The Legal Landscape of Cyber Threat Intelligence Sharing: A Study on International Legal Standards and Best Practices

1. Maryam Ziaei*: Department of Labor Law, Shiraz University, Shiraz, Iran
*****Correspondence: e-mail: Ziaeimary24@gmail.com

Abstract

Cyber Threat Intelligence (CTI) sharing is an essential component of modern cybersecurity strategies, enabling organizations to detect, mitigate, and preempt cyber threats through collaboration. However, the exchange of CTI is hindered by a complex array of legal, operational, and security challenges that limit its effectiveness. This article explores the international legal landscape surrounding CTI sharing, examining existing treaties, conventions, and national laws that impact its flow across borders. It discusses the tension between data privacy laws, conflicting national regulations, and intellectual property concerns, which often impede the seamless exchange of threat intelligence. The article further analyzes the operational barriers to CTI sharing, including trust issues, data format complexities, and interoperability concerns, as well as the security risks of exposing sensitive information during intelligence exchanges. Key recommendations for improving CTI sharing include the development of harmonized legal frameworks, enhanced international cooperation, and the promotion of transparency, accountability, and consent in the sharing process. The article also highlights the importance of building trust between stakeholders, fostering collaboration between public and private sectors, and leveraging emerging technologies such as blockchain and artificial intelligence to address both legal and operational challenges. The future of CTI sharing depends on overcoming these barriers and creating an environment where information can flow freely and securely across borders, helping organizations collectively combat the evolving threat landscape.

Keywords: Cyber Threat Intelligence (CTI), Legal Frameworks, Data Privacy, International Cooperation, Cybersecurity, Threat Intelligence Sharing.

Received: 11 November 2022
Revised: 14 December 2022
Accepted: 25 December 2022
Published: 01 January 2023

Citation: Ziaei, M. (2023). The Legal Landscape of Cyber Threat Intelligence Sharing: A Study on International Legal Standards and Best Practices. *Legal Studies in Digital Age*, 2(1), 13-26.

1. Introduction

Cyber Threat Intelligence (CTI) refers to the process of collecting, analyzing, and disseminating information related to current or potential cyber threats. It provides valuable insights into the tactics, techniques, and procedures (TTPs) used by malicious actors, which can help organizations and governments defend against, mitigate, or preempt cyberattacks. In an era of increasingly sophisticated cyber threats, the role of CTI has become central to global cybersecurity efforts. Cyber threats today are not only more frequent but also more complex, with adversaries employing advanced techniques that can bypass traditional defense mechanisms. As cyberattacks have far-reaching implications, targeting critical infrastructure, financial systems, and personal data, the need for timely and actionable intelligence to counter these threats has become paramount. CTI enables organizations to stay ahead of cyber adversaries by providing context and foresight, allowing them to take proactive measures. This includes sharing intelligence to create a broader, collaborative defense against the shared threats that cross borders and sectors (Abu et al., 2018).

At its core, CTI involves gathering data from various sources, including open-source intelligence, internal logs, and third-party threat feeds, then analyzing this data to identify potential risks. The output of this intelligence is meant to inform decision-making processes and operational responses to emerging threats. However, its utility is often hindered by legal and regulatory challenges, particularly around data privacy and international cooperation. The complexities of managing and sharing cyber threat data are further complicated by the differing legal and ethical standards across jurisdictions, leading to the emergence of numerous obstacles that limit the effectiveness of CTI sharing. Legal concerns such as data protection, privacy laws, and national security interests often create friction, making it difficult for organizations to share intelligence freely across borders (Albakri et al., 2019). As cyber threats are inherently transnational, effective CTI sharing requires harmonizing legal standards and ensuring that intelligence flows smoothly between governments, private sector entities, and international organizations.

The purpose of this article is to explore the legal landscape surrounding cyber threat intelligence sharing, focusing on international legal standards and best practices. As the global digital ecosystem expands, the need for secure and efficient sharing of cyber threat data is more critical than ever. By identifying the legal frameworks that govern CTI sharing, this article aims to highlight the challenges, gaps, and potential solutions to improving international collaboration in the fight against cybercrime. The article will delve into existing international treaties and conventions that provide a framework for CTI sharing, as well as the regulations that govern data privacy and protection in different jurisdictions. One key challenge in this regard is reconciling the privacy concerns associated with personal data with the need for sharing threat information that may involve sensitive organizational data. Legal frameworks such as the General Data Protection Regulation (GDPR) in the European Union impose strict requirements on data handling, creating tension between regulatory compliance and the practicalities of sharing cyber threat intelligence across borders (Albakri et al., 2018).

This study will also address the various national and regional legal approaches to CTI sharing, focusing on the divergent legal landscapes in countries such as the United States, the European Union, and other global actors. For instance, the US has a more permissive stance on data sharing in cybersecurity contexts, driven by national security imperatives, while the EU's strict data protection laws impose limits on the extent and manner in which CTI can be shared. By examining these differences, this article aims to provide a comprehensive overview of the international legal environment and its impact on CTI sharing. Furthermore, the article will explore best practices for overcoming the legal and regulatory barriers to information sharing, drawing from case studies and expert insights on successful models of cross-border collaboration (Sarhan et al., 2022; Sauerwein et al., 2021). These best practices may include the use of anonymization techniques, the establishment of legal safe harbors for sharing CTI, and the adoption of standardized frameworks for information exchange.

As the global cyber threat landscape continues to evolve, it is clear that effective CTI sharing can no longer be viewed as an optional component of cybersecurity strategies but as a necessity for the protection of national and international security. To address this, the international community must work toward aligning legal standards and promoting a culture of collaboration. This requires not only harmonizing laws but also building trust among stakeholders across different sectors, including government agencies, private enterprises, and academic institutions. The article will analyze how international organizations, such as the United Nations and the European Union, are working to foster cooperation and establish legal frameworks that facilitate secure and lawful CTI sharing across borders (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021). Through this exploration, the article seeks to provide insights into the current state of CTI sharing laws, the challenges that hinder their effectiveness, and the ways in which these challenges can be overcome to improve global cybersecurity efforts.

In summary, the growing complexity of cyber threats necessitates robust and collaborative approaches to intelligence sharing. Legal frameworks play a critical role in ensuring that this collaboration is both effective and secure. By examining the international and national legal standards that govern CTI sharing, this article aims to shed light on the legal obstacles and best practices that can help improve the global response to cybersecurity threats.

