



Role of Cyber Intelligence in Countering Cyber Threats: A Narrative Review

Okoma, Victoria N.

Computer Science Department, Federal Polytechnic Oko, Anambra State, Nigeria

Abstract

With the cyber threat landscape constantly changing, robust cyber intelligence practices continue to be adopted worldwide. New studies emphasize the importance and value of cyber intelligence as a powerful tool to help neutralize cyber threats; companies with sophisticated cyber intelligence functions had a lower rate and severity of cyberattacks. As the cyber threats continue to escalate at a dramatic rate, the cybersecurity industry can be expected to experience significant growth, and cybersecurity spending will grow to about \$1 trillion per year in the near future. Increased ransomware attacks are happening across the globe and in 2021, ransomware attacks in the US increased by 250% compared to 2020, CISA states. But there are lots of organizations, particularly small to medium-sized companies (SMEs), that don't have cyber intelligence awareness. In 2022, the Department of Homeland Security reported that about 60% of SMEs don't have dedicated cyber intelligence capabilities, which makes them vulnerable to exploitation. This gap highlights an urgent need to increase awareness and support for cyber intelligence efforts across the board, particularly among SMEs, to combat cyber threats successfully. In this study, we conduct a thorough review of the literature, case studies, and expert knowledge and discuss the role of cyber intelligence in addressing cyber threats. It discusses several aspects, such as cyber intelligence integration in security operations, effectiveness of threat intelligence sharing, and proactive approaches to security. The outcomes showed that the organizations that are using cyber intelligence are able to anticipate, identify and respond to the cyber threats more quickly.. Incorporating cyber intelligence improves threat detection and allows for preventive actions. In addition, the exchange of cyber threat information helps in improving defences against any new threat. By adopting cyber intelligence, organizations can gain an edge over cyber adversaries, reduce their vulnerabilities, and reduce impacts from cyber attacks. Security experts describe several terms related to cyber threats. Security experts use a variety of terms that tie into cyber threats.

Keywords Cyber Intelligence, Cyber Threats, Cybersecurity, Threat Detection, Proactive Defense, Threat Intelligence Sharing

Citation Okoma, V. N. (2026). Role of Cyber Intelligence in Countering Cyber Threats: A Narrative Review. *American Journal of Applied Sciences and Engineering* 7(3) 1-10.
<https://doi.org/10.5281/zenodo.23256229>



1. Introduction

Rapid growth in cybersecurity threats is forecast to create significant gains for the cybersecurity sector around the world, with cybersecurity expenditure estimated to amount to about \$1 trillion each year in the near future (Myrsalieva et al., 2026; Rizvi et al., 2025). The increasing number of cyber threats is a problem for everyone, be they an individual, a business or a government in today's digital world. These threats are constantly changing and improving, and there is a need to take forward looking and proactive steps to effectively manage risks. In this pursuit, cyber intelligence proves to be an essential element, providing insights and actionable intelligence to proactively identify, detect and defuse cyber threats before they can inflict damage. Cyber intelligence involves gathering, analyzing, and sharing information about potential cyber threats, vulnerabilities, and adversaries (Dekker & Alevizos, 2023; Saeed et al., 2023; Sun et al., 2023). It aggregates data from multiple sources such as open source intelligence, human intelligence, technical intelligence, and signals intelligence for complete situational awareness and to assist decision-making. The role of cyber intelligence in combating cyber threats is inestimable. Increasingly, organizations as they make use of digital technologies to function, are becoming more susceptible to cyber assaults (Ainslie et al., 2023). Recent reports indicate that cyber threats are becoming more common and more problematic (Aslan et al., 2023; George et al., 2023; Shandler & Gomez, 2023). The Federal Bureau of Intelligence's (FBI's) Internet Crime Complaint Center (IC3) reported 791,790 complaints of suspected internet crime in 2020, resulting in losses of more than \$4.2 billion (Belmabrouk, 2023). According to the Certified Information Systems Auditor (CISA) in the USA, ransomware attacks went up 250% from 2020 to 2021 (Beardwood, 2023; Hyslip & Burruss, 2023). Even as awareness and understanding of cyber intelligence is increasing, there are still many entities that do not have the same awareness and understanding. Small to medium enterprises (SMEs) are vulnerable, with the Department of Homeland Security reporting in 2022 that about 60% of these do not have a dedicated cyber intelligence team (Chaudhary & Bansal, 2022; Ilca et al., 2023). The numbers highlight the importance of powerful cyber intelligence capabilities to protect against cyber adversaries in cyberspace. Furthermore, the impact of cybercrime is increasing in financial terms, as well as in terms of reputational damage, legal liability, and regulatory penalties for organizations. This financial cost reflects the need for proactive cyber intelligence efforts to minimize exposure to cyber risk and strengthen resiliency to new threats. Given these issues, this narrative review aims to discuss both the capacities and the contributions of cyber intelligence in the fight against cyber threats in a comprehensive manner. This study will incorporate literature review, frameworks, and case studies to identify the importance of cyber intelligence in improving the overall cybersecurity position and reducing the effects of cyber threats on organizations and society. This review aims to offer insights and recommendations for those looking to enhance their cyber intelligence capabilities and to respond to the evolving cyber threat landscape. In summary, this review highlights the need for cyber intelligence as a proactive and strategic solution to cyber threats. With timely and actionable intelligence, organizations can proactively detect, predict and react to cyber attacks, reducing risk and protecting digital assets and operations.

