Generative AI in Cybersecurity: A Systematic and Netnographic Review of Opportunities, Threats, and Challenges

Emmanuel Anti[1], Pius Ewoh[1]

[1]University of Vaasa, Wolffintie 34, 65200 Vaasa, Finland

Abstract

This research examines the opportunities, threats, and challenges of applying Generative AI (GenAI) in cybersecurity through a comprehensive Systematic Literature Review (SLR) and Netnography. This study expands the existing literature by analyzing how GenAI can facilitate the creation of AI-driven defenses against AI-generated threats, augment human-AI collaboration in security operations, advocate for the ethical and transparent use of AI, and enhance access to sophisticated tools for smaller organizations. The findings underscore GenAI's dual influence, providing robust capabilities for threat identification and automation but simultaneously facilitating more advanced cyberattacks and eliciting concerns over bias, supervision, and skill erosion. This study enhances the understanding of GenAI's transformative impact on cybersecurity practices by integrating academic research with real-time community feedback, while also outlining the practical and ethical implications of its adoption. The study provides timely insight into leveraging GenAI's potential while mitigating its risks, thus significantly advancing cybersecurity and AI governance research.

Keywords

Generative AI, Cybersecurity, Opportunities, Threats, Challenges, Literature review, Netnography

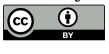
1. Introduction

Generative AI (GenAI), a subset of artificial intelligence, utilizes deep neural networks to create human-like content in response to complex and varied prompts [1, 2]. GenAI can be applied across various domains, and currently, it is transforming multiple industries, including content creation, virtual assistants, personalized education, digital art, business process management, market research, and human-computer interaction [2]. As various industries continue to embrace AI technologies for enhancing processes, increasing efficiency, and driving innovation [1], GenAI stands out for its ability to adapt and evolve solutions in a dynamic and ever-changing environment [3]. Further, Santos Gabriel [3] explains that GenAI's rapid insights enable businesses to adapt quickly to external changes, enhance communication, and manage customer complaints, thereby maintaining a competitive edge.

In cybersecurity, GenAI can potentially enhance threat detection by generating a wide range of threat scenarios, identifying abnormal system behavior, decrypting passwords, detecting phishing attempts and malware, and automating security responses [4]. In addition, Sai et al. [4] explain that GenAI can be applied in cybersecurity to simulate IoT system attack scenarios, thereby identifying vulnerabilities and enhancing security strategies. This is achieved by creating realistic network topologies and traffic patterns for hands-on cybersecurity training. According to Golda et al. [5], tools and platforms that can aid in cybersecurity using generative AI include deepfake detection tools, anomaly detection systems, automated incident response systems, and generative adversarial networks for intrusion detection. The application of GenAI in cybersecurity can offer several benefits, but it also encounters challenges like inadequate training data, adversarial attacks, and complex maintenance demands [5]. Further, inadequate data can lead to ineffective controls, while adversarial machine learning can exploit models, evading AI-enabled malware and intrusion detection controls [4, 5, 6].

Despite growing interest in GenAI's role in cybersecurity, there is limited clarity on its practical opportunities, emerging threats, and implementation challenges, requiring further study to mitigate

8th Conference on Technology Ethics (TETHICS2025), November 11–12, 2025, Vaasa, Finland



uncertainties and enhance strategies. These include ethical implications, long-term effects, adoption challenges, cost inefficiency, regulatory issues, skills gaps, and compatibility issues with existing systems [7]. Responsible GenAI use in cybersecurity requires understanding its ethical implications, long-term effects, adoption challenges, regulatory concerns, and system compatibility to ensure seamless integration and enhanced security. This research explores GenAI's opportunities, threats, and challenges in cybersecurity, while offering practical and theoretical contributions to the field. The research question for this study is: *What are the opportunities, threats, and challenges of using GenAI for cybersecurity?*

As AI evolves and digital reliance deepens, cybersecurity faces a decisive turning point that will determine how effectively societies can safeguard their digital future. The use of generative AI as both a tool for protection and a vector for attack demands a critical assessment. Understanding the opportunities, threats, and ongoing challenges is crucial for guiding future research and practice. Therefore, this study aims to review the current literature and online discourse surrounding generative AI in cybersecurity through both a Systematic Literature Review (SLR) and a netnographic lens.