2. Cyber Threat Intelligence: Concept and Evolution

Cyber Threat Intelligence (CTI) refers to the knowledge and insights derived from analyzing and interpreting data related to potential and ongoing cyber threats. The primary goal of CTI is to provide actionable information that organizations can use to identify, mitigate, and prevent cyberattacks. It is distinct from regular security data, as it not only includes indicators of compromise (IOCs) like malware hashes, IP addresses, and domain names, but also provides context about the behavior, techniques, and motivations of threat actors. By offering a deeper understanding of the adversary's tactics, techniques, and procedures (TTPs), CTI empowers organizations to enhance their defense strategies, anticipate potential attacks, and respond with greater precision. This strategic approach to cybersecurity enables defenders to stay one step ahead of attackers, reducing the impact of cyber incidents and improving incident response efforts (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

CTI plays a vital role in cybersecurity by bridging the gap between raw data and decision-making. It helps organizations understand the broader context of security events, offering insights that go beyond individual alerts or incidents. The components of CTI typically include data collection, data analysis, and dissemination. Data collection involves gathering raw intelligence from a wide range of sources, including network logs, intrusion detection systems (IDS), threat feeds, open-source intelligence (OSINT), and dark web monitoring. Once collected, this data is analyzed to uncover patterns, identify vulnerabilities, and assess the threat landscape. Finally, the intelligence is disseminated to relevant stakeholders in a usable format, enabling them to make informed decisions about securing their networks, systems, and applications. Effective CTI helps organizations shift from reactive to proactive security, allowing them to anticipate and mitigate threats before they materialize (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

The evolution of CTI can be traced through various stages, from its early days as a national-level cybersecurity tool to the current era of international collaboration. Initially, CTI was largely used in isolated, national contexts, where governments and large organizations would gather intelligence primarily for defensive purposes. In the early stages of cybersecurity, the focus was predominantly on individual incidents, such as specific attacks or vulnerabilities, rather than on developing a broader understanding of the threat landscape. Governments, financial institutions, and private organizations operated within their own silos, with limited information sharing between them. As cyber threats began to grow in sophistication and scale, it became evident that a more coordinated, global approach was necessary. This realization was accelerated by the increasing number of high-profile cyberattacks that transcended national borders, such as those targeting critical infrastructure, financial systems, and private data. The attacks were not confined to specific countries or regions, underscoring the need for sharing threat intelligence across borders to mount a unified defense (Abu et al., 2018).

As the global digital landscape grew more interconnected, the evolution of CTI led to the development of international frameworks for information sharing. Governments, multinational organizations, and private companies began to recognize the importance of collaboration in combating cyber threats. The rise of sophisticated threat actors—ranging from state-sponsored hackers to cybercriminal groups—further highlighted the necessity of pooling resources and sharing intelligence. The goal became to create a collective defense model, where the sharing of cyber threat data would benefit all parties, thus reducing the overall risk to critical infrastructure and national security. This shift toward international collaboration has led to the creation of various platforms, alliances, and initiatives designed to facilitate the exchange of CTI. For example, organizations such as the European Union Agency for Cybersecurity (ENISA) and the Global Forum on Cyber Expertise (GFCE) have been instrumental in fostering international cooperation in the field of cybersecurity. Furthermore, standards like the OpenDXL and STIX/TAXII protocols have been developed to enable standardized information sharing across different sectors and regions (Albakri et al., 2019).

As the importance of CTI grew, so too did the complexity and variety of intelligence types. Cyber threat intelligence is often categorized into four distinct types: technical, tactical, operational, and strategic. Each type plays a specific role in cybersecurity and provides unique insights into different aspects of the threat landscape. Technical intelligence involves the analysis of data that can directly inform the detection and mitigation of threats. This includes indicators of compromise (IOCs) such as malware hashes, IP addresses, domain names, and file signatures. Technical intelligence is typically used by security tools such as intrusion detection systems (IDS) and firewalls to block or alert on suspicious activity. It is highly granular and often used in the immediate response to cyber threats. While technical intelligence is critical for day-to-day defense, it alone is insufficient for creating a comprehensive cybersecurity strategy, as it focuses only on the specific details of an attack rather than the broader picture (Albakri et al., 2018).

Tactical intelligence provides insights into the methods and tools used by threat actors to execute cyberattacks. This type of intelligence focuses on understanding the tactics, techniques, and procedures (TTPs) employed by adversaries. By identifying patterns in attack strategies, tactical intelligence helps organizations improve their detection capabilities and develop more effective defenses. For example, tactical intelligence may reveal that a particular hacker group frequently uses spear-phishing emails with malicious attachments to gain initial access to a target network. This knowledge can help organizations recognize and defend against similar attacks in the future. Tactical intelligence is often shared through threat intelligence platforms and is typically actionable within days or weeks (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

Operational intelligence goes beyond the immediate tactics used in an attack and looks at the broader context of cyber incidents. It involves understanding the operational goals of threat actors and analyzing incidents over a longer timeline. Operational intelligence is particularly useful in identifying emerging threats or trends and forecasting potential attack vectors. For example, operational intelligence might track the activities of a cybercrime group over several months to understand their methods, goals, and key targets. This type of intelligence often informs the strategic direction of cybersecurity initiatives, helping organizations prioritize defenses against the most likely threats. Operational intelligence typically includes the analysis of ongoing campaigns and is often used by government agencies, law enforcement, and large corporations to track and disrupt the activities of cybercriminals or state-sponsored actors (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

Strategic intelligence focuses on the long-term, high-level understanding of the cyber threat landscape. It provides insights into the broader trends and forces shaping the global cybersecurity environment. Strategic intelligence includes the identification of emerging cyber threats, shifts in the geopolitical landscape, and the motivations behind various cyberattacks. This type of intelligence is often used by decision-makers, such as government officials and C-level executives, to shape policies, allocate resources, and guide the overall direction of cybersecurity efforts. For example, strategic intelligence might reveal that a particular region is becoming a hotspot for cyberattacks targeting critical infrastructure, prompting governments and corporations to invest in stronger defenses in that region. While strategic intelligence is not typically used for immediate, day-to-day defense, it provides essential context for long-term planning and policy development (Albakri et al., 2019).