2. Literature Review

Cyber threats have been on the rise and are a significant challenge for organisations and governments around the world. The cyber intelligence area of cyber security is still emerging and evolving, aiming to deliver proactive cyber intelligence and information to effectively detect, evaluate, and resist cyber risks (Kotsias et al., 2023; Shin & Lowry, 2020; Sun et al., 2023). There are multiple definitions and theories about cyber intelligence published by academics. For instance, cyber intelligence is the practice of assessing cyber adversary capabilities and intentions, and also gathering information about their activities and information for decision makers (Alsmadi, 2019; Brown et al., 2015; Sun et al., 2023). Furthermore, several frameworks are proposed and can be used in organizations for collecting, analysing, disseminating, and applying cyber intelligence in a structured manner, such as the Cyber Intelligence Cycle (Ahrend et al., 2016; Tounsi & Rais, 2018). Cyber intelligence can be gathered from various sources in several ways, from more technical sources such as malware analysis and network traffic monitoring to more human intelligence sources such as insider threat reporting and social engineering techniques. Specifically, open-source intelligence (OSINT) has emerged as a powerful tool for cyber intelligence (Chaudhary & Bansal, 2022; Day et al., 2017) that gathers information from websites, social media platforms, and other public sources on the internet (Day et al., 2017; Pai & Prasad, 2021; Potz, 2021). Several studies have highlighted the importance of cyber intelligence in detecting and attributing threats, and have demonstrated how cyber intelligence can be used to help identify the

source, motivations, and techniques of cyber adversaries. Cyber threat intelligence (CTI) has been discussed as a method for identifying who was responsible for a cyber attack by analyzing the attack indicators, including the malware signatures, infrastructure analysis, and attack behavior (Kant & Amrita, 2022; Lanz, 2022; Möller, 2023; Santos et al., 2025). While cyber intelligence has potential benefits, it is confronted with several challenges and limitations such as volume and velocity of data, complexity of cyber threats, and the need for specialized analysts and technologies. Furthermore, challenges like information sharing, data privacy, and legal restrictions add to the difficulties of successful use of cyber intelligence at the cross-border level. Scholars and practitioners have presented the best practices and recommendations for cyber intelligence program implementation. This also involves the development of strong information-sharing partnerships (Kayode-Ajala, 2023), the use of threat intelligence platforms and tools (Leszczyna & Wróbel 2019), the promotion of collaboration and information sharing within organizations (Shin & Lowry, 2020), and the continuous training and skill development of cyber intelligence analysts (Kayode-Ajala, 2023; Shin & Lowry, 2020). Empirical studies and case studies offer lessons learned about the value cyber intelligence can bring to the fight against certain cyber threats and to improve organizational resilience. The impact of cyberattacks and how quickly an organization can recover from any security incident can be analyzed using cyber intelligence capabilities, as demonstrated in the following studies: the NotPetya ransomware attack and the SolarWinds supply chain compromise (Enache, 2022; Kausar et al., 2023; Möller, 2023). Organizations can build intelligence capabilities that are proactive and strategic by using a variety of tools, techniques and approaches to gather, analyze and act on cyber threats effectively. But the issues and constraints associated with cyber intelligence must be further tackled through sustained investment in technology, training, and working together and sharing information between public and private organizations. The integration of cyber intelligence into security operations is part of the process. The process includes