2. Background Literature

Artificial Intelligence (AI) has become an essential technological advancement, driving innovation across various sectors, including healthcare, manufacturing, and cybersecurity. It involves the development of intelligent systems designed to mimic human cognition in decision-making and problem-solving [8, 9]. Deep learning, a critical subfield of AI, uses artificial neural networks to process large datasets and perform complex pattern recognition and decision-making tasks [10]. One of the most transformative deep learning applications is Generative Artificial Intelligence (GenAI), which automates the interpretation, prediction, and transformation of unstructured data into meaningful insights [10]. GenAI refers to applications built on advanced models such as Large Language Models (LLMs), exemplified by systems like ChatGPT. It often draws on techniques from the broader field of Natural Language Processing (NLP), but focuses on generating human-like content with minimal human input. These systems can enhance cybersecurity by improving threat detection, vulnerability assessment, and automated incident response [11, 12]. Cybersecurity tools such as Splunk and DarkTrace also integrate GenAI to identify anomalies, optimize security frameworks, and reinforce defensive strategies against cyberattacks [13]. The ability of GenAI to process and analyze vast amounts of security data in real time makes it an indispensable tool for digital security.

Despite its potential, GenAI also introduces new security risks and ethical challenges. Recent literature has documented increased AI-driven cyberattacks, including adversarial machine learning, backdoor poisoning, and automated phishing [14]. The emergence of deepfake social engineering attacks has further complicated cybersecurity efforts, allowing cybercriminals to manipulate data, forge identities, and deceive security protocols [15]. GenAI raises concerns regarding privacy, bias, and regulatory compliance, as its applications require vast amounts of sensitive data, making it a target for cyber threats [10]. Addressing its vulnerabilities is crucial as organizations increasingly integrate GenAI into their cybersecurity frameworks. Scholars have highlighted the importance of developing robust AI governance models to ensure AI-powered systems' ethical and secure use [16]. Some studies propose a co-creation approach, where AI security is integrated from the initial stages of development, ensuring transparency, fairness, and human oversight [17]. Researchers also emphasize the need for regulatory frameworks to monitor AI-driven cybersecurity strategies, advocating for compliance measures that balance technological innovation with risk mitigation [18].

Another significant concern in the literature is the interpretability and reliability of GenAI models in cybersecurity applications. While GenAI can significantly enhance cybersecurity operations, it also struggles with generalizability, adversarial robustness, and ethical decision-making [19]. Some scholars argue that AI security models must be continuously trained and fine-tuned to ensure they adapt to evolving cyber threats [20]. Others highlight the risk of AI-generated misinformation and manipulation, stressing the necessity of human-AI collaboration to improve decision accuracy and prevent security breaches [21]. Further, the literature also explores GenAI's role in offensive and defensive cybersecurity

measures. While some researchers have examined how GenAI enhances cybersecurity by detecting anomalies, preventing intrusions, and automating security protocols, others caution against its potential misuse by threat actors who leverage AI to bypass security measures [10, 13]. The dual-use nature of AI poses a paradox in cybersecurity, necessitating further research on AI adversarial defenses, red-blue teaming strategies, and AI-driven risk assessment models [19].

Given the increasing reliance on GenAI in cybersecurity, research remains fragmented on how organizations can integrate AI-powered security systems while minimizing ethical, privacy, and regulatory risks. Some scholars advocate for multi-layered cybersecurity frameworks that incorporate AI-powered threat intelligence and attack simulations to counter cyber threats proactively [20]. Others argue that AI security models should be designed with interpretability and transparency, ensuring accountability in automated decision-making [16].