The evolution of CTI has been marked by an increasing recognition of its importance at both national and international levels. From its early days as a niche component of cybersecurity, it has grown into a critical element of global efforts to combat cyber threats. As the cyber threat landscape continues to evolve, so too must the strategies for collecting, analyzing, and sharing threat intelligence. This evolution reflects a growing understanding that cybersecurity is a shared responsibility and that collaboration, both within and between nations, is essential for effective defense against the ever-expanding range of cyber threats.

3. International Legal Frameworks

The landscape of international legal frameworks governing the sharing of Cyber Threat Intelligence (CTI) is complex and constantly evolving. The rise of global cyber threats has underscored the necessity of international collaboration, yet this collaboration is frequently hindered by a patchwork of legal standards and regulations that vary across borders. Several international treaties, conventions, and regulations aim to address the challenges of CTI sharing, but they often have different implications depending on the jurisdiction and the stakeholders involved. These international legal standards are critical for creating a cooperative environment in which countries and organizations can share threat intelligence to enhance collective cybersecurity.

Among the most influential international legal frameworks is the General Data Protection Regulation (GDPR), enacted by the European Union in 2018. The GDPR regulates the processing of personal data within the European Union and has significant implications for CTI sharing. One of the core principles of the GDPR is that any data processing must respect individuals' privacy rights, ensuring that their data is handled with transparency and in a way that minimizes risks to their personal information. This principle presents challenges for CTI sharing, particularly when intelligence is shared across borders and jurisdictions that may have differing privacy standards. In many cases, the sharing of CTI involves processing personal data, such as IP addresses, email addresses, or other identifiers that could be linked to individuals or organizations. While

GDPR allows for the processing of such data under certain circumstances, it imposes strict requirements for data controllers, such as ensuring data is shared only when necessary and with appropriate safeguards. For organizations looking to share CTI within the framework of GDPR, they must navigate the delicate balance between ensuring effective cybersecurity and adhering to the regulation's strict privacy requirements (Albakri et al., 2019).

The Budapest Convention on Cybercrime, another key international framework, was adopted by the Council of Europe in 2001 and is the first international treaty aimed at addressing internet and computer crimes. This convention provides a legal framework for cooperation among signatory countries in areas such as the collection of electronic evidence, jurisdictional issues, and cross-border cooperation in prosecuting cybercrimes. Article 23 of the Convention, in particular, addresses the issue of international cooperation in the context of cybercrime investigations and the exchange of information related to computer systems and data. The Budapest Convention allows for the sharing of information related to cybercrimes across borders, but it also imposes certain limitations, particularly when it comes to protecting privacy rights. Although the Convention facilitates the exchange of CTI, it is often subject to national legal considerations regarding the scope of permissible surveillance, the protection of data, and the enforcement of laws across borders. Furthermore, while the Convention has been widely ratified, some key countries, such as Russia and China, have not signed or ratified it, limiting its global applicability (Albakri et al., 2018).

In addition to these global frameworks, various regional approaches have been developed to govern CTI sharing, each tailored to the specific legal and geopolitical context of the region. In the European Union, for example, the EU Agency for Cybersecurity (ENISA) plays a crucial role in facilitating cooperation between member states in the area of cybersecurity. The EU's Cybersecurity Act, adopted in 2019, strengthens ENISA's role and sets out a European cybersecurity certification framework. This framework establishes common standards for cybersecurity practices across the EU and encourages the sharing of CTI among member states. However, the EU faces unique challenges in harmonizing its legal and regulatory landscape for CTI sharing, primarily due to the varied privacy laws within its member states and the implications of the GDPR. The European Union's approach to CTI sharing is also influenced by its commitment to protecting individual privacy rights, which can sometimes conflict with the need for real-time information sharing to combat cyber threats effectively (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

In the United States, CTI sharing is governed by a combination of national cybersecurity laws and policies, such as the Cybersecurity Information Sharing Act (CISA) of 2015, which encourages private sector entities to share cyber threat information with the federal government and other organizations. CISA aims to streamline the process of sharing CTI while ensuring that organizations are not legally exposed to liability for sharing information in good faith. The law provides liability protection for companies that share information about cyber threats, but it also sets standards for how this information must be shared and with whom. In practice, however, there are several challenges to the effective implementation of CISA, including concerns over the adequacy of information-sharing platforms, the lack of clarity on what constitutes "sensitive" information, and issues related to the privacy of individuals whose data may be included in CTI. While CISA facilitates the flow of information between the private sector and the government, it also presents legal complexities in terms of balancing national security concerns with the privacy of individuals and businesses (Albakri et al., 2019).

In the ASEAN region, cybersecurity cooperation is governed by a range of multilateral initiatives and agreements, such as the ASEAN Cybersecurity Cooperation Strategy. While ASEAN countries have recognized the importance of collaboration in addressing cyber threats, the legal frameworks for CTI sharing remain fragmented. Many ASEAN countries have different legal standards concerning data protection, surveillance, and privacy, which complicates the sharing of CTI across borders. Moreover, some ASEAN members have limited legal frameworks governing cybersecurity and are still in the process of establishing comprehensive national policies. This inconsistency in legal standards poses a significant challenge to cross-border CTI sharing within the region (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

In Africa, the African Union's Convention on Cyber Security and Personal Data Protection provides a legal framework for the protection of personal data and the enhancement of cybersecurity across the continent. However, similar to ASEAN, the legal infrastructure in many African countries is still developing, and there is a lack of standardization in cybersecurity laws and policies. While there is growing recognition of the need for CTI sharing to combat cyber threats in Africa, the challenge lies in aligning legal standards across diverse national contexts, where some countries lack robust data protection laws or have limited capacity to implement international standards effectively (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

One of the most significant challenges in the international sharing of CTI is the difficulty of harmonizing legal frameworks across jurisdictions. The key obstacle is that different countries have varying legal approaches to cybersecurity, data protection, and privacy. For example, the United States and European Union take contrasting approaches to privacy. In the US, the emphasis is often on national security and business interests, with less stringent requirements for protecting personal data compared to the EU, which has a more robust privacy framework under the GDPR. This difference creates tensions in cross-border CTI sharing, as organizations may be reluctant to share intelligence with entities in other jurisdictions for fear of violating privacy laws or exposing themselves to liability. Similarly, national security concerns often complicate CTI sharing, especially when intelligence is related to sensitive or classified information. Many countries have laws that restrict the sharing of such data with foreign governments or private organizations, citing national security as the primary justification.