Integration of Cyber Intelligence into Security Operations

Proactive and multi-faceted cyber strategy and practice must be combined with an effective integration of cyber intelligence into security operations to implement a successful cybersecurity program. With timely and actionable intelligence, organizations can improve the effectiveness of their ability to detect, prevent, and respond to cyber threats. The use of cyber intelligence in a security operation is analysed with an emphasis on the strategies, challenges and best practices. Cyber intelligence is a key part in greatly improving threat detection and prevention in security operations. When indicators of compromise (IOCs) are analyzed properly, they can be used to proactively discover and block potential threats before they can enter an organization's network, such as malicious IP addresses, file hashes, and domain names. Threat intelligence feeds can be used to automatically block known malicious entities (KMEs) in security devices like firewalls, intrusion detection systems (IDS), and endpoint protection platforms (EPP) (Chakraborty & Nisha, 2022; Torres et al., 2022). Cyber intelligence can be instrumental during a security incident; it can be used to provide valuable insights that can help in incident response and mitigation. Organizations can effectively prioritize alerts, validate incidents, and orchestrate response actions by correlating real-time threat intelligence with security event data (Aslan et al., 2023; González-Granadillo et al., 2021). Moreover, threat intelligence is useful in developing incident response playbooks, which will assist the security teams in handling and mitigating security incidents and ensuring minimum disruption in the organizational processes (Koloveas et al., 2021; Leite et al., 2022). Organizations can prioritize and remediate vulnerabilities using cyber intelligence through the provision of data about new threats, attack techniques, and the availability of patches. The incorporation of threat intelligence information in the vulnerability management process can enable organizations to identify assets with greater risks of attacks, the vulnerability of those assets to known threats, and prioritization of the remediation efforts. Moreover, CTI can help design a cyber threat-informed vulnerability management strategy and target systemic vulnerabilities.

Creating a robust cyber security culture within the organization requires educating employees about the rising challenges in the cyber world and best practices (Mughal, 2022). Cyber intelligence can be used to create scenarios for security awareness and training initiatives, including real-life examples of cyber attacks, threat actor methods and mitigations. The use of threat intelligence in simulated phishing exercises, security awareness training modules and even table top exercises will provide organizations the capability to arm their employees with the necessary skills in detecting and handling the threats in their everyday work environment. The security operations should be kept up to date constantly in order to ensure that organizations remain up-to-date in terms of the threats. Through

the use of cyber intelligence, organizations will always have access to the latest information about the new threats, trends and even the tactics of the adversaries and can tailor their security measures to counteract such threats. Conducting regular threat assessments, intelligence-driven risk assessments and even post-incident reviews will enable organizations to determine their vulnerabilities and invest in people, processes and technology in order to tackle the emerging threats. It is important for organizations to have the necessary cyber intelligence to feed into their security operations in order to be able to adopt a proactive and dynamic security posture. But integration is not just about overcoming the obstacles between silos – it also relies on the commitment to invest in technology, training, and constant enhancements and changes to stay ahead of threats. As a strategic enabler to security operations, cyber intelligence can help to better safeguard their organization assets, data and reputation in a more complex and dynamic threat landscape.

2.2 Effectiveness of Cyber Threat Intelligence Sharing

The success of cyber threat intelligence sharing is well documented as a key part in improving resilience among organisations, industries and countries. Through the sharing of timely and actionable threat intelligence, the stakeholders are able to get insights on how to deal with cyber threats, help incident response and also improve the defenses against new cyber threats. The sharing of cyber threat intelligence allows organizations to have a wider perspective on the cyber threat landscape. Being aware of the information on the new attacks, methods of attack, and indicators of compromise (IOCs) will enable the stakeholders to better understand their situation and be able to identify and take action on any potential threat to their system and data (Schlette et al., 2021; Tounsi & Rais, 2018). This common understanding is the foundation of the efforts that are needed for an organization to invest and plan their defenses based on the threats that exist. The sharing of cyber threat intelligence helps with threat detection and response. When organizations share their information, they can glean insights into threat actor tactics and motivations and improve the organization's threat intelligence capabilities. Information-sharing communities are utilized for sharing resources and expertise that reduce the costs and optimize the usage of the resources. However, problems such as technical compatibility and data privacy should be considered with proper governance practices. Collaboration and trust lead to the creation of a good cyber threat intelligence sharing process, and this leads to greater cybersecurity resilience in the face of changing threats.