Even with ongoing advancements, there remains a significant need for further research on the impact of GenAI in cybersecurity. Literature underscores the challenges associated with AI bias, adversarial attacks, and regulatory ambiguities, reinforcing the need for comprehensive AI governance policies [10, 18]. Future studies should focus on developing advanced AI security protocols, enhancing AI adversarial defenses, and exploring ethical AI deployment models to bridge existing knowledge gaps. As AI continues to evolve, integrating responsible AI practices, continuous model training, and ethical oversight will be critical in ensuring GenAI's secure and sustainable application in cybersecurity.

3. Methodology

We employed a two-fold review process combining a Systematic Literature Review (SLR) and Netnography to address our research question. The SLR followed the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines [22], which involve systematically identifying, screening, selecting, and synthesizing relevant peer-reviewed studies. Watson and Webster [23] highlight the importance of literature reviews in academic research, emphasizing that reviewing prior, relevant literature is fundamental to any scholarly project. Schryen [24] further argues that literature reviews critically assess and synthesize existing knowledge, enabling scholars to uncover weaknesses, challenge theoretical assumptions, and build upon prior research rather than duplicate efforts.

Additionally, Netnography, which adapts ethnographic techniques to study cultures and communities through computer-mediated communications and online interactions [25, 26], enables researchers to analyze digital communities, social behaviors, online discourse, and fluid cultural and technological landscapes of online environments [26]. Further, Netnography is a naturalistic and unobtrusive qualitative method that integrates multiple data sources, including interviews, data scraping, and online observation, to analyze social practices and naturally occurring interactions in digital environments [26, 27].

Applying both SLR and netnography provided a comprehensive view of the GenAI–cybersecurity landscape, combining academic rigor with industry relevance. The SLR offered structured, peer-reviewed insights into conceptual frameworks and theoretical implications. At the same time, netnography captured real-time, practitioner-driven concerns, emerging trends, and practical applications from online discussions, industry reports, and expert commentary. This contrast highlighted that academia and industry often work in parallel with little real collaboration or exchange. By integrating these perspectives, the study bridged the gap between systematic academic research and fast-moving industry insights, producing a more balanced and relevant understanding of GenAI's opportunities and risks in cybersecurity.

3.1. Review Process

The SLR focused on peer-reviewed academic research, while the Netnography approach analyzed online articles, industry reports, and expert discussions to capture real-time insights on GenAI in cybersecurity. We conducted a structured database search using predefined search strings to identify relevant literature. The search strategy was designed to cover academic literature and industry-relevant discussions across multiple data sources. To ensure relevance and rigor, we established the following inclusion criteria for

selecting studies, which comprised studies published from 2018 to 2025 to focus on recent advancements in GenAI and cybersecurity, peer-reviewed journal articles, articles written in English, conference papers, industry reports, expert discussions, and studies discussing GenAI applications, threats, and governance in cybersecurity. We excluded studies older than 2018 unless they provide foundational insights, articles not written in English, and studies unrelated to AI in cybersecurity, such as general AI ethics without a cybersecurity focus.

The timeline of 2018 to 2025 was selected to capture the critical phase of generative AI's integration into cybersecurity workflows and public consciousness, especially following the release of prominent models such as GPT-3 (2020), ChatGPT (2022), and GPT-4 (2023). The five-year range ensures the inclusion of both early-stage and mature discussions.

We searched academic databases, including IEEE Xplore, Elsevier, and Scopus. We further identified industry and online sources such as cybersecurity blogs, government reports, AI research repositories, and expert discussions from platforms like the World Economic Forum, ZDNET, The Verge, Quora, and WIRED (see Appendix A). The search string we devised to find relevant academic articles included the keywords listed in Table 1.