Furthermore, concerns about trust and accountability often arise in international CTI sharing. Many countries are hesitant to share intelligence with governments or private organizations from other jurisdictions due to fears that their own cybersecurity operations might be compromised or that the intelligence could be used for purposes other than improving cybersecurity. This lack of trust is exacerbated by the differing political and strategic interests of nations, particularly when it comes to sharing sensitive threat data with adversaries or potential competitors in the global arena. Consequently, while there is a growing recognition of the need for international cooperation in addressing cyber threats, legal and geopolitical considerations continue to present significant barriers to effective CTI sharing (Albakri et al., 2018).

In conclusion, the international legal landscape for CTI sharing is marked by a complex web of treaties, regulations, and regional frameworks that govern how information about cyber threats is exchanged across borders. While initiatives like the GDPR and the Budapest Convention on Cybercrime have established important legal foundations, challenges remain in harmonizing laws across jurisdictions, balancing privacy and national security concerns, and overcoming trust issues. The success of international CTI sharing ultimately depends on creating legal frameworks that can foster cooperation while respecting the legal, political, and cultural differences between countries and regions.

4. National Laws and Policies Impacting CTI Sharing

National laws and policies significantly shape the landscape of Cyber Threat Intelligence (CTI) sharing. While international frameworks provide a broad legal structure, it is the specific laws and regulations within each country that dictate the practicalities of sharing intelligence on a national level. These country-specific legal considerations vary widely, particularly regarding data protection, cybersecurity, and the role of government agencies in regulating or facilitating CTI exchange. The challenge lies in harmonizing these national frameworks to allow for effective, cross-border intelligence sharing while also addressing concerns related to privacy, security, and sovereignty.

In the United States, CTI sharing is governed by a combination of federal and state laws, as well as industry-specific regulations. The Cybersecurity Information Sharing Act (CISA) of 2015, for example, facilitates the voluntary sharing of cybersecurity information between private sector entities and the federal government. CISA aims to encourage businesses to share cyber threat data without fear of legal repercussions, such as violating privacy laws or disclosing proprietary information. It provides liability protections for organizations that share information in good faith, ensuring that companies can collaborate without exposing themselves to significant legal risk. However, while CISA has made progress in encouraging CTI sharing, challenges remain in balancing the need for cybersecurity with the protection of sensitive data. The US's approach is also influenced by other laws such as the Federal Trade Commission's (FTC) regulations, which enforce data protection principles, and the Foreign Intelligence Surveillance Act (FISA), which governs the surveillance of foreign entities. These laws can sometimes create tensions, as intelligence sharing may be limited by concerns over national security, privacy, and the protection of intellectual property (Albakri et al., 2019).

In the United Kingdom, the legal framework governing CTI sharing is shaped by a mixture of domestic regulations and international obligations. The UK's approach is heavily influenced by the European Union's General Data Protection Regulation (GDPR), as the country was bound by EU law prior to Brexit. Post-Brexit, the UK has implemented its own data protection laws, such as the Data Protection Act 2018, which closely mirrors the GDPR. These regulations require organizations to handle personal data with strict care, ensuring that any sharing of cyber threat data that includes personal identifiers complies with privacy standards. Additionally, the UK's National Cyber Security Centre (NCSC) plays a central role in supporting both public and private sector entities in sharing cyber threat intelligence. The NCSC provides guidelines for safe data sharing, focusing on the protection of critical infrastructure and offering a structured approach to exchanging threat data in the face of escalating cyber risks. However, challenges still exist in balancing the desire for effective CTI sharing with the need to protect personal data and national interests, particularly as cyber threats often have transnational origins (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

China, on the other hand, has a more restrictive approach to CTI sharing, influenced by its focus on state security and a controlled internet environment. The Chinese government maintains strict oversight of both domestic and international cyber activities through regulations such as the Cybersecurity Law of 2017, which outlines extensive measures for the protection of critical infrastructure and personal data within the country. Under this law, organizations are required to store data within China’s borders and comply with government-directed monitoring of cyber activities. While China has engaged in various initiatives to strengthen global cybersecurity cooperation, its approach to CTI sharing is tightly regulated, especially when it comes to sharing information with foreign entities. This legal framework is reflective of China’s broader cybersecurity strategy, which prioritizes national security and state control over the flow of information. Furthermore, concerns related to espionage, intellectual property theft, and national sovereignty further complicate the willingness to share CTI with other nations, particularly when the data may involve sensitive governmental or industrial information (Abu et al., 2018).

Russia follows a similar approach to China in terms of the role of the state in controlling cybersecurity activities. The Russian Federal Law on Information, Information Technologies, and Protection of Information (2006) governs the exchange of data, including CTI. The law imposes strict requirements for the storage and transmission of data, particularly when it pertains to sensitive national information. Russian cybersecurity policy is also influenced by its strategic interests, and while Russia participates in international cybersecurity cooperation, it is often reluctant to share certain types of threat intelligence with Western countries due to national security concerns and geopolitical tensions. Additionally, Russian law requires that companies operating within the country store their data on domestic servers, complicating efforts for cross-border CTI sharing. As a result, Russia’s approach to CTI is characterized by a focus on national security, privacy, and control over the information that can be shared across borders (Albakri et al., 2019).

National security agencies play a significant role in shaping the legal landscape for CTI sharing. In many countries, these agencies are the primary stakeholders responsible for both gathering and disseminating cyber threat intelligence. In the United States, for example, agencies such as the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) work closely with private sector entities to share cyber threat data. The National Security Agency (NSA) and the Central Intelligence Agency (CIA) also have a critical role in collecting cyber intelligence related to foreign threats. The collaboration between government agencies and private enterprises is often formalized through public-private partnerships (PPPs), which allow for the exchange of intelligence while maintaining oversight and ensuring compliance with relevant laws and regulations. These partnerships are particularly important in sectors like finance, energy, and telecommunications, where the risk of cyberattacks is high, and a coordinated response is crucial.

