World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Cyber threat intelligence sharing: A strategic tool for enhancing national and global security postures

Ifeyinwa Nkemdilim Obiokafor [1,*], Moses Okechukwu Onyesolu [2] and Michael Sunday Julius [3]

[1] *Department of Cyber Security, Admiralty University of Nigeria.*
[2] *Department of Computer Science, Nnamdi Azikiwe University, Awka. Nigeria.*
[3] *ICT/Computer Science, Evangel University Akaeze, Nigeria.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 17(02), 444-453

Publication history: Received on 12 October 2025; revised on 18 November 2025; accepted on 20 November 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.17.2.1503

Abstract

In the contemporary digital landscape, cyber threats have become a pervasive and formidable challenge, transcending national borders and posing significant risks to critical infrastructures, economies, and societies worldwide. Cyber Threat Intelligence (CTI) sharing has emerged as a crucial strategy in fortifying both national and global cybersecurity frameworks. This review provides a comprehensive examination of CTI sharing, synthesizing current research on its mechanisms, models, and challenges across governmental, industrial, and international domains. By facilitating the exchange of threat-related information among stakeholders, CTI sharing enhances situational awareness, expedites incident response, and fosters a collaborative defense posture. The strategic importance of CTI sharing lies in its ability to provide timely and actionable intelligence, enabling organizations and nations to detect, prevent, and respond to cyber threats more effectively. This review identifies significant barriers to CTI sharing, including legal constraints, trust deficits, and technological disparities. Despite these challenges, emerging trends such as automation, AI-driven threat detection, and blockchain-facilitated trust models offer promising solutions to enhance the efficacy of CTI sharing. The findings of this review advocate for a globally coordinated, standardized, and incentivized approach to CTI sharing as an indispensable tool in modern cybersecurity policy and practice. By leveraging CTI sharing, organizations and nations can foster collective resilience against evolving cyber threats, ultimately enhancing national and global security postures. This review provides valuable insights for researchers, policymakers, and practitioners seeking to enhance cybersecurity frameworks through CTI sharing.

Keywords: Cyber Threat Intelligence; Cybersecurity Frameworks; Threat Intelligence Sharing; Global Cybersecurity; Threat Detection

1. Introduction

In today's interconnected digital landscape, cyber threats have escalated in both frequency and sophistication, posing significant risks to national security, economic stability, and societal well-being. High-profile incidents such as ransomware attacks on critical infrastructure and widespread data breaches have underscored the vulnerabilities inherent in modern information systems [1, 2, 14]. These challenges are further compounded by the transnational nature of cyber threats, which often outpace the defensive capabilities of individual organizations and nation-states. Cybersecurity has evolved into a national security imperative due to the pervasive digitization of critical infrastructures and geopolitical cyber aggressions. Threats like Advanced Persistent threat (APT), ransomware, cyber-espionage, and supply chain attacks necessitate real-time, cross-jurisdictional intelligence sharing [2, 4]. Cyber Threat Intelligence (CTI) is the systematic collection and dissemination of indicators of compromise (IoCs), tactics, and adversary behaviors that enables proactive defense and mutual reinforcement between nations, sectors, and institutions [20].

* Corresponding author: Obiokafor Ifeyinwa Nkemdilim

Cyber threats have become a pervasive and formidable challenge, transcending national borders and posing significant risks to critical infrastructures, economies, and societies worldwide [2]. The increasing complexity and frequency of cyber-attacks have underscored the need for robust and collaborative cybersecurity strategies that can effectively detect, prevent, and respond to these threats. Against this backdrop, CTI sharing has emerged as a crucial component of modern cybersecurity frameworks, enabling organizations and nations to share threat-related information, best practices, and lessons learned to enhance their collective defense posture [16, 22].

Addressing these evolving threats, CTI sharing has surfaced as a vital strategy for enhancing cybersecurity resilience. CTI sharing involves the dissemination of threat-related information such as indicators of compromise, tactics, techniques, and procedures (TTPs) among stakeholders to facilitate proactive defense measures [16]. By fostering collaboration across governmental, industrial, and international domains, CTI sharing enhances situational awareness, accelerates incident response, and contributes to a collective defense posture [20]. CTI sharing has become a cornerstone of cybersecurity strategies, facilitating the exchange of valuable insights and intelligence among stakeholders to improve situational awareness, expedite incident response, and foster a collaborative defense posture. However, despite its strategic importance, CTI sharing is not without its challenges. Issues such as legal constraints, trust deficits, and technological disparities can hinder the effectiveness of CTI sharing initiatives [1].