Table 1
Databases and search strings

Database	Search String
IEEE Xplore	("Generative AI") AND ("Cybersecurity")
Scopus	("Generative AI") AND ("Cybersecurity")

3.2. Screening and Selection Process

We identified and screened 543 peer-reviewed articles through the Systematic Literature Review (SLR) and 50 online sources through Netnography. This approach ensured a comprehensive analysis by integrating academic research and real-world insights from online sources.

3.2.1. Screening and Selection for the SLR

The SLR began with a title and abstract review to determine whether studies met our inclusion criteria, including topic relevance, language, and publication year. Specifically, we focused on keywords such as GenAI, Artificial Intelligence, and Cybersecurity to assess alignment with our research objectives. However, many studies were excluded as they lacked direct relevance to GenAI in cybersecurity or focused solely on traditional AI models without discussing generative models. Next, we conducted a full-text review to assess the eligibility of each study and remove duplicate entries. Following this rigorous selection process, we concluded on 58 articles that provided substantial contributions to understanding the role of GenAI in cybersecurity, including its opportunities, threats, and challenges. Figure 1 describes the screening process for the SLR.

3.2.2. Screening and Selection for the Netnographic Analysis

To complement the academic literature, we incorporated netnography to analyze real-world applications, expert discussions, and emerging trends related to GenAI in cybersecurity. This involved reviewing industry reports, cybersecurity blogs, discussion forums, and expert analyses from the World Economic Forum, ZDNET, The Verge, Quora, and WIRED. Relevant content was identified using targeted keywords (e.g., "Generative AI," "Artificial Intelligence," "Cybersecurity") and evaluated against the research objectives. We employed the screening criteria outlined in Table 2 to ensure the credibility of online sources. We initially identified 50 online sources, and after applying our eligibility and screening criteria we excluded 27 sources.

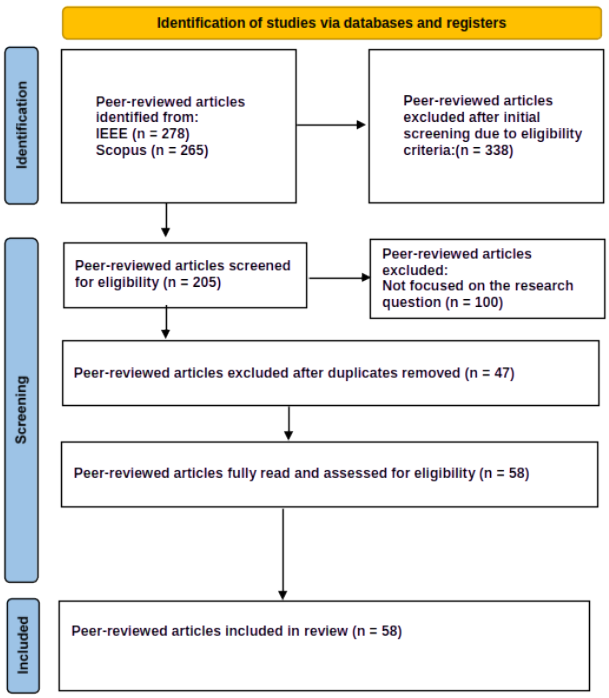


Figure 1: PRISMA flow chart diagram

Table 2
Criteria for online sources

Screening Criteria	Description
Relevance	Articles had to address GenAI applications in cybersecurity.
Source Credibility	We prioritized recognized industry sources, cybersecurity research organizations, and expert-authored content.
Recency	Only articles published within the last five years were considered to reflect the latest developments.
Practical and Industry Insights	We analyzed expert opinions to understand GenAI's real-world applications and evolving security risks.

Through this process, we selected 23 online sources (see Appendix A), supplementing the 58 peer-reviewed academic articles from the SLR. These sources provided a holistic perspective, integrating scholarly insights and industry-driven expertise. The selection process is illustrated in Figure 2.

4. Findings

Themes were identified through inductive thematic analysis of the selected literature and online data, revealing eight key themes related to the opportunities, threats, and challenges of generative AI in cybersecurity, as summarized in Table 3.