In the UK, similar dynamics exist, where public sector agencies such as the NCSC collaborate with private enterprises to share intelligence. The UK government also encourages businesses to participate in information-sharing initiatives, particularly through industry-specific groups such as the Information Sharing and Analysis Centres (ISACs), which allow for the exchange of cyber threat data within a particular sector. The role of private enterprises in CTI sharing is crucial, as they often have the most up-to-date information on threats targeting their networks and systems. In this context, the private sector is seen as an essential partner in identifying emerging threats and contributing to national cybersecurity efforts. However, challenges remain in ensuring that the private sector shares information in a timely and accurate manner, particularly when it involves the disclosure of vulnerabilities or breaches that could have significant financial or reputational impacts (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

Private enterprises also have a pivotal role in shaping national CTI-sharing practices. Many organizations, particularly those in high-risk sectors such as banking, energy, and healthcare, are actively engaged in the collection and sharing of cyber threat intelligence. They are often the first to detect cyberattacks and, as such, play a critical role in providing real-time data on emerging threats. The motivation for these companies to share intelligence is often driven by a desire to protect their own networks as well as the broader ecosystem in which they operate. However, concerns related to privacy, intellectual property, and regulatory compliance often lead to hesitancy in sharing sensitive information. Moreover, while some countries, such as the US, have introduced legal protections to encourage information sharing, others, like China and Russia, impose restrictions on how and with whom intelligence can be shared. These national differences highlight the ongoing challenges in developing global CTI-sharing mechanisms that are both effective and compliant with local laws and policies (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

In summary, national laws and policies play a pivotal role in shaping the framework for CTI sharing. While governments and private enterprises recognize the importance of collaboration in the face of growing cyber threats, the legal environment often presents obstacles that hinder the free flow of information. Differences in data protection laws, national security regulations, and the role of government agencies create a complex web of legal considerations that must be navigated by all stakeholders. For CTI sharing to be effective, there must be a balance between ensuring cybersecurity and protecting privacy and national interests, a task that requires continuous dialogue and cooperation among governments, private sector entities, and international organizations.

5. Best Practices for Cyber Threat Intelligence Sharing

Effective Cyber Threat Intelligence (CTI) sharing relies on a combination of legal and ethical principles, operational best practices, and collaborative platforms. While the benefits of sharing threat intelligence are clear, ensuring that this exchange complies with relevant legal standards and upholds ethical considerations is crucial. Legal principles such as transparency, accountability, and consent serve as the foundation for trust and cooperation between organizations, governments, and other stakeholders involved in the exchange of CTI. These principles help safeguard privacy, respect the rights of individuals and organizations, and ensure that the shared intelligence is used for legitimate and productive purposes.

Transparency is a core principle that ensures the parties involved in CTI sharing understand how and why data is being shared. By establishing clear protocols and procedures, organizations can ensure that the information is shared only with trusted partners and for the purposes of enhancing cybersecurity. This transparency is particularly important when personal or sensitive data is involved. For example, when threat intelligence includes data such as IP addresses or email addresses that could be linked to individuals, transparency allows stakeholders to assess the potential privacy implications of sharing that data. Furthermore, transparency helps to avoid any misunderstandings about the scope of the shared intelligence, the parties involved, and the intended use. Ensuring accountability in CTI sharing is equally important. This principle demands that organizations take responsibility for how they collect, process, and share CTI, as well as for any potential misuse of that information. Accountability mechanisms, such as audit trails, data handling policies, and legal contracts, help mitigate the risk of data abuse and ensure that information is used in accordance with agreed-upon terms and legal requirements (Albakri et al., 2019).

Consent is another fundamental legal and ethical standard in CTI sharing, especially when it comes to handling personal data. Under regulations such as the General Data Protection Regulation (GDPR), consent must be obtained before personal data is processed or shared. This principle ensures that individuals and organizations retain control over their own information. While consent is a necessary safeguard in data protection, it can complicate the CTI sharing process when organizations or governments must obtain explicit consent before sharing intelligence. In cases where obtaining consent may be impractical or impossible, a balance must be struck between the benefits of CTI sharing and the potential risks to privacy. Ethical considerations also extend to the protection of intellectual property and sensitive business information, where companies sharing CTI need to ensure that proprietary data is not inadvertently disclosed to competitors or adversaries. While legal frameworks can help define the boundaries, ethical guidelines are often necessary to address situations where legal obligations are ambiguous or not fully applicable.

Operational best practices for CTI sharing focus on ensuring that intelligence is shared in ways that promote collaboration, minimize legal risks, and maximize the effectiveness of the shared information. One such best practice is establishing clear data governance policies. These policies should outline how data is collected, classified, stored, and shared, as well as who is authorized to access and use the intelligence. Data governance also involves the implementation of access controls and encryption to protect sensitive information from unauthorized access. By implementing these controls, organizations can help ensure that CTI sharing complies with legal and regulatory requirements while protecting the integrity and confidentiality of the data. Another operational best practice is to integrate CTI sharing into broader cybersecurity strategies, where intelligence sharing is considered part of an overall risk management process. Organizations should prioritize the collection and dissemination of relevant and actionable intelligence, ensuring that the shared information is timely, accurate, and specific. This approach allows organizations to respond quickly to emerging threats and reduce the time between the identification of a threat and the deployment of countermeasures.

It is also essential for organizations to establish strong communication and collaboration frameworks that support effective CTI sharing. This includes setting up protocols for sharing information with external partners, such as government agencies, industry groups, and other organizations that may face similar threats. Effective communication channels should facilitate the rapid exchange of intelligence, especially in the event of ongoing or imminent cyber incidents. Establishing a network of trusted partners is crucial for ensuring that the shared intelligence is acted upon quickly and appropriately. In addition to formalized communication channels, organizations should also establish incident response teams that can act swiftly on shared intelligence, helping to reduce the impact of a cyberattack or data breach.