The implementation of effective Cyber Threat Intelligence (CTI) sharing mechanisms is hindered by several challenges, including legal and regulatory constraints, data privacy concerns, lack of standardized protocols, and trust issues among stakeholders [1, 8, 21]. Furthermore, disparities in technological capabilities and resource availability across organizations can impede the adoption of CTI sharing practices. Nevertheless, recent technological advancements offer promising solutions to overcome these obstacles. Innovations such as blockchain-based platforms, privacy-preserving data sharing techniques, and automated threat intelligence systems have the potential to address concerns related to data integrity, confidentiality, and interoperability [6, 16, 17, 22]. By leveraging these developments, organizations can create secure, efficient, and trustworthy frameworks for CTI sharing, ultimately strengthening their overall cybersecurity posture and enhancing collective resilience against evolving cyber threats.

This review aims to synthesize current research on CTI sharing, examining its strategic importance, benefits, mechanisms, models, and challenges of CTI sharing across governmental, industrial, and international domains, and the emerging frameworks designed to enhance its efficacy. By analyzing benefits, challenges, emerging trends in CTI sharing, public-private partnerships, multilateral initiatives, and technological innovations, this paper seeks to underscore the strategic role of CTI in fostering collective resilience against evolving cyber threats and advocate for a globally coordinated, standardized, and incentivized approach to CTI sharing as an indispensable tool in modern cybersecurity policy and practice.

1.1. Context and Urgency of Cyber Threats in Modern Geopolitics

The present-day digital landscape is characterized by an escalating threat landscape, where cyber threats have evolved into a pervasive and formidable challenge. These threats transcend national borders, posing significant risks to critical infrastructures, economies, and societies worldwide [1, 12, 20]. The interconnected nature of modern digital ecosystems has created an environment where cyber threats can spread rapidly, causing widespread disruption and damage. As a result, it is imperative for organizations and nations to develop robust and collaborative cybersecurity strategies that can effectively detect, prevent, and respond to these threats. The growing frequency and sophistication of cyberattacks highlight the pressing need for robust cybersecurity measures [20]. These threats pose significant risks, disrupting essential services, destabilizing geopolitical relations, and undermining economic stability. The interconnected nature of global systems means that a cyber incident in one nation can have far-reaching consequences, underscoring the importance of international cooperation and collective cybersecurity efforts. For instance, the 2017 WannaCry ransomware attack affected over 150 countries, and repeated social engineering attack tactics affected over 200 users account in 2023, highlighting the global nature of cyber vulnerabilities [6, 9, 18, 19]. Such incidents emphasize the need for international cooperation and information sharing to preempt and mitigate cyber threats effectively.

1.2. Cyber Threat Intelligence and Threat Landscapes

CTI refers to the collection, analysis, and dissemination of information regarding potential or existing cyber threats. [4] disclosed that CTI encompasses data on the threat actors, their capabilities, intentions, and the tactics, techniques, and procedures (TTPs) they employ. By understanding these elements, organizations can proactively defend against cyber threats. A rapidly shifting cyber threat landscape is marked by increasingly sophisticated cyber threats, including advanced persistent threats (APTs), ransomware attacks, and state-sponsored espionage [2, 7, 15, 19]. The proliferation of Internet of Things (IoT) devices and the increasing reliance on cloud services have expanded the attack surface,

making traditional security measures insufficient. In this dynamic environment, timely and actionable CTI becomes indispensable for effective cybersecurity [1, 3].

2. The Concept and Lifecycle of Cyber Threat Intelligence (CTI)

CTI is a critical component of modern cybersecurity strategies, providing organizations with actionable insights to anticipate, prevent, and respond to cyber threats. Understanding the various levels of CTI and its lifecycle is essential for effective implementation.

2.1. Levels of Cyber Threat Intelligence

CTI operates at three distinct levels, each serving different organizational needs: *Tactical Intelligence* - This level focuses on immediate threats and is primarily used by security operations teams. It includes indicators of compromise (IOCs) such as IP addresses, domain names, and file hashes. Tactical intelligence enables rapid detection and response to specific threats. *Operational Intelligence* - Operational intelligence provides insights into the methodologies and capabilities of threat actors. It encompasses information about specific campaigns, attack vectors, and tools used by adversaries. This intelligence aids in understanding the broader context of threats and informs medium-term security strategies. *Strategic Intelligence* - Strategic intelligence offers a high-level overview of the threat landscape, including emerging trends, geopolitical considerations, and potential risks to national security. It is designed for senior decision-makers to guide long-term planning and policy development [1, 4, 8, 20]