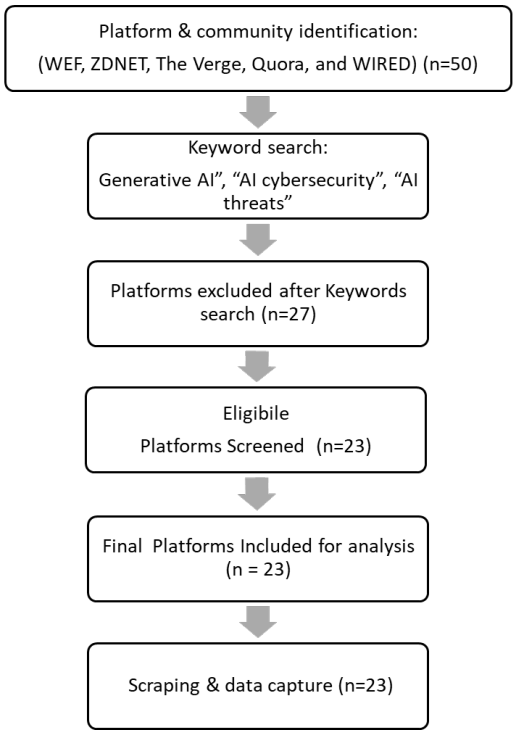


Figure 2: Netnographic analysis diagram

Table 3: Opportunities, threats, and challenges of GenAI in cybersecurity

Theme	Opportunities	Threats	Challenges
Efficiency and Productivity	Automates routine tasks, freeing up cybersecurity teams for strategic work [10, 13, 16, 19, 28, 29, 30, 31, 14].	The risk of over-dependence on GenAI reduces human judgment skills [10, 16, 32].	Balancing GenAI's automated responses with human oversight to ensure appropriate action in nuanced scenarios [16, 17, 21, 33].
Threat Detection and Analysis	Enhances threat detection by identifying patterns in data, correlating signals, and detecting anomalies [5, 13, 19, 21, 30, 31, 14, 34, 35, 36, 37].	Attackers can use GenAI to refine and scale their attacks, making them harder to detect and mitigate [5, 19, 31, 14, 35, 37, 38, 39].	Maintaining model accuracy and avoiding false positives to ensure genuine threats are not missed or ignored by overwhelmed security teams [36, 40].
Skills Development	Provides low-level support, enabling junior staff to focus on high-priority tasks [41, 42].	The risk of a growing skills gap arises from over-reliance on GenAI, leading to a loss of cybersecurity expertise [10, 16].	Upskilling cybersecurity professionals to effectively use GenAI while ensuring the retention of critical cybersecurity and threat detection knowledge [16, 19, 29, 30, 41].