Collaborative platforms and initiatives have emerged as powerful tools for facilitating CTI sharing while addressing some of the legal and operational challenges. One notable example of such initiatives is the Information Sharing and Analysis Centers (ISACs), which are sector-specific organizations that collect and analyze cyber threat intelligence within specific industries. ISACs play a critical role in promoting information exchange by providing a trusted environment for organizations to share sensitive intelligence without the fear of legal repercussions. These centers typically focus on specific sectors, such as energy, finance, healthcare, or critical infrastructure, allowing them to tailor their services to the unique needs and threats faced by those industries. For instance, the Financial Services ISAC (FS-ISAC) helps financial institutions share intelligence on emerging cyber threats, enabling rapid response and coordination. The ISACs also facilitate the development of best practices, offer training programs, and foster collaboration between public and private sector entities. Their role in helping organizations comply with legal and regulatory requirements while facilitating effective CTI sharing cannot be overstated (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

In addition to ISACs, other collaborative platforms have been established to facilitate global CTI sharing. One such initiative is the European Union Agency for Cybersecurity (ENISA), which supports member states and private organizations in enhancing cybersecurity through collaboration and information exchange. ENISA's work focuses on creating a strong cybersecurity culture across Europe, developing common standards for CTI sharing, and promoting the creation of cross-border cybersecurity partnerships. Similarly, industry-specific platforms such as the Health Information Trust Alliance (HITRUST) have become central hubs for the exchange of threat intelligence in the healthcare sector. These platforms allow stakeholders to share threat data and collaborate on improving cybersecurity measures within their sectors, making the exchange of information more efficient and impactful.

Public-private partnerships (PPPs) have also become a central element in the landscape of CTI sharing. These partnerships typically involve cooperation between government agencies, law enforcement, and private sector entities, with the goal of enhancing collective cybersecurity efforts. PPPs enable the sharing of critical information that may otherwise remain siloed within the private sector or government, thereby fostering a more coordinated response to cyber threats. A key benefit of PPPs is that they allow for the integration of real-time, actionable intelligence from multiple sources, helping organizations and governments to make informed decisions based on the latest threat data. The US Department of Homeland Security, for example, has worked extensively with private sector partners to enhance cyber resilience through initiatives like the National Cybersecurity and Communications Integration Center (NCCIC), which provides a collaborative space for public and private entities to share information on emerging cyber threats (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021). These partnerships also allow for joint efforts to address complex cyber threats that cross borders, ensuring that resources are pooled and efforts are streamlined.

In conclusion, the sharing of Cyber Threat Intelligence is an essential component of modern cybersecurity, but it must be done in a way that adheres to legal and ethical standards while promoting operational effectiveness. Legal principles such as transparency, accountability, and consent provide the foundation for trust, while operational best practices ensure that CTI sharing is both secure and effective. Collaborative platforms such as ISACs and public-private partnerships play a critical role in facilitating the exchange of intelligence and ensuring compliance with regulatory requirements. By following these best practices and engaging in collaborative initiatives, organizations can help build a more resilient cybersecurity ecosystem, where intelligence is shared quickly and effectively to counter the ever-evolving threat landscape.

6. Challenges and Barriers to Effective CTI Sharing

Effective Cyber Threat Intelligence (CTI) sharing is often impeded by a range of legal, operational, and security challenges that create barriers to seamless and collaborative cybersecurity efforts. While the benefits of CTI sharing are widely recognized, the hurdles involved in overcoming these challenges are significant. These barriers stem from a complex combination of legal frameworks, practical operational considerations, and the inherent risks associated with the exchange of sensitive data across organizational and national boundaries. Understanding these challenges is crucial for developing solutions that can promote safer, more efficient sharing of cyber threat intelligence.

Legal barriers are some of the most significant obstacles to effective CTI sharing. One of the key challenges stems from data privacy laws, which vary widely across jurisdictions. For instance, in regions like the European Union, data protection regulations, such as the General Data Protection Regulation (GDPR), impose stringent rules on the collection, processing, and sharing of personal data. These laws require organizations to obtain explicit consent from individuals before sharing their data, and they mandate that data be shared only under specific circumstances where privacy risks can be mitigated. While these regulations are essential for protecting individual rights, they can hinder the free flow of threat intelligence, particularly when personal data is involved. The complexity of these legal frameworks makes it difficult for organizations to navigate the nuances of compliance, especially when dealing with cross-border sharing of CTI. The GDPR, for example, may conflict with national security laws that encourage broader intelligence-sharing practices or may require organizations to obtain legal counsel to ensure compliance, which can delay the sharing process (Albakri et al., 2019).

Moreover, conflicting national regulations can create significant friction in the global exchange of CTI. Different countries have different standards for what constitutes acceptable data protection, privacy, and cybersecurity practices. For instance, while the United States prioritizes national security and intelligence gathering, often facilitating the exchange of sensitive data, other countries may have more stringent regulations that prioritize data sovereignty and individual privacy. These discrepancies can lead to challenges when organizations or governments seek to collaborate internationally. While some nations encourage open sharing of CTI to enhance collective security, others may impose restrictions based on political, legal, or security concerns. These conflicting national regulations may result in a lack of clarity about how CTI can be shared legally, which may discourage organizations from sharing intelligence for fear of breaching local laws or international agreements (Abu et al., 2018).

Another legal barrier that complicates CTI sharing is the issue of intellectual property (IP) rights. Many companies are hesitant to share threat intelligence because of concerns that sensitive information, such as proprietary software vulnerabilities or cybersecurity tactics, may be exposed. In some cases, organizations may have invested significant resources into developing cybersecurity technologies and processes, and sharing this intelligence could potentially put their competitive edge at risk. Intellectual property laws protect the innovations and trade secrets of organizations, but these same laws can inhibit collaboration when companies fear that sharing their knowledge could lead to a loss of their competitive advantage or expose them to legal risks. This reluctance to share valuable cybersecurity information can result in missed opportunities to prevent or mitigate cyberattacks (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

In addition to legal barriers, operational challenges also play a significant role in limiting the effectiveness of CTI sharing. One of the primary operational barriers is the issue of trust. Organizations, especially those in competitive industries, may be reluctant to share threat intelligence with others due to concerns about how the information will be used. Trust is essential for any collaborative effort, and in the context of CTI sharing, organizations must feel confident that their partners will not misuse the shared information or expose them to additional risks. This is particularly challenging in the private sector, where competitors may be hesitant to share intelligence, even when it is for the greater good of cybersecurity. To build trust, organizations must establish clear agreements, guidelines, and security measures that protect the data and ensure that it is used solely for its intended purpose. Without the establishment of such trust-building frameworks, the willingness to share CTI is likely to remain low, preventing effective collaboration (Albakri et al., 2019).

Another operational challenge is the complexity and inconsistency of data formats. Cyber threat intelligence is often shared in diverse formats, ranging from structured data (e.g., indicators of compromise such as IP addresses, domain names, or file hashes) to unstructured data (e.g., email communications or reports). Different organizations may use different standards and platforms for storing and sharing CTI, making it difficult to integrate and interpret intelligence from various sources. The lack of standardized data formats means that organizations may need to invest significant resources in converting or normalizing data before it can be used. Additionally, the interoperability of different cybersecurity tools and platforms is another challenge that complicates the sharing of intelligence. Without common standards for data formatting and compatibility, the process of sharing CTI becomes more cumbersome, reducing the timeliness and effectiveness of threat response efforts (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

Security concerns also pose a significant challenge to CTI sharing, particularly when sensitive or confidential information is involved. One of the primary risks is the exposure of shared data, which may inadvertently leak details about vulnerabilities, attack methods, or internal security measures. If such information falls into the wrong hands, it could lead to retaliatory attacks or further exploitation by malicious actors. For example, intelligence shared with one organization may be accessed by a hacker if proper security protocols are not in place, potentially turning shared CTI into a vulnerability. Ensuring that shared intelligence is securely transmitted, stored, and handled is paramount to minimizing these risks. Encryption, access control, and data anonymization are crucial practices to ensure that sensitive information is protected throughout the sharing process.

Additionally, there is the potential for misuse of shared data, which can create security risks of its own. If shared CTI is misused or shared with unauthorized parties, it can lead to unintended consequences, such as the exploitation of vulnerabilities or the manipulation of intelligence for malicious purposes. Moreover, sharing incomplete or inaccurate intelligence can lead to ineffective responses to cyber threats, wasting resources and potentially exacerbating the problem. To mitigate these risks, organizations must ensure that there are robust oversight mechanisms in place, including data validation processes, auditing, and monitoring systems, that track how CTI is shared and used. These systems help maintain the integrity of shared intelligence and ensure that it is used for its intended purpose of improving cybersecurity rather than compromising it (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

In summary, the challenges to effective CTI sharing are multifaceted, involving legal barriers such as data privacy regulations and intellectual property concerns, as well as operational issues like trust, data complexity, and interoperability. Additionally, security concerns about the exposure of sensitive information or the misuse of shared data further complicate the sharing process. Addressing these challenges requires a coordinated effort among governments, private sector organizations, and international bodies to create clear, consistent legal frameworks and technical standards, as well as to build trust and ensure the security of shared information. While overcoming these barriers may be difficult, the increasing complexity and scale of cyber threats make it essential to find ways to overcome these challenges to enable effective CTI sharing on a global scale (Abu et al., 2018; Amaro et al., 2022).

7. Recommendations and Future Directions

The legal landscape surrounding Cyber Threat Intelligence (CTI) sharing is intricate, influenced by a wide range of international and national regulations that sometimes hinder the seamless exchange of threat data. In order to overcome these challenges, several key legal reforms could significantly enhance the efficiency of CTI sharing while ensuring that privacy, security, and sovereignty concerns are respected. One of the foremost recommendations for improving international legal cooperation is the creation of harmonized legal frameworks that can facilitate cross-border sharing of cyber threat data. Currently, differing national and regional regulations create a fragmented approach to CTI sharing. A more unified legal framework, similar to the European Union's GDPR but with broader international application, could streamline data protection requirements while allowing for the exchange of critical threat intelligence. Such a framework would need to focus on reconciling privacy concerns with the operational need for rapid intelligence exchange. It would also need to establish clear guidelines for the handling of sensitive information, ensuring that legal protections for individuals and organizations are not compromised in the name of cybersecurity (Abu et al., 2018).

Additionally, international treaties that govern cybersecurity, such as the Budapest Convention on Cybercrime, could be further strengthened to include specific provisions for CTI sharing. These updates would provide clarity on how nations should handle the cross-border flow of cyber threat data and help to align legal standards. It is also essential that governments and international organizations work together to establish mutual recognition of cybersecurity certifications and standards, so that threat intelligence shared across borders is consistent and meets a minimum threshold of trustworthiness. Legal cooperation should be supported by regular diplomatic dialogue on cyber threats, which would help to create a global consensus on what constitutes “acceptable” sharing of CTI. By improving the alignment of cybersecurity laws across countries, a foundation could be laid for more efficient collaboration that benefits all stakeholders (Albakri et al., 2019; Ma et al., 2023; Purohit et al., 2023; Schaberreiter et al., 2019).

Building trust among stakeholders is a critical factor in fostering effective CTI sharing. Trust is often the key barrier preventing organizations and governments from sharing their sensitive data. As a result, creating mechanisms for transparency, accountability, and mutual benefit is vital to enhancing collaboration. Trust can be built through clearly defined agreements, such as Memoranda of Understanding (MOUs) and data-sharing contracts, which outline the responsibilities, expectations, and benefits for all parties involved. These agreements can help ensure that intelligence is shared only for legitimate, pre-agreed purposes and with safeguards against misuse. Additionally, ensuring that stakeholders, particularly private sector entities, are reassured about the protection of their intellectual property and confidential information is essential for fostering participation in CTI sharing programs. Public-private partnerships (PPPs) have proven to be a useful model for facilitating trust-building. In these collaborations, government agencies can provide a secure framework for data exchange, while private entities can share their critical intelligence with public authorities without fear of violating competitive or privacy concerns (Albakri et al., 2019).

Another strategy for fostering trust is the establishment of secure and standardized platforms for CTI sharing. These platforms can act as neutral spaces where stakeholders can exchange information while ensuring that their data remains protected. Trust can also be built by ensuring that there are clear, legally binding agreements regarding the use of shared intelligence. In many cases, ensuring that these agreements are standardized across regions or sectors would help to further reduce friction in sharing. Collaborative frameworks that provide a structured environment for continuous and reliable information exchange will further improve the overall security posture of participating organizations and governments (Menges et al., 2019; Papanikolaou et al., 2022; Yücel et al., 2021).

Technological innovation plays a pivotal role in addressing the operational and legal challenges associated with CTI sharing. Emerging technologies such as blockchain and artificial intelligence (AI) offer promising solutions to some of the most pressing issues in the cybersecurity space. Blockchain, for example, can provide an immutable and transparent ledger for CTI transactions. By using blockchain technology, organizations can ensure that threat intelligence data is both traceable and tamper-proof, making it easier to verify the authenticity and integrity of the shared information. This would help mitigate concerns about the accuracy and reliability of data shared across jurisdictions. Furthermore, blockchain can also address the challenge of data sovereignty by ensuring that data sharing is conducted according to agreed-upon protocols and that data ownership remains clearly defined, even across borders (Rangaraju, 2023; Suryotrisongko et al., 2022; Tang et al., 2023).