2.3 The Role of Cyber Intelligence in Proactive Defense Strategies

With the changing nature of the cyber threat landscape, organizations have to take proactive actions in order to defeat their adversaries and be more effective in managing cyber risks. The element of cyber intelligence plays an essential role in making proactive defense because it provides an organization with the required contextual knowledge and situational awareness to anticipate, detect and neutralize any kind of emerging threat (Ainslie et al., 2023). Organizations can gain insights into indicators of compromise, suspicious activity, and potential attack paths before they are exploited by continually monitoring and analysing threat data from multiple sources. Proactive threat hunting can be used to identify and disrupt threats before they realize themselves into full-fledged attacks, helping organizations to prepare for potential threats. This proactive strategy allows organizations to stop attacks before they can happen, lower the amount of time cybercriminals stay in an organization's system and avoid data breaches and security incidents. By continuously evaluating and adapting their security posture in real-time according to the latest threat intelligence, organizations can achieve a cyber adaptive security posture that is more effective. Incorporating threat intelligence into risk management strategies will enable organizations to focus security investments, direct resources, and optimize defensive posture to the most relevant and impactful threats. By offering actionable insights and context during a security incident, cyber intelligence supports organizations' incident response capabilities—helping them make decisions fast and take the right action. This is a proactive approach that organizations can adopt in their efforts to contain and reduce the impact of security incidents, thus preventing business disruptions and reducing costs associated with any cyber attacks.

Through the use of collaboration and information sharing in the use of cyber intelligence, organizations are able to collaborate with each other and prevent the common cyber threats and attackers. Organizations are able to join information sharing communities and share their information about any cyber threats, best practices and what they have learned from any experience. With the development of the cyber landscape, cyber intelligence has been an

important part of any proactive defense approach through which companies are able to proactively detect, neutralize and anticipate any cyber threats. With timely and actionable intelligence, organizations can prepare themselves for any dangers and undertake threat hunting, better their risk management, have an improved incident response and work in collaboration with trusted parties in order to share information. Through taking proactive measures in their approach to cybersecurity, organizations are able to be prepared for any attackers or cyber threats.

3. Methodology

The researcher adopted the narrative review methodology in analyzing past researches about the adequacy of the role of cyber intelligence in countering cyber threats; narrative review. Narrative inquiry, which is mostly used in descriptive or explanatory research, is a technique where various primary sources of study are synthesized to develop an interpretation based on existing theories and the reviewer's expertise (Aguboshim, 2021; Jones, 2004; Siddaway et al., 2019). The method is ideal for a holistic investigation of scholarly topics that allow the identification of insights through vast literature and collective knowledge (Aguboshim et al., 2023). In this paper, the author conducted a review of peer-reviewed journals by using the processes of keyword and term identification, selection, quality assessment, data extraction and synthesis as part of the narrative inquiry process. The studies were selected for review depending on their relationship to the topic of study and the role of cyber intelligence in countering cyber threats. Peer-reviewed journals, academic publications, white papers and reports not older than ten years were used in the review.

3.1 Data Collection

Data collection for the research work on the role of cyber intelligence in countering cyber threats involved identification of relevant literature related to the subject area. A literature search and review was carried out by gathering and reviewing literature and materials that are related to the existing studies on cyber intelligence and its application against cyber threats. The academic databases used were relevant to intelligence studies, namely PubMed, IEEE Xplore, ACM Digital Library and Google Scholar, journals, and conferences. Search terms used in the literature search were: cyber intelligence, threat intelligence, cyber threats, cybersecurity, information sharing, and pro-active defense. Additionally, case studies and examples of organizations or government agencies that were successful in using cyber intelligence to enhance their defensive measures and mitigate cyber threats were identified. The case studies were analyzed to get practical implications of using cyber intelligence for proactive defense strategies. Government reports and policies on cyber intelligence and cybersecurity strategy were also studied. Words like "cyber intelligence," "threat intelligence," "cyber threats," "cyber security," "information sharing," and "proactive defence" have been used in order to find out the related research work, studies, articles, frameworks, and reports. Going through industry-related reports and surveys helps in finding out industry-specific information and best practices. Open-source intelligence was monitored in real time for cyber threats. The researcher also worked in collaboration with stakeholders for having different perspectives on the topic and verifying findings. In the end, data documentation and organization were reviewed, as it is important for analysis and drawing meaningful conclusions.

3.2 Data analysis and Synthesis

Following the collection of data on the importance of cyber intelligence in dealing with cyber threats, the next steps included analysis, synthesis, and making conclusions based on the collected information. In the process of analysis, several data sources were examined and analyzed, which included literature, case studies, primary research, and reports from industry and government. We sought to highlight the prevailing themes, trends, and insights about the importance of cyber intelligence in proactive defense strategies. Quantitative approaches were applied to evaluate the effectiveness, problems, and best practices associated with the use of cyber intelligence in dealing with cyber threats. Then the data analyzed was synthesized into a story that is suitable for the purposes of our research. The results were presented in logical sections including advantages and problems, best practices and future directions. The connections between various sources of data enabled us to have a holistic overview of the importance of the topic to stakeholders in cybersecurity. Important findings and insights emerging from the process of analysis and synthesis of data were identified. Specific trends, success factors, and lessons learned about the role of cyber intelligence in proactive defense strategies were identified.