Theme	Opportunities	Threats	Challenges
Data Privacy and Integrity	Offers secure data handling with built-in privacy features, enhancing data security [5, 10, 36].	Vulnerability to data poisoning, where adversarial actors may corrupt training data to undermine threat detection capabilities [10, 13, 17, 19, 21, 28, 14, 33, 37, 38].	Ensuring data used in GenAI models is clean, unbiased, and secure, protecting against adversarial manipulation [5, 10, 13, 16, 19, 21, 33, 36].
Cyber Defense and Resilience	Improves resilience by predicting potential threats and enabling proactive countermeasures [5, 13, 19, 20, 21, 30, 14, 37, 40, 43].	GenAI systems can be targeted with adversarial attacks, leading to compromised defenses and potentially disastrous consequences [19, 21, 14, 37, 38].	Designing robust GenAI systems that can withstand adversarial threats and adapt to evolving cybersecurity risks [20, 36].
Transparency and Explainability	Designing robust AI systems that can withstand adversarial threats and adapt to evolving cybersecurity risks [20, 31].	Lack of transparency can lead to mistrust and hinder the adoption of GenAI-powered solutions in cybersecurity [5, 44, 45].	Ensuring GenAI solutions in cybersecurity offer explainable outputs, enabling security teams to trust and effectively utilize AI-generated insights [5, 10, 17, 21].
Innovation and Adaptability	Supports dynamic responses by adapting to evolving cyber threats, providing a flexible, machine-scale approach to defense [5, 13, 19, 20, 37, 40].	Threat actors also use GenAI to innovate and develop sophisticated new attack vectors, intensifying the cyber arms race [13, 19, 33, 39, 45].	Continuously updating AI systems to adapt to new types of threats while balancing stability and innovation in security protocols [13, 19, 20, 21, 31, 37, 40].
Ethical and Regulatory Compliance	GenAI can support regulatory compliance by generating reports, aiding documentation, and flagging compliance issues [5, 17, 20, 21, 33, 36, 40, 45, 46].	Potential for misuse in creating sophisticated phishing and social engineering attacks, posing ethical concerns [5, 10, 13, 17, 21, 31, 14, 37, 38, 39, 45, 47].	Navigating regulatory frameworks and ethical considerations, ensuring AI's use in cybersecurity is responsible and aligns with legal standards [5, 13, 17, 19, 21, 33, 37, 42, 45, 47].

Our findings indicate that GenAI possesses transformative potential for strengthening the cybersecurity of organizations' critical infrastructure, while simultaneously introducing significant threats and challenges. Although it offers advancements in efficiency, threat detection, cyber defense, and innovation, its implementation also raises ethical, regulatory, and security concerns that require careful mitigation. Integrating human expertise remains crucial to mitigating risks associated with data privacy, adversarial attacks, and transparency. Additionally, the rapid evolution of GenAI necessitates continuous adaptation and regulatory oversight to ensure responsible implementation. These insights contribute to an evolving discourse on leveraging GenAI for cybersecurity while proactively managing its risks, shaping future research, and policy development.

Furthermore, our findings indicate that challenges can lead to innovations when GenAI technology

is properly managed. Additionally, the opportunities for utilizing GenAI technology are limited. A more effective partnership with stakeholders is likely to lead to a new revolution, resulting in improved precision and the discovery of innovative approaches to cybersecurity and design using GenAI.

5. Discussion

Our study contributes to the growing body of research on the evolution and application of GenAI in cybersecurity, highlighting its transformative potential and associated risks. The findings reveal that while GenAI enhances efficiency, threat detection, cyber defense, and innovation, it also introduces ethical, regulatory, and security challenges that require careful management. By integrating insights from academic literature and real-world industry perspectives, our study explores the implications of GenAI adoption in cybersecurity, highlighting the need for responsible implementation, continuous adaptation, and regulatory oversight to address emerging threats and challenges while maximizing its potential benefits. This highlights the dual nature of GenAI, presenting both substantial opportunities and inherent risks, with the advantages ultimately outweighing the challenges.

GenAI enhances decision-making, data synthesis, and communication within autonomous systems while supporting predictive maintenance, anomaly detection, and adaptive threat response, which are key to cybersecurity efficiency [48]. By automating routine tasks, GenAI frees cybersecurity teams to focus on strategic decision-making, threat analysis, and high-level planning [49]. Further, LLMs and advanced models enhance intrusion detection, risk assessment, and cyber-attack strategy development, streamlining operations and improving overall efficiency and effectiveness in cybersecurity [49]. While GenAI may enhance productivity through task automation, it does not possess the innate human abilities to think critically, creatively, or solve problems in novel ways. Instead, it is a valuable aid that augments human capabilities [50], as these human skills involve understanding context, emotions, and ethical considerations that exceed the current capabilities of GenAI [49]. However, over-reliance on automation may weaken human judgment, making skilled oversight essential to ensure ethical use, contextual understanding, and balanced decision-making in complex security scenarios [48, 50].