Artificial intelligence, on the other hand, can streamline the processing and analysis of large volumes of threat data, improving the speed and efficiency of CTI sharing. AI algorithms can automatically detect patterns and anomalies in cyber threat data, helping organizations identify emerging threats and vulnerabilities more rapidly. Additionally, AI can assist in improving interoperability by enabling different systems and platforms to communicate with each other more effectively, despite differences in data formats and protocols. This would reduce some of the operational barriers to CTI sharing, such as the complexity of data formats and the lack of compatibility between different tools and platforms. By leveraging AI and blockchain, organizations can not only ensure that their CTI sharing processes are faster and more reliable but also more secure and compliant with legal requirements (Albakri et al., 2019).

8. Conclusion

The global landscape of Cyber Threat Intelligence (CTI) sharing is shaped by a complex web of legal, operational, and security challenges, but it also offers substantial opportunities for enhancing collective cybersecurity efforts. Through improved legal frameworks, trust-building strategies, and technological advancements, stakeholders can overcome these barriers and create a more efficient and effective CTI-sharing environment. Legal reforms, such as the harmonization of international regulations and treaties, are essential for ensuring that data protection and privacy concerns are addressed while allowing for the timely exchange of critical threat information. Building trust among stakeholders, particularly between governments, private sector entities, and public-private partnerships, is equally important in overcoming reluctance to share intelligence. Collaborative platforms and clearly defined agreements are crucial in facilitating trust and ensuring that shared data is used for legitimate purposes.

Emerging technologies, including blockchain and artificial intelligence, offer innovative solutions to many of the operational and legal obstacles associated with CTI sharing. These technologies can enhance transparency, improve data integrity, and streamline the process of analyzing and sharing large volumes of threat intelligence data. As the cyber threat landscape continues to evolve, it is imperative that legal, operational, and technological innovations work in tandem to create a secure and cooperative environment for CTI sharing. By addressing the challenges and capitalizing on opportunities, stakeholders can significantly improve their collective cybersecurity posture and better protect against the increasingly sophisticated and dynamic threats that continue to emerge in the digital age.

The future of CTI sharing lies in continued collaboration, innovation, and reform. The ongoing evolution of legal frameworks, the strengthening of partnerships between governments and private entities, and the adoption of cutting-edge technologies will be essential in achieving a more resilient and responsive global cybersecurity ecosystem. As cyber threats become more complex and widespread, a unified and proactive approach to CTI sharing will be crucial in safeguarding critical infrastructure, data, and systems worldwide.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abu, S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Albakri, A., Boiten, E. A., & Lemos, R. d. (2018). Risks of Sharing Cyber Incident Information. 1-10. https://doi.org/10.1145/3230833.3233284

Albakri, A., Boiten, E. A., & Lemos, R. d. (2019). Sharing Cyber Threat Intelligence Under the General Data Protection Regulation. 28-41. https://doi.org/10.1007/978-3-030-21752-5_3

Ma, X., Dong-sheng, Y. U., Du, Y., Li, L., Wen, N., & Lv, H. (2023). A Blockchain-Based Incentive Mechanism for Sharing Cyber Threat Intelligence. *Electronics*, *12*(11), 2454. https://doi.org/10.3390/electronics12112454

Menges, F., Sperl, C., & Pernul, G. (2019). Unifying Cyber Threat Intelligence. 161-175. https://doi.org/10.1007/978-3-030-27813-7_11

Papanikolaou, A., Alevizopoulos, A., Ilioudi, C., Demertzis, K., & Rantos, K. (2022). A Cyber Threat Intelligence Management Platform for Industrial Environments. https://doi.org/10.5121/csit.2022.122206

Purohit, S., Neupane, R. L., Bhamidipati, N. R., Vakkavanthula, V., Wang, S., Rockey, M., & Calyam, P. (2023). Cyber Threat Intelligence Sharing for Co-Operative Defense in Multi-Domain Entities. *Ieee Transactions on Dependable and Secure Computing*, *20*(5), 4273-4290. https://doi.org/10.1109/tdsc.2022.3214423

Rangaraju, S. (2023). Ai Sentry: Reinventing Cybersecurity Through Intelligent Threat Detection. *Eph - International Journal of Science and Engineering*, *9*(3), 30-35. https://doi.org/10.53555/ephijse.v9i3.211

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2022). Cyber Threat Intelligence Sharing Scheme Based on Federated Learning for Network Intrusion Detection. *Journal of Network and Systems Management*, *31*(1). https://doi.org/10.1007/s10922-022-09691-3

Sauerwein, C., Fischer, D., Rubsamen, M., Rosenberger, G., Stelzer, D., & Breu, R. (2021). From Threat Data to Actionable Intelligence: An Exploratory Analysis of the Intelligence Cycle Implementation in Cyber Threat Intelligence Sharing Platforms. 1-9. https://doi.org/10.1145/3465481.3470048

Schaberreiter, T., Kupfersberger, V., Rantos, K., Spyros, A., Παπανικολάου, A., Ilioudis, C., & Quirchmayr, G. (2019). A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources. 1-10. https://doi.org/10.1145/3339252.3342112

Suryotrisongko, H., Musashi, Y., Tsuneda, A., & Sugitani, K. (2022). Robust Botnet DGA Detection: Blending XAI and OSINT for Cyber Threat Intelligence Sharing. *IEEE Access*, *10*, 34613-34624. https://doi.org/10.1109/access.2022.3162588

Tang, B., Wang, J., Qiu, H., Yu, J., Yu, Z., & Liu, S. (2023). Attack Behavior Extraction Based on Heterogeneous Cyberthreat Intelligence and Graph Convolutional Networks. *Computers Materials & Continua*, *74*(1), 235-252. https://doi.org/10.32604/cmc.2023.029135

Yücel, Ç., Lockett, A., Chalkias, I., Mallis, D., & Katos, V. (2021). MAIT: Malware Analysis and Intelligence Tool. *Information & Security an International Journal*, *50*, 49-65. https://doi.org/10.11610/isij.5024