4. Findings and Discussion

The key findings from the identification process encompassed several concrete observations as shown in Table1.

Table 1: Key Findings on the Role of Cyber Intelligence in Countering Cyber Threats

S/No.	Type of Cyber Intelligence	Benefits	Implementation Challenges	Best Practices	Future Directions
1	Strategic Cyber Intelligence. Threat trends and future risk assessments	Enhances decision making and situational awareness	Timing of trends and future risk assessments is constrained	Combination of intelligence in risk management and strategic planning	Future prediction and analysis of strategic cyber threats via artificial intelligence are used to manage risks and planning.
2	Tactical and Operational Cyber Intelligence. Tactics, techniques and procedures. Indicators of compromise, vulnerability and attacks Patterns	Help in detection and response of the threats	Data overload and interoperability and skills problems	Continuous monitoring and threats hunting.	Detection, prediction and response powered by Artificial Intelligence.
3	Collaborative Cyber Intelligence and Information Sharing: information sharing among stakeholders of the cybersecurity incident and threat landscape	Enhances collective defense and threat awareness of stakeholders	Privacy, trust, interoperability, and regulatory issues	Reliable information sharing and public-private partnerships	Automated, privacy-preserving, and information-sharing about threats among stakeholders of the cybersecurity incident and threat landscape

The results shown in Table 1 indicate that the number of organizations adopting cyber intelligence for proactive cyber defense is increasing. The cyber intelligence tools found in the literature span from primarily reactive security solutions to intelligence-based solutions that look to the future and forecast how cyber threats might arise, be understood, and be mitigated. The results were broken down into three strategic categories, strategic cyber intelligence, operational/tactical cyber intelligence, and collaborative and information sharing cyber intelligence. Organizations can leverage different aspects of each category to enhance their cybersecurity Strategic cyber intelligence is a valuable tool that can be used to make informed cybersecurity decisions. It is based on the threats reported, the risks that are emerging and the geopolitical situation and geopolitical projections to provide decision-makers with a broader view of the cyber threat landscape. It offers a number of significant advantages such as enhanced situational awareness, prediction of future threats, and better prioritization of cybersecurity investments and resources.

The results showed that the companies that used intelligence in the ERM process were more likely to successfully link their cyber security activities to the threats and vulnerabilities they faced. But the challenges of strategic cyber intelligence might include inadequate supply of reliable and timely intelligence, a lack of analysts, challenges of turning intelligence into actionable decision, and a dynamic threat landscape. These are all signs of the need for continuous threat assessment, engagement of senior management, intelligence-driven policy making, and embedding of cyber intelligence within organizational governance. Continued growth in the use of AI to support strategic analysis, predictive threat assessment, and the integration of cyber intelligence into organizational and national cybersecurity policies and strategies are expected in the future. Operational and tactical cyber intelligence is the timely and relevant assistance needed for cyber defense. It includes adversarial tactics, techniques and procedures (TTPs), adversarial attack patterns, adversarial vulnerabilities, adversarial indicators of compromise (IoCs), and information on current cyber campaigns.

The results show that this intelligence helps organizations improve early threat detection, perform proactive threat hunting, respond quickly to incidents and recognize and mitigate vulnerabilities before they are exploited, minimizing potential impact of cyber incidents. The fragmented security tools, technical interoperability issues, security data volume, lack of real-time monitoring and a shortage of skilled cybersecurity personnel, however, pose challenges to implementation. It is thus essential to continuously monitor, employ cutting-edge threat-detection capabilities, adopt proactive threat hunting, deploy the right levels of automation, feed the latest intelligence feeds, and have the right incident-response capabilities in place for effective implementation. In future, it is anticipated

that more and more countries will deploy AI and machine learning to drive automated threat detection, automated response and predictive analytics, and incorporate with Security Operations Centers (SOCs) and extended detection and response capabilities. Collaborative and information sharing cyber intelligence is about the need for information sharing and collaboration between organizations, government, industry players and the cybersecurity communities. Ad hoc and local defensive measures are not always adequate to counter complex and dynamic attacks that may find their way past organizational boundaries. Collective Defense, Awareness of emerging threats, speeding up dissemination of indicators and attack information, and increasing sector-wide

Resilience are all boosted by effective Intelligence Sharing. Data privacy and confidentiality concerns, lack of trust, incompatible systems and standards, regulations, unwillingness to share sensitive data, and lack of information sharing infrastructure, however, limit information sharing. The results highlight the importance of trusted information-sharing mechanisms, public-private partnerships, standardized standards and protocols, trusted sharing of information, and cyber threat intelligence-sharing platforms. Going forward, automated and secure intelligence sharing ecosystems, intelligence standardisation, privacy-preserving methods, public-private intelligence collaboration and demand for greater international cooperation to tackle transnational cyber threats are expected to be forthcoming. There were a few consistent factors that led to success in all three categories. The quality, timeliness and relevance of intelligence is heavily reliant upon the quality of the information that feeds data collection mechanisms, therefore it is important to have robust data collection mechanisms in place. Sophisticated threat detection technologies help convert vast amounts of security information into valuable intelligence.

Through the threat hunting approach, security teams can employ a structured process to go through the information for signs of malicious activity, even when there are no security events. Stakeholder collaboration will similarly increase the speed and extent of threat data collection, thus improving the intelligence process. The results also indicate that among the measures that organizations could undertake to improve their cyber resilience is continuous monitoring, incident response, risk management, and workforce development. This way, the organization will be able to detect any changes in the threat environment and act quickly whenever there is any suspicious activity. Response to any incident will help reduce the impact of the attack. On the other hand, flexible risk management will enable the organization to change its security policy and priorities when necessary. Workforce Training and Development is also critical due to sophisticated technologies of intelligence require knowledgeable workers to interpret the intelligence and translate it into proper security measures. The implementation challenges highlight the need to view cyber intelligence as more than just a technical project. Cyber Intelligence is a result of the engagement of people, processes, technologies, governance and collaboration. The best detection technologies will be of little benefit if they do not have trained people to interpret the results. Similarly, if there is no privacy protection, or trust building measures, on information sharing platforms, nothing will happen. To achieve success, it's important to integrate an organizational strategy, rather than investing in each security technology separately.

Table 1 shows the future directions identified, with the cyber intelligence becoming more dynamic. Artificial intelligence, machine learning, predictive analysis, automated threat detection and response, secure intelligence sharing mechanisms, and other capabilities are expected to increase organizations' ability to process vast amounts of increasingly complex threat information. But with technological progress, it is necessary to have suitable governance, privacy protection, interoperability standards, professional development, and sensible sharing of information. As automation increases, there are a number of needs for proper governance, validation, and accountability. To summarize, from the results obtained, it can be concluded that cyber intelligence is not only limited to detecting cyber threats. This is because strategic intelligence helps make decisions and priorities, operational intelligence helps to detect and hunt threats, while collaborative intelligence helps to share information for collective defense. These are all examples of complementary functions that are all elements of a more proactive cyber security approach. Findings from literature review, case studies, industry reports and policy documents support the credibility of the findings. The data points converge and offer a wide foundation for the advantages, hurdles, and best practices for the future of cyber intelligence. The results highlight the importance of cyber intelligence as a proactive defense tool and offer actionable recommendations for organizations looking to enhance their cybersecurity posture and resilience in today's ever-changing cyber threat landscape.

5. Implications and Recommendations

Our analysis reveals the significant importance for organizations to integrate cyber intelligence into their defense strategies, to effectively deal with the emerging cyber threats. Policymaker should revise policies to reflect the value of cyber intelligence and call for collaboration among players. Also, academics and research centres should research and develop cyber intelligence methodologies to meet the changing threats. It is essential that organizations put in place comprehensive training and education programs to educate their staff on cyber intelligence concepts. To create an environment of information sharing, public-private partnerships must be promoted by the governments and industry stakeholders to create information sharing frameworks and platforms. Furthermore, prioritizing data privacy and security and establishing cyber threat intelligence sharing platforms for collective defense capabilities should be emphasized. Finally, with respect to the dearth of skilled people, measures should be taken to improve this, such as educational programs and work training. These recommendations can help stakeholders improve their resilience and implement cyber intelligence into proactive defense efforts.

6. Conclusion

Organizations can apply cyber intelligence to improve their situational awareness, which can assist in applying a proactive approach to address new threats. Minimizing potential security impact and use of cyber intelligence assists in the early detection and prevention of cyber threats. Cyber intelligence can be used proactively to search for the threats and prevent them from becoming a problem for the organization. Cyber intelligence goes into risk management processes to help organizations prioritize its investments in security and to deal with security threats that are high risk. The sharing of information amongst organizations makes the collective defence capability stronger and assists to develop resilience to cyber threats. Technical interoperability and data privacy are some of the issues that pose a challenge to successful cyber intelligence integration. These challenges will need to be met through a collective effort and investment in technology, training and governance structures. Last, but not least, proactive defense mechanisms should be designed and put in place based on cyber intelligence by organizations, governments and industry partners. In the complex threat landscape of today, one of the most important ways to protect assets, data and operations is to accept cyber intelligence as a strategic enabler of resilience. Our study offers valuable insights and recommendations to enhance posture and resilience in the face of evolving risks.

References

- Aguboshim, F. C. (2021). Adequacy of sample size in a qualitative case study and the dilemma of data saturation: A narrative review. *World Journal of Advanced Research and Reviews*, 10(03), 180-187. <https://doi.org/10.30574/wjarr.2021.10.3.0277>
- Aguboshim, F. C., Obiokafor, I. N., & Emenike, A. O. (2023). Sustainable data governance in the era of global data security challenges in Nigeria: A narrative review. *World Journal of Advanced Research and Reviews*, 17(02), 378-385. <https://doi.org/10.30574/wjarr.2023.17.2.0154>
- Ahrend, J. M., Jirotko, M., & Jones, K. (2016). *On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge* [Paper presentation]. 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-10), London, UK. <https://doi.org/10.1109/CyberSA.2016.7503279>
- Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 132:103352. <https://doi.org/10.1016/j.cose.2023.103352>
- Alsmadi, I. (2019). *Cyber intelligence analysis*. In: The NICE Cyber Security Framework. Springer, Cham. https://doi.org/10.1007/978-3-030-02360-7_6
- Aslan, Ö., Aktu, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6):1333. <https://doi.org/10.3390/electronics12061333>
- Beardwood, J. (2023). Cyberbreaches in Critical Infrastructure: It's not just about personal data breaches anymore (Part 1)? A comparison of the new security regime for critical infrastructures in Canada, USA and EU. *Computer Law Review International*, 24(4), 109-114. <https://doi.org/10.9785/cri-2023-240404>
- Belmabrouk, K. (2023). Cyber criminals and data privacy measures. In *Contemporary Challenges for Cyber Security and Data Privacy* (pp. 29). DOI: 10.4018/979-8-3693-1528-6.ch011

- Brown, S., Gommers, J., & Serrano, O. (2015). *From cyber security information sharing to threat management* [Paper presentation]. 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15) (pp. 43-49). <https://doi.org/10.1145/2808128.2808133>
- Chakraborty, S., & Nisha, T. N. (2022). Next generation proactive cyber threat hunting - a complete framework. AIP Conference Proceedings, 2519(1), 030093. <https://doi.org/10.1063/5.0109674>
- Chaudhary, M., & Bansal, D. (2022). Open source intelligence extraction for terrorism-related information: A review. *WIREs Data Mining and Knowledge Discovery*, 12(5):e1473. <https://doi.org/10.1002/widm.1473>
- Day, T., Gibson, H., & Ramwell, S. (2017). Fusion of OSINT and Non-OSINT Data. In B. Akhgar, P. Bayerl, & F. Sampson (Eds.), *Open Source Intelligence Investigation* (pp. 133-152). Advanced Sciences and Technologies for Security Applications. Springer. https://doi.org/10.1007/978-3-319-47671-1_9
- Dekker, M., & Alevizos, L. (2023). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, 1-19. <https://doi.org/10.1002/spy2.333>
- Enache, G. I. (2022). Formulas for counteracting cyber threats in regards to computer products supply chains. *Proceedings of the International Conference on Business Excellence*, 16(1).
- George, A. S., George, A. S. H., & Baskar, T. (2023). Digitally immune systems: Building robust defences in the age of cyber threats. *Partners Universal International Innovation Journal*, 1(4), 155-172. <https://doi.org/10.5281/zenodo.8274514>
- González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), 4759. <https://doi.org/10.3390/s21144759> Top of Form
- Hyslip, T. S., & Burruss, G. W. (2023). 5. Ransomware. *Handbook on Crime and Technology*, 86.
- Ilca, L. F., Lucian, O. P., & Balan, T. C. (2023). Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response. *Sensors*, 23(15):6757. <https://doi.org/10.3390/s23156757>
- Jones, K. (2004). Mission drift in qualitative research, or moving toward a systematic review of qualitative studies, moving back to a more systematic narrative review. *Qualitative Report*, 9(1), 95-112.
- Kant, N., & Amrita. (2022). How cyber threat intelligence (CTI) ensures cyber resilience using artificial intelligence and machine learning. In *Methods, implementation, and application of cyber security intelligence and analytics* (p. 32). IGI Global. <https://doi.org/10.4018/978-1-6684-3991-3.ch005>
- Kausar, S., Leghari, A. R., & Iftikhar, E. (2023). Analysis of the cyber security challenges and solutions. *Journal of Positive School Psychology*, 7(1), 163-171.
- Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, 6(8), 1-21.
- Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). inTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics*, 10(7):818. <https://doi.org/10.3390/electronics10070818>
- Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, 32(1), 35-51. <https://doi.org/10.1080/0960085X.2022.2088414>
- Lanz, Z. (2022). Risk in U.S. critical infrastructure: An analysis of publicly available U.S. government alerts and advisories. *International Journal of Intelligence & Cybercrime*, 5(1), 43-70. <https://doi.org/10.52306/FWOZ7041>
- Leite, C., den Hartog, J., Ricardo dos Santos, D., & Costante, E. (2022). Actionable cyber threat intelligence for automated incident response. In H. P. Reiser & M. Kyas (Eds.), *Secure IT Systems. NordSec 2022* (Vol. 13700, pp. 323-339). Springer, Cham. https://doi.org/10.1007/978-3-031-22295-5_20
- Leszczyna, R., & Wróbel, M. R. (2019). Threat intelligence platform for the energy sector. *Software: Practice and Experience*, 49(8), 1225-1254. <https://doi.org/10.1002/spe.2705>
- Möller, D. P. F. (2023). Ransomwareattacks and scenarios: Cost factors and loss of reputation. In: *Guide to in Digital Transformation* (pp. 00-00). *Advances in Information Security*, vol. 103. Springer, Cham. https://doi.org/10.1007/978-3-031-26845-8_6
- Mughal, A. A. (2022). Building and securing the modern security operations center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, 5(1), 1-15. <https://research.tensorgate.org/index.php/IJBIBDA/article/view/21>

- Myrsalieva, A., Abdrakhmanova, E., Suiunduk uulu, D., & Moldomyrzaev, M. (2026). The role of cyberattacks in political and economic stability: Transforming national and international approaches. *Law, State and Telecommunications Review*, 18(2), 355–385. <https://doi.org/10.26512/lstr.v18i2.59089>
- Pai, Y., & Prasad, K. (2021). Open source intelligence and its applications in next generation cyber security - a literature review. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 5(2):1. <https://www.srinivaspublication.com>
- Potz, T. (2021). *The increasing importance of OSINT as a source of intelligence* [Master's thesis, University of Zagreb, Faculty of Political Science]. Croatian Digital Theses Repository. <https://urn.nsk.hr/urn:nbn:hr:114:806851>
- Rizvi, I., Raj, S., & Singh, V. (2025). Cybersecurity in the digital age. In L. O. Yesufu & P. N. E. Nohuddin (Eds.), *Technology for societal transformation*. Springer. https://doi.org/10.1007/978-981-96-1721-0_8
- Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational resilience. *Sensors*, 23(16):7273. <https://doi.org/10.3390/s23167273>
- Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors*, 25(14), 4272. <https://doi.org/10.3390/s25144272>
- Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, 23(4), 2525-2556. <https://doi.org/10.1109/COMST.2021.3117338>
- Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks? Undermining public confidence in government. *Journal of Information Technology & Politics*, 20(4), 359-374. <https://doi.org/10.1080/19331681.2022.2112796>
- Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the cyberthreat-intelligence (CTI) capability? *Computers & Security*, 92:101761. <https://doi.org/10.1016/j.cose.2020.101761>
- Siddaway, A. P., Wood, A. M., & Hedges, L. V. (2019). How to do a systematic review: A best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. *Annual Review of Psychology*, 70, 747-770. <https://doi.org/10.1146/annurev-psych-010418-102803>
- Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials*, 25(3), 1748-1774. <https://doi.org/10.1109/COMST.2023.3273282>
- Torres, M. A. A. E. E., Guerrero, F. T., & Budgud, A. T. (2022). *Data-driven cyber threat intelligence: A survey of Mexican territory* [Paper presentation]. 2nd EAI International Conference on Smart Technology (pp. 89-110), EAI/Springer Innovations in Communication and Computing. https://doi.org/10.1007/978-3-030-97913-8_7
- Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72, 212-233. <https://doi.org/10.1016/j.cose.2017.09.001>