Threat detection, according to Vadisetty and Polamarasetti [51], can be enhanced by GenAI by identifying patterns in data, correlating signals, and detecting anomalies with greater accuracy, significantly improving cybersecurity defenses. Further, Mavikumbure et al. [19] explain that by creating baseline profiles of normal network behavior, GenAI can flag deviations as potential intrusions, refining intrusion detection systems (IDS) by reducing false positives and improving response time. Additionally, GenAI accelerates incident response by analyzing vast amounts of log files and network traffic, automating threat identification, and countering evolving cyber threats [19, 51]. However, Gupta et al. [13] argue that attackers can exploit GenAI to refine and scale attacks, making them more evasive and harder to detect by automating social engineering, phishing campaigns, malware generation, and attack payloads, thereby increasing the sophistication of cyber threats. This suggests that malicious actors (insiders or external) can develop AI models to automate hacking procedures, identify vulnerabilities, and execute exploitation strategies, posing a substantial cybersecurity risk. The dual-use capabilities of GenAI necessitate robust countermeasures to prevent AI-driven security advancements from being exploited by adversaries. This includes stringent content filtering, enhanced security measures, and responsible AI governance to mitigate the risks posed by malicious actors. The dual-use nature of GenAI demands robust countermeasures, including stringent content filtering, enhanced security measures, and responsible AI governance, to prevent its exploitation for phishing attacks, malware generation, and other cyber threats [13, 51]. Additionally, ethical frameworks and industry-wide regulations are essential to mitigate risks and prevent the weaponization of GenAI technologies [51].

Regarding skills development, GenAI offers low-level support that allows junior staff to take on more complex responsibilities, particularly in cybersecurity, where advances in large language models have enabled less-skilled individuals to create sophisticated malware through prompt engineering, significantly expanding the pool of potential cyber threat actors [52]. While this has the potential to accelerate learning, there is a real concern that over-reliance on GenAI could lead to a skills gap through

the automation of complex tasks that traditionally require significant expertise [52, 53]. Upskilling in cybersecurity should combine the use of GenAI for personalized learning with comprehensive training that fosters foundational knowledge, soft skills, and a lifelong learning mindset tailored to individual needs [53].

In the area of data privacy and integrity, GenAI's built-in privacy features, combined with models like Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) integrated with traditional and deep learning-based anomaly detection, can enhance secure data handling, improve threat detection, and enable the generation of privacy-preserving synthetic datasets—especially valuable when real data are scarce or sensitive [54]. However, GenAI models are vulnerable to data poisoning, where compromised training data can lead to high-quality but misleading outputs that closely resemble clean responses, making it difficult to detect false information [55]. Therefore, protecting training datasets from adversarial manipulation is crucial, as attacks like model poisoning can inject malicious data that biases outputs or degrades performance, threatening the integrity, safety, and reliability of AI-generated media and risking security and privacy violations [56].

GenAI strengthens cyber defense by analyzing large data volumes to detect anomalies, predict and identify emerging threats in real time, automate threat intelligence, and support proactive, adaptive security strategies [40, 57]. AI systems become integral to organizational infrastructures, including cybersecurity, as they expand the attack surface and must be secured, protecting their data, models, and the underlying infrastructure to prevent exploitation by malicious actors [57]. Adversarial attacks on GenAI models, such as input manipulation and data poisoning, can compromise cybersecurity defenses by deceiving systems or corrupting training data, thereby undermining the integrity of these models. In contrast, adversarial learning techniques are being developed to bolster model robustness and ensure reliable threat prediction in real-world scenarios [58]. A key challenge is designing resilient systems that can withstand and adapt to such threats [59].

Transparency and explainability remain central to fostering trust in GenAI-powered solutions, as the complex, "black box" nature of AI systems can obscure decision-making and undermine accountability, making it crucial to strike a balance that promotes understanding without compromising trust [60]. Ensuring the interpretability and trustworthiness of AI models is vital for effective cybersecurity, as it enables the validation of predictions, assessