Trust Management. In: 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT). IEEE, Sakheer, Bahrain, pp 1–6

48. Saha S, Neogy S, Paul A, Sengupta J (2017) Suitability of Different Cryptographic Approaches for Securing Data Centric Applications. In: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). IEEE, Chennai, pp 603–608

49. Teisserenc B, Sepasgozar S (2021) Adoption of Blockchain Technology through Digital Twins in the Construction Industry 4.0: A PESTELS Approach. https://doi.org/10.3390/buildings11120670

50. Aarthi S, Bharathi N (2022) Analysis of Security and Privacy Issues over Vehicular Communication in Internet Of Vehicles. In: 2022 International Mobile and Embedded Technology Conference (MECON). IEEE, Noida, India, pp 500–505

51. Hernandez J, McKenna L, Brennan R (2022) TIKD: A Trusted Integrated Knowledge Dataspace for Sensitive Data Sharing and Collaboration. In: Curry E, Scerri S, Tuikka T (eds) Data Spaces. Springer International Publishing, Cham, pp 265–291

52. Aslam MJ, Din S, Rodrigues J, Ahmad A, Choi G (2020) Defining Service-Oriented Trust Assessment for Social IoT. IEEE Access 8:206459–206473. https://doi.org/10.1109/ACCESS.2020.3037372

53. Wallis T, Leszczyna R (2022) EE-ISAC—Practical Cybersecurity Solution for the Energy Sector. Energies 15:2170. https://doi.org/10.3390/en15062170

54. Colella A, Castiglione A, De Santis A (2014) The Role of Trust and Co-partnership in the Societal Digital Security Culture Approach. In: 2014 International Conference on Intelligent Networking and Collaborative Systems. IEEE, Salerno, pp 350–355

55. Li G, Fang C-C (2022) Exploring Factors that Influence Information Resources Sharing Intention via the Perspective of Consensus Perception of Blockchain. Inf Technol Manag 23:23–38. https://doi.org/10.1007/s10799-021-00338-4

56. Awan K, Din I, Almogren A, Kim, Altamem (2021) vTrust: An IoT-Enabled Trust-Based Secure Wireless Energy Sharing Mechanism for Vehicular Ad Hoc Networks. Sensors 21:7363. https://doi.org/10.3390/s21217363

57. Lodi G, Baldoni R, Elshaafi H, Mulcahy BP, Csertan G, Gonczy L (2010) Trust Management in Monitoring Financial Critical Information Infrastructures. In: Chatzimisios P, Verikoukis C, Santamaría I, (eds) Mobile Lightweight Wireless Systems. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 427–439

58. Wang Y (2021) Design of Trustworthy Cyber–Physical–Social Systems With Discrete Bayesian Optimization. J Mech Des 143:071702. https://doi.org/10.1115/1.4049532

59. Laufenberg D, Li L, Shahriar H, Han M (2020) Developing a Blockchain-Enabled Collaborative Intrusion Detection System: An Exploratory Study. In: Arai K, Kapoor S, Bhatia R (eds) Advances in Information and Communication. Springer International Publishing, Cham, pp 172–183

60. Habib SM, Vassileva J, Mauw S, Mühlhäuser M (2016) Trust Management X: 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings. Springer International Publishing, Cham

61. Lahbib A, Toumi K, Laouiti A, Laube A, Martin S (2019) Blockchain based Trust Management Mechanism for IoT. In: 2019 IEEE Wireless Communications and Networking Conference.Morocco, pp 1–8

62. Al-Aswad H, El-Medany WM, Balakrishna C, Ababneh (2021) BZKP: Blockchain-based Zero-Knowledge Proof Model for Enhancing Healthcare Security. https://doi.org/10.1080/25765299.2020.1870812

63. Hung Y-TC, Dennis AR, Robert L (2004) Trust in Virtual Teams: Towards an Integrative Model of Trust Formation. In: 37th Annual Hawaii International Conference on System Sciences, 2004..

65. Nguyen K, Pal S, Jadidi Z, Dorri A, Juldak R (2022) A Blockchain-Enabled Incentivised Framework for Cyber Threat Intelligence Sharing in ICS. In: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events IEEE, Pisa, Italy, pp 261–266

66. Huang H, Zhang J, Hu J, Fu Y, Qin C (2022) Research on Distributed Dynamic Trusted Access Control Based on Security Subsystem. https://doi.org/10.1109/TIFS.2022.3206423

67. Tounsi W, Rais H (2018) A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks. Comput Secur 72:212–233. https://doi.org/10.1016/j.cose.2017.09.001

68. Mivule K (2017) Data Swapping for Private Information Sharing of Web Search Logs. Procedia Comput Sci 114:149–158. https://doi.org/10.1016/j.procs.2017.09.017

69. Palmo Y, Tanimoto S, Sato H, Kanai A (2021) A Consideration of Scalability for Software Defined Perimeter Based on the Zero-trust Model. 10th International Congress on Advanced Applied Informatics

70. Zhou S, Zhang G, Meng X (2022) LocTrust: A Local and Global Consensus-Combined Trust Model in MANETs. Peer--Peer Netw Appl 15:355–368. https://doi.org/10.1007/s12083-021-01250-y

71. Elshaafi H, McGibney J, Mulcahy B, Botvich D (2011) Enhancement of Critical Financial Infrastructure Protection Using Trust Management. In: Lee C, Seigneur J-M, Park JJ, Wagner RR (eds) Secure and Trust Computing, Data Management, and Applications. Springer Berlin Heidelberg, Berlin, Heidelberg,

72. Deshpande VM, Nair MK (2018) Towards Trusted Computing-A Novel Holistic Policy Based Approach. In: 2018 3rd International Conference for Convergence in Technology. Pune, pp 1–7

73. Arachchilage NAG, Namiluko C, Martin A (2013) A taxonomy for securely sharing information among others in a trust domain. In: 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). IEEE, London, United Kingdom, pp 296–304

74. Quigley K (2013) "Man plans, God laughs": Canada's national strategy for protecting critical infrastructure: Canada's Strategy for Protecting Critical Infrastructure. https://doi.org/10.1111/capa.12007

75. Awan K, UdDin I, Almogren A, Guizani, Altameem, Jadoon (2019) RobustTrust A Pro-Privacy Robust Distributed Trust Management Mechanism for IoT. https://doi.org/10.1109/ACCESS.2019.2916340

76. Ma Z, Liu L, Meng W (2020) DCONST: Detection of Multiple-Mix-Attack Malicious Nodes Using Consensus-Based Trust in IoT Networks. In: Liu JK, Cui H (eds) Information Security and Privacy. Springer International Publishing, Cham, pp 247–267

77. Purohit S, Calyam P, Wang S, Yempalla R, Varghese J (2020) DefenseChain: Consortium Blockchain for Cyber Threat Intelligence Sharing and Defense. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, Paris, France, pp 112–119

78. Latif R (2022) ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things. IEEE Access 10:46526–46537. https://doi.org/10.1109/ACCESS.2022.3169788

79. Chan K, Cho J-H, Adali S (2012) Composite Trust Model for an Information Sharing Scenario. In: 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing. IEEE, Fukuoka, Japan, pp 439–446

80. Randall RG, Allen S (2021) Cybersecurity Professionals Information Sharing Sources and Networks in the U.S. Electrical Power Industry. https://doi.org/10.1016/j.ijcip.2021.100454

81. Panahifar F, Byrne PJ, Salam MA, Heavey C (2018) Supply Chain Collaboration and Firm's Performance: The Critical Role of Information Sharing and Trust. https://doi.org/10.1108/JEIM-08-2017-0114

82. Ebrahimi M, Haghighi MS, Jolfaei A, Shamaeian N, Tadayon M (2022) A Secure and Decentralized Trust Management Scheme for Smart Health Systems. https://doi.org/10.1109/JBHI.2021.3107339

83. Hoque MA, Hasan R (2022) A Trust Management Framework for Connected Autonomous Vehicles Using Interaction Provenance. In: ICC 2022 - IEEE, Seoul, Korea, Republic of, pp 2236–2241

84. Fischer-Hübner S, Angulo J, Karegar F, Pulls T (2016) Transparency, Privacy and Trust – Technology for Tracking and Controlling My Data Disclosures: Does This Work?

85. Brignoli MA, Mazzaro S, Fortunato G, Cora A, Matta, Romano, Ruggiero, Cosci (2020) Combining exposure indicators and predictive analytics for threats detection in real industrial IoT sensor networks. In: 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT. IEEE, Roma, Italy, pp 423–428

86. Dunnett K, Pal S, Jadidi Z, Putra G, Jurdak R (2022) A Democratically Anonymous and Trusted Architecture for CTI Sharing using Blockchain. In: 2022 International Conference on Computer Communications and Networks (ICCCN). IEEE, Honolulu, HI, USA, pp 1–7

87. Sadique F, Bakhshaliyev K, Springer J, Sengupta S (2019) A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P). In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, Las Vegas, NV, USA, pp 0493–0498

88. Liu P, Chetal A (2005) Trust-based secure information sharing between federal government agencies. J Am Soc Inf Sci Technol 56:283–298. https://doi.org/10.1002/asi.20117

89. Dunnett K, Pal S, Putra G, Jadidi Z, Jurdak (2022) A Trusted, Verifiable and Differential Cyber Threat Intelligence Sharing Framework using Blockchain.

90. Mavzer KB, Konieczna E, Alves H, Yucel, Chalkias I, Mallis D, Cetinkaya D, Sanchez L (2021) Trust and Quality Computation for Cyber Threat Intelligence Sharing Platforms. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, Rhodes, Greece, pp 360–365

91. Gao Y, Li X, Li J, Gao Y, Guo N (2018) Graph Mining-based Trust Evaluation Mechanism with Multidimensional Features for Large-scale Heterogeneous Threat Intelligence. In: 2018 IEEE International Conference on Big Data (Big Data). IEEE, Seattle, WA, USA, pp 1272–1277

92. González G, Faiella M, Medeiros I, Azevedo, Gonzalez S (2021) ETIP: An Enriched Threat Intelligence Platform for Improving OSINT Correlation, https://doi.org/10.1016/j.jisa.2020.102715

93. Schaberreiter T, Kupfersberger V, Rantos K, Spyros, Papanikolaou, Iliudis (2019) A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources. In:

Proceedings of the 14th International Conference on Availability, Reliability and Security. ACM, Canterbury CA United Kingdom, pp 1–10

94. Pahlevan M, Voulkidis A, Velivassaki T-H (2021) Secure exchange of cyber threat intelligence using TAXII and distributed ledger technologies - application for electrical power and energy system. In: The 16th International Conference on Availability, Reliability, Security.Austria, pp 1–8
95. Zhang F, Guo S, Qiu X, Xu , Qi, Wang (2021) Federated Learning Meets Blockchain: State Channel based Distributed Data Sharing Trust Supervision Mechanism. https://doi.org/10.1109/JIOT.2021.3130116
96. Li F, Wang D, Wang Y, Yu X, Wu N, Yu J, Zhou H (2020) Wireless Communications and Mobile Computing Blockchain-Based Trust Management in Distributed IoT. https://doi.org/10.1155/2020/8864533
97. Homan D, Shiel I, Thorpe C (2019) A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology. In: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, CANARY ISLANDS, Spain, pp 1–6
98. Shao S, Gong W, Yang H, Guo S, Chen L, Xiong A (2021) Data Trusted Sharing Delivery: A Blockchain Assisted Software-Defined Content Delivery Network. https://doi.org/10.1109/JIOT.2021.3124091
99. Haque MdF, Krishnan R (2021) Toward Automated Cyber Defense with Secure Sharing of Structured Cyber Threat Intelligence. Inf Syst Front 23:883–896. https://doi.org/10.1007/s10796-020-10103-7
100. Štumpf O, Bureš T, Matěna V (2015) Security and Trust in Data Sharing Smart Cyber-Physical Systems. In: Proceedings of the 2015 European Conference on Software Architecture Workshops. ACM,
101. Yuan E, Wenzel G (2005) Assured Counter-Terrorism Information Sharing Using Attribute Based Information Security (ABIS). In: 2005 IEEE Aerospace Conference. IEEE, Big Sky, MT, pp 1–12
102. Suryotrisongko H, Musashi Y, Tsuneda A, Sugitani K (2022) Robust Botnet DGA Detection: Blending XAI and OSINT for Cyber Threat Intelligence Sharing. https://doi.org/10.1109/ACCESS.2022.3162588
103. Wagner C, Dulaunoy A, Wagener G, Iklody A (2016) MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. ACM, Vienna Austria, pp 49–56
104. Briliyant OC, Tirsa NP, Hasditama MA (2021) Towards an Automated Dissemination Process of Cyber Threat Intelligence Data using STIX. IEEE, Depok, Indonesia, pp 109–114
105. Salomon JM (2022) Public-Private Partnerships and Collective Cyber Defence. In: 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon). IEEE, Tallinn, Estonia, pp 45–63