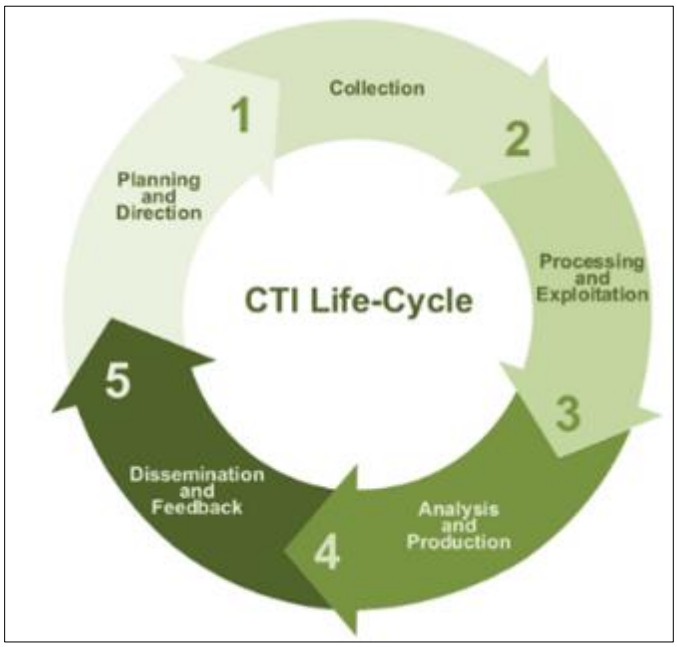

Figure 1 The various stages of a CTI life cycle [1]

2.2. The Cyber Threat Intelligence Lifecycle

The CTI lifecycle as depicted in figure 1, is a sophisticated and iterative process that methodically transforms raw data into actionable intelligence, thereby enabling organizations to proactively detect, prevent, and respond to the dynamic and increasingly complex cyber threats that permeate the digital landscape [1, 4, 21]. This multifaceted process encompasses a series of intricately connected stages, including meticulous data collection from a diverse array of sources, rigorous processing to standardize, filter, and contextualize data, in-depth analysis to identify patterns, trends, and anomalies, strategic dissemination of final intelligence products to stakeholders in a timely, relevant, and actionable format, and constructive feedback to refine future efforts, ensuring continuous improvement, enhancing the quality, relevance, and accuracy of CTI, and ultimately fortifying organizational resilience and agility in the face of an ever-evolving and increasingly sophisticated cyber threat landscape [2, 16].

2.3. Tools and Frameworks Supporting CTI

The development of Cyber Threat Intelligence (CTI) tools and frameworks has revolutionized the way organizations collect, analyze, and share threat information, with pivotal examples including Structured Threat Information eXpression (STIX), a standardized language that enables consistent and structured sharing of threat intelligence across diverse organizations and platforms, Trusted Automated Exchange of Intelligence Information (TAXII), a protocol that facilitates secure and automated CTI exchange over HTTPS, seamlessly working in conjunction with STIX to streamline threat intelligence sharing, and the MITRE ATT&CK framework, a comprehensive knowledge base of adversary tactics, techniques, and procedures that provides a structured approach to understanding, analyzing, and mitigating cyber threats, ultimately enhancing the efficiency, effectiveness, and collaboration of CTI processes, and significantly strengthening overall cybersecurity posture [3, 8, 10, 16, 20].

3. Benefits of Cyber Threat Intelligence (CTI) Sharing

Research has shown [2] that CTI sharing has emerged as a pivotal strategy in enhancing both national and global cybersecurity postures. By facilitating the exchange of threat-related information among stakeholders, CTI sharing offers numerous benefits, including bolstering national security, fostering international cooperation, and improving risk mitigation and response capabilities.

3.1. National Security Advantages

CTI sharing significantly contributes to national security by providing timely and relevant information regarding potential cyber threats. This proactive approach enables nations to anticipate and mitigate risks associated with cyber warfare, ultimately safeguarding critical assets. The collaboration between various stakeholders, such as government entities, private sectors, and international partners, facilitates a comprehensive understanding of emerging threats. By sharing intelligence on cyber vulnerabilities and attack methodologies, Nigeria can bolster its defenses and develop targeted countermeasures to safeguard critical infrastructure and citizens. Through Cyber Threat Intelligence (CTI) sharing, Nigeria can present a unified front against cyber adversaries, amplifying collective security efforts nationwide. As the country navigates increasingly complex cyber threats, integrating threat intelligence into its national cybersecurity strategy is crucial for fortifying defenses and protecting citizens, businesses, and infrastructure from cyber-attacks. CTI sharing intelligence on cyber vulnerabilities and attack methodologies, nations can develop stronger defense mechanisms and countermeasures [10, 11, 12]. Furthermore, CTI sharing promotes a unified front against adversaries, enhancing collective security efforts. As nations face increasingly sophisticated cyber adversaries, the integration of threat intelligence becomes vital for reinforcing national defenses and ensuring the protection of citizens and infrastructures against cyber warfare.

3.2. International Cooperation and Deterrence

Global cyber threats demand a global response, emphasizing the importance of international cooperation and collective action. CTI sharing fosters collaboration among nations, enabling them to collectively address cyber threats that transcend borders. By sharing threat intelligence, countries can coordinate their defense strategies, harmonize their cybersecurity policies, and establish joint response mechanisms. This collaborative approach not only enhances the effectiveness of individual national defenses but also serves as a deterrent to potential adversaries by demonstrating a united and resilient front. For instance, the joint advisory issued by the United Kingdom and its allies, including the United States, France, and Germany, warning about a Russian state-sponsored cyber campaign targeting organizations involved in supporting Ukraine, exemplifies the importance of international CTI sharing in addressing state-sponsored cyber threats [9, 19].

3.3. Risk Mitigation, Faster Response Times, and Resilience

CTI sharing enhances an organization's ability to detect, respond to, and recover from cyber incidents. By accessing shared intelligence, organizations can identify threats more quickly, understand the tactics and techniques employed by adversaries, and implement appropriate countermeasures. This leads to reduced response times and minimizes the potential impact of cyber-attacks [4]. Moreover, CTI sharing contributes to building resilience by enabling organizations to learn from each other's experiences and adapt their security measures accordingly. The collective knowledge gained through CTI sharing allows for the development of more robust and adaptive cybersecurity strategies, ensuring that organizations are better prepared to withstand and recover from cyber incidents [2, 20]. CTI sharing is a strategic tool that enhances national security, fosters international cooperation, and improves organizational resilience against cyber threats. By embracing CTI sharing, stakeholders can collectively strengthen their cybersecurity postures and effectively combat the evolving landscape of cyber threats [9, 21].

4. Challenges in CTI Sharing

While Cyber Threat Intelligence (CTI) sharing is crucial for enhancing cybersecurity, its effectiveness is hindered by multifaceted challenges, including legal constraints stemming from diverse data protection regulations such as the Nigeria Data Protection Regulation (NDPR), General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA), which restrict cross-border sharing of personal data and compromise the utility of shared intelligence [1, 5, 17]. Furthermore, technical incompatibilities stemming from diverse formats and protocols lead to interoperability challenges, delays, and communication breakdowns. The inconsistent adoption of standardized frameworks, such as STIX/TAXII, further compounds these issues [8, 16]. Moreover, complex political dynamics, characterized by geopolitical tensions and divergent national interests, can impede international collaboration, as nations may withhold critical information due to mistrust, strategic considerations, or competing priorities, ultimately undermining global efforts to mitigate cyber threats and ensure collective security [2, 18].

[9] reported that inter-organizational trust is a critical challenge in CTI sharing, as private entities may hesitate to share intelligence with governments due to concerns about misuse, regulatory repercussions, confidentiality, and competitive advantage. Historical incidents of surveillance and data misuse have also eroded trust between the public and private sectors, making it essential to build confidence through transparent policies and mutual agreements on data handling to facilitate effective collaboration and information exchange. [18] detected that the classification and handling of sensitive information pose challenges to effective CTI sharing. Over-classification can hinder timely sharing, particularly when declassification processes are slow, delaying critical information from reaching those who need it. Additionally, sharing detailed threat data risks exposing proprietary methods or sensitive operations, requiring organizations to balance transparency with protecting their own interests and security.

Addressing these challenges requires harmonizing legal frameworks, standardizing technical protocols, fostering trust through transparent practices, and developing clear guidelines for data classification and sharing.

5. CTI Sharing Models and Frameworks

Effective CTI sharing is facilitated through various models and frameworks that foster collaboration among governments, industries, and the broader cybersecurity community. These structures are designed to enhance situational awareness, expedite incident response, and strengthen collective defense mechanisms.

5.1. Government-Led Initiatives

Government agencies play a crucial role in facilitating Cyber Threat Intelligence (CTI) sharing efforts. In Nigeria, agencies like the Nigerian Communications Commission (NCC) and the National Information Technology Development Agency (NITDA) work together to enhance cybersecurity through initiatives like the Nigeria Computer Emergency Response Team (ngCERT). These efforts demonstrate the importance of government-led initiatives in CTI sharing, protecting critical infrastructure, and promoting a secure digital environment in Nigeria [5, 12]

In the US, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) have historically, coordinated public-private partnerships to protect critical infrastructure, although recent administrative changes have raised concerns about continuity. In contrast, the European Union Agency for Cybersecurity (ENISA) promotes the establishment of Information Sharing and Analysis Centers (ISACs) across EU member states, facilitating sector-specific threat intelligence exchange [11, 22]. Additionally, the North Atlantic Treaty Organization (NATO) enhances cyber defense through initiatives like the Cooperative Cyber Defence Centre of Excellence (CCDCOE) and partnerships with private entities, such as its agreement with FireEye to share non-classified technical information on cyber threats, demonstrating the importance of government-led initiatives in CTI sharing [9, 11, 18].

5.2. Industry Consortia

Industry consortia play a vital role in facilitating Cyber Threat Intelligence (CTI) sharing among sector-specific stakeholders in Nigeria. For instance, the Nigeria Inter-Bank Settlement System (NIBSS) and the Bankers' Committee collaborate to share cyber threat information, enhancing the financial sector's resilience against cyber-attacks. Similarly, industry-specific initiatives can help sectors like oil and gas, telecommunications, and healthcare share and analyze intelligence on emerging cybersecurity risks, ultimately protecting Nigeria's critical infrastructure from cyber threats. Industry consortia facilitate Cyber Threat Intelligence (CTI) sharing among sector-specific stakeholders in Nigeria. Such as, financial institutions in Nigeria can leverage collaborative platforms similar to the Financial Services

Information Sharing and Analysis Center (FS-ISAC) model, enabling them to share cyber threat information and enhance the sector's resilience against cyber-attacks [1, 11, 18].

The Financial Services Information Sharing and Analysis Center (FS-ISAC), established in 1999, enables financial institutions to share cyber threat information, thereby enhancing the sector's resilience against cyber-attacks. Similarly, the Automotive Information Sharing and Analysis Center (Auto-ISAC) serves as a central hub for the automotive industry to share and analyze intelligence on emerging cybersecurity risks, leveraging platforms like Cyware to enhance automated threat intelligence sharing. These sector-specific organizations demonstrate the importance of collaborative CTI sharing in protecting industries from cyber threats [2, 5, 9, 13, 22].

5.3. Public-Private Partnerships

Public-private partnerships are essential for comprehensive Cyber Threat Intelligence (CTI) sharing in Nigeria, as collaborations between government entities and private organizations enable the sharing of critical information to protect infrastructure and mitigate cyber threats. Initiatives like the Nigeria Computer Emergency Response Team (ngCERT) and partnerships between Nigerian government agencies and private sector companies can facilitate information sharing to safeguard critical infrastructure. Such collaborative approaches can enhance CTI sharing and cybersecurity, demonstrating the effectiveness of public-private partnerships in Nigeria's cybersecurity landscape. Public-private partnerships collaborations between government entities and private organizations enable the sharing of critical information to protect infrastructure and mitigate cyber threats. Enterprises like InfraGard, a partnership between the FBI and private sector members, facilitate information sharing to safeguard U.S. critical infrastructure. Similarly, the National Cyber-Forensics and Training Alliance (NCFTA) bring together law enforcement, private industry, and academia to identify and mitigate cybercrime threats through strategic alliances, demonstrating the effectiveness of collaborative approaches in enhancing CTI sharing and cybersecurity [5, 11, 12, 20].

5.4. Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) involves collecting and analyzing publicly available information in Nigeria to identify potential cyber threats, leveraging local online sources, social media platforms, and public repositories to gather early indicators of emerging threats. By adopting diverse Cyber Threat Intelligence (CTI) sharing models and frameworks, including government-led initiatives like the Nigeria Computer Emergency Response Team (ngCERT), industry collaborations, and public-private partnerships, Nigeria can strengthen its cybersecurity landscape, foster collaboration, enhance threat detection, and enable rapid response to cyber incidents [12]. Open-Source Intelligence (OSINT) as a platform for collecting and analyzing publicly available information to identify potential cyber threats, leveraging sources such as social media platforms like Twitter and Reddit to gather early indicators of evolving threats, as well as public repositories like GitHub or Pastebin to uncover leaked credentials or malicious code [1, 16]. However, OSINT requires careful validation to ensure the accuracy and relevance of the gathered information [9].

Eventually, diverse Cyber Threat Intelligence (CTI) sharing models and frameworks, including government-led initiatives, industry consortia, public-private partnerships, and OSINT, collectively strengthen the cybersecurity landscape by fostering collaboration, enhancing threat detection, and enabling rapid response to cyber incidents.

6. Global Case Studies and Comparative Perspectives

Cyber Threat Intelligence (CTI) sharing practices vary significantly across regions, influenced by legal frameworks, political dynamics, and technological capabilities. This section examines the approaches of the United States and the European Union, explores cybersecurity collaboration in the Asia-Pacific (APAC) region, and highlights strategies adopted by emerging economies.

6.1. Nigeria vs. Regional Approaches in Africa

Nigeria and Regional Approaches in Africa, Nigeria's Cyber Threat Intelligence (CTI) sharing framework leverages national initiatives like the Nigeria Computer Emergency Response Team (ngCERT) and public-private partnerships. Similarly, other African regions, including South Africa's CSIRT-SA and Kenya's KE-CERT, have established their own CTI sharing frameworks. These diverse approaches highlight opportunities for knowledge sharing and collaboration, ultimately strengthening Africa's cybersecurity landscape through coordinated efforts [9, 12].

6.2. United States vs. European Union Approaches

The United States and European Union (EU) have developed distinct approaches to Cyber Threat Intelligence (CTI) sharing. The US model emphasizes public-private partnerships, leveraging initiatives like Information Sharing and

Analysis Centers (ISACs) to facilitate sector-specific threat intelligence exchange, although recent administrative decisions have raised concerns about continuity. In contrast, the EU adopts a more centralized approach, with agencies like the European Union Agency for Cybersecurity (ENISA) promoting ISAC establishment across member states, while informal alliances like the Club de Berne facilitate intelligence sharing among EU intelligence services, enhancing collective cybersecurity efforts. These differing approaches reflect unique regional priorities and frameworks for CTI sharing [2, 4].

6.3. Asia-Pacific Cybersecurity Collaboration

The APAC region has witnessed significant advancements in cybersecurity collaboration, with various initiatives promoting information sharing, joint threat mitigation, and capacity building among nations. Notably, the ASEAN-Japan Cybersecurity Community Alliance (AJCCA) launched the Threat Intelligence Sharing Working Group (TIS WG) in 2025, bringing together cybersecurity communities from five ASEAN countries to foster regional cooperation [22]. Additionally, Australia's 2023-2030 Cyber Security Strategy prioritizes strong public-private partnerships, proposing a Cyber Incident Review Board and establishing an Executive Cyber Council to facilitate threat information sharing across the economy [18]. Furthermore, a regional coalition of policymakers and private technology agencies has been formed to combat cybercrime, with a focus on accelerating public-private partnerships and promoting broader sharing of threat intelligence. These initiatives collectively demonstrate the APAC region's commitment to bolstering cybersecurity collaboration and information sharing, ultimately enhancing the region's resilience to cyber threats [9, 11].

6.4. Strategies in Emerging Economies

Emerging economies are adopting innovative strategies to enhance CTI sharing, as exemplified by India's Information Sharing and Analysis Center (ISAC), which operates as an independent non-profit organization, collaborating closely with the National Critical Information Infrastructure Protection Center (NCIIPC) to facilitate public-private partnerships in cybersecurity [4, 11]. Another notable initiative is the International Multilateral Partnership Against Cyber Threats (IMPACT), headquartered in Malaysia, which serves as a global platform for cybersecurity collaboration, offering services such as a Global Response Centre and Network Early Warning System to member countries [2]. These diverse approaches to CTI sharing highlight the importance of tailored strategies that consider regional contexts and capabilities, enabling effective collaboration and threat mitigation in emerging economies.

Regional disparities highlight the need for capacity building in developing economies. International cooperation and support are essential to ensure that all nations can participate effectively in CTI sharing, thereby enhancing global cybersecurity resilience.

7. Methodology

This study adopts a qualitative, integrative literature review methodology to systematically explore and synthesize existing knowledge on Cyber Threat Intelligence (CTI) sharing. Relevant peer-reviewed journal articles, conference proceedings, white papers, technical reports, and government publications from 2015 to 2025 were collected using IEEE Xplore, SpringerLink, ScienceDirect, Scopus, and Google Scholar academic databases. Keywords used included “Cyber Threat Intelligence,” “CTI sharing,” “cybersecurity collaboration,” “AI in threat detection,” “blockchain security,” and “global cybersecurity frameworks.” Studies were selected based on relevance to CTI mechanisms, international collaboration, policy frameworks, and technological enablers. Only English-language sources that offered substantial evidence, models, or critical perspectives were included. Extracted data were categorized into key themes; CTI frameworks and lifecycles, strategic benefits, barriers to sharing, global and regional models, and future directions. Comparative analysis was applied to evaluate the effectiveness and scalability of CTI practices across sectors and regions. This methodology enabled a comprehensive and critical synthesis, offering actionable insights into how CTI sharing can enhance both national and global cybersecurity postures.

8. Findings

The review of Cyber Threat Intelligence (CTI) sharing highlights its strategic importance in bolstering threat detection, situational awareness, and incident response capabilities, ultimately enabling proactive defense through the distribution of real-time, actionable intelligence across organizations and borders. However, despite the existence of various CTI sharing models, including government-led platforms, industry-specific Information Sharing and Analysis Centers (ISACs), and open-source initiatives, these efforts are often hindered by a lack of interoperability and global cohesion, resulting in fragmented frameworks. Furthermore, persistent legal and trust barriers, such as varying data protection laws and trust deficits between entities, impede effective CTI sharing, as organizations may be reluctant to

share information due fears of privacy violations, reputational harm, and competitive disadvantage often hinder organizations' willingness to share threat intelligence. The underutilization of emerging technologies like Artificial Intelligence (AI), automation, and blockchain also limits the potential of CTI sharing, despite their capacity to improve speed, accuracy, and trust. Additionally, regional disparities in CTI mechanisms and capabilities between developed and developing economies create asymmetries in threat visibility and response capabilities. Nevertheless, emerging trends such as automation, AI-driven threat detection, and blockchain-facilitated trust models offer promising solutions to enhance the efficacy of CTI sharing. To overcome these challenges and unlock the full potential of CTI sharing, there is a pressing need for globally accepted CTI standards, legal harmonization, and incentive-driven public-private partnerships to foster broader participation and collaboration, ultimately enabling organizations and nations to better understand the threat landscape, detect, prevent, and respond to cyber threats more effectively.

9. Discussion

The findings highlighted the pivotal role of Cyber Threat Intelligence (CTI) sharing in strengthening national and global cybersecurity. However, several challenges impede its effectiveness, including legal and regulatory discrepancies across jurisdictions, trust issues, and concerns over data privacy and misuse. To overcome these hurdles, innovative solutions are being explored to facilitate secure, efficient, and trustworthy CTI sharing.

One of the primary challenges in CTI sharing is navigating diverse data protection laws and regulations across jurisdictions, which created barriers to information exchange. Additionally, trust issues persisted, with organizations hesitant to share sensitive information due to concerns over reputational harm, competitive disadvantages, or data misuse. To address these challenges, Artificial Intelligence (AI) and automation, blockchain, and federated learning cutting-edge technologies are being leveraged. AI-driven platforms can analyze vast datasets in real-time, identifying patterns and anomalies to enable swift threat response and enhance situational awareness. Blockchain technology provides a decentralized, immutable framework for secure and trustworthy CTI sharing, ensuring data integrity and trust among participants. Federated learning enables collaborative training of machine learning models without sharing sensitive data, preserving privacy while leveraging collective intelligence [2, 6, 22].

Moreover, policy innovations and trust-building mechanisms are crucial to incentivizing participation and establishing standardized protocols. Blockchain-based incentive mechanisms can reward organizations for contributing valuable threat intelligence, while clear guidelines and frameworks can alleviate concerns over data misuse and confidentiality. To fully harness the potential of CTI sharing, it is essential to address the challenges hindering adoption, including cost, complexity, and lack of awareness. By leveraging innovative technologies and policy solutions, organizations can enhance their cybersecurity postures and contribute to a more secure digital landscape [11, 22].

Undeniably, the future of CTI sharing holds much promise; nevertheless, it requires a concerted effort from all stakeholders. Governments, industries, and academia must work together to develop and implement standardized frameworks, invest in research and development, and promote awareness about the benefits of CTI sharing. Positively, this will enable us to create a more robust and adaptive CTI sharing ecosystem, better equipped to address emerging cyber threats and protect our digital assets.

10. Conclusion

Cyber Threat Intelligence (CTI) sharing emerged as a strategic imperative in the fight against evolving cyber threats that transcend borders and threaten national and global security. By facilitating the timely exchange of actionable intelligence, CTI sharing enhances collective situational awareness, strengthens incident response capabilities, and fosters a unified defense posture across governments, industries, and international partners. The benefits of CTI sharing are multifaceted, including improved national security, deeper international cooperation, risk mitigation, and greater resilience in the face of cyber adversaries. To fully harness the potential of CTI sharing, a coordinated global approach is essential. This requires governments to lead with clear policies and frameworks that facilitate information exchange while protecting privacy and national interests. Industry must actively participate in collaborative initiatives, supported by advanced technologies like AI, blockchain, and federated learning. Academia and researchers must fill knowledge gaps and innovate solutions to emerging challenges. By working together and investing in CTI sharing ecosystems and policy innovations, the global community can collectively strengthen its cyber resilience and ensure a secure digital future.

Additionally, the success of CTI sharing initiatives depends on several significant factors, including the development of trust and confidence among stakeholders, the establishment of standardized frameworks and protocols, and the

investment in enabling technologies. By addressing these challenges and opportunities, a more secure and resilient digital landscape can be created that benefits individuals, organizations, and nations alike. Ultimately, the future of CTI sharing embraces significant potential, but then, it requires sustained, cross-sectoral investment and collaboration. By prioritizing interoperability, transparency, and inclusivity, we can build a more robust and effective CTI sharing ecosystem that enhances collective cybersecurity and supports a safer digital future. As the cyber threat landscape continues to evolve, staying ahead of the curve requires embracing innovation, fostering collaboration, and prioritizing collective cybersecurity. This collective effort will pave the way for a more secure and prosperous future, empowering individuals, organizations, and nations alike.

Future Directions and Research Gaps

As cyber threats continue to grow in complexity and scale, advancing Cyber Threat Intelligence (CTI) sharing mechanisms has become imperative. Emerging technologies such as Artificial Intelligence (AI), blockchain, and federated learning offer promising avenues to enhance CTI sharing. However, their integration presents new challenges and research opportunities that must be addressed. To stay ahead of adversaries, it is crucial to develop explainable AI models that provide transparency in decision-making processes, ensuring trust and accountability in automated CTI systems.

Further research is needed to overcome the challenges associated with blockchain and federated learning, such as scalability, interoperability, and standardization. Developing efficient and universally accepted frameworks will be critical to the widespread adoption of these technologies in CTI sharing. Moreover, policy innovations and trust-building mechanisms are essential to balance security needs with privacy rights and encourage collaboration among stakeholders.

Progressing, CTI sharing requires a holistic strategy that combines cutting-edge technology with robust policy frameworks, enabling effective collaboration and threat mitigation. By addressing current challenges and exploring emerging technologies, stakeholders can enhance collective cybersecurity resilience in the face of evolving threats. This will necessitate sustained investment in research and development, as well as collaboration among governments, industries, and academia to create a more secure digital landscape. By working together, a more robust and effective CTI sharing ecosystem that supports a safer digital future can be built.

Compliance with ethical standards

Acknowledgments

The authors would like to extend their sincere gratitude to the anonymous reviewers for their insightful comments and suggestions, which significantly improved the quality of this paper. Additionally, the corresponding author extends heartfelt appreciation to Prof. M. O. Onyesolu for his invaluable mentorship, guidance, and support throughout the research process, and acknowledges the significant research contributions of Dr M. S. Julius.

Disclosure of conflict of interest

No conflict-of-interest to be disclosed.

References

[1] Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., and Foo, E. (2024). Current approaches and future directions for cyber threat intelligence sharing: A survey. Journal of Information Security and Applications, 83, 103786. https://doi.org/10.1016/j.jisa.2024.103786

[2] Alazab, M., Khurma, R. A., García-Arenas, M., Jatana, V., Baydoun, A., and Damaševičius, R. (2024). Enhanced threat intelligence framework for advanced cybersecurity resilience. Egyptian Informatics Journal, 27, 100521. https://doi.org/10.1016/j.eij.2024.100521

[3] Allouche, Y., Tapas, N., Longo, F., Shabtai, A., and Wolfsthal, Y. (2021). TRADE: TRusted anonymous data exchange: threat sharing using blockchain technology (No. arXiv:2103.13158). arXiv. https://doi.org/10.48550/arXiv.2103.13158

[4] Aminu, M., Akinsanya, A., Oyedokun, O., Dickson, A., and Dako, D. A. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. International Journal of Computer Applications Technology and Research, 13, 11–27. https://doi.org/10.7753/IJCATR1308.1002

[5] Borden, R., Mooney, J., Taylor, M., and Sharkey, M. (2019). Threat information sharing under GDPR - ProQuest. 15(3), 30–35.

[6] Calvin, C., Eulerich, M., and Holt, M. (2025). Characteristics of cybersecurity and IT involvement by the IA activity. International Journal of Accounting Information Systems, 56, 100726. https://doi.org/10.1016/j.accinf.2025.100726

[7] Cheung, K.-F., Yue, M.-C., Bell, M. G. H., and Tseng, C.-L. (2025). Cybersecurity with attacker-defender models: Game-theoretic frameworks. In Reference Module in Social Sciences. Elsevier. https://doi.org/10.1016/B978-0-443-28993-4.00081-0

[8] Cohen, D., Te'eni, D., Yahav, I., Zagalsky, A., Schwartz, D., Silverman, G., Mann, Y., Elalouf, A., and Makowski, J. (2025). Human–AI enhancement of cyber threat intelligence. International Journal of Information Security, 24(2), 99. https://doi.org/10.1007/s10207-025-01004-4

[9] Jasper, S. E. (2017). U.S. cyber threat intelligence sharing frameworks. International Journal of Intelligence and CounterIntelligence, 30(1), 53–65. https://doi.org/10.1080/08850607.2016.1230701

[10] Jiang, Y., Meng, Q., Shang, F., Oo, N., Hong Minh, L. T., Lim, H. W., and Sikdar, B. (2025). MITRE ATTandCK applications in cybersecurity and the way forward. 1(1). https://arxiv.org/html/2502.10825v1

[11] Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., and Brożek, P. (2022). Global digital convergence: impact of cybersecurity, business transparency, economic transformation, and AML efficiency. Journal of Open Innovation: Technology, Market, and Complexity, 8(4), 195. https://doi.org/10.3390/joitmc8040195

[12] Nainna, M. A., Bass, J., and Speakman, L. (2024). Cyber threat intelligence sharing in Nigeria. Communications of the IIMA, 22(1). https://doi.org/10.58729/1941-6687.1450

[13] Obiokafor, I. N. (2023). Approaches to a secure, sustainable, and diversified Nigerian economy in a cashless society. World Journal of Advanced Research and Reviews, 20(2), Article 2. https://doi.org/10.30574/wjarr.2023.20.2.2266

[14] Obiokafor, I. N., Onyesolu, M. O., Olusanya, F. A., Oboti, N. P., and Ajonuma, M. E. (2024). Cyber intelligence's efficacy in mitigating cyber threats: a narrative review. Anspoly journal of innovative development (AJID), 2(1), Article 1.

[15] Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., and Shakarian, P. (2017). Darkweb cyber threat intelligence mining. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316888513

[16] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., and Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys and Tutorials, 25(3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282

[17] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., and Doss, R. (2022). Zero Trust Architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

[18] Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. Procedia Computer Science, 235, 1649–1663. https://doi.org/10.1016/j.procs.2024.04.156

[19] Tounsi, W., and Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers and Security, 72, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

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

[21] Yang, L., Wang, M., and Lou, W. (2025). An automated dynamic quality assessment method for cyber threat intelligence. Computers and Security, 148, 104079. https://doi.org/10.1016/j.cose.2024.104079

[22] Zhou, Y., Zhang, Y., Yang, Q., Liu, Y., Rong, C., and Tian, Z. (2025). A blockchain based efficient incentive mechanism in tripartite cyber threat intelligence service marketplace. Blockchain: Research and Applications, 100263. https://doi.org/10.1016/j.bcra.2024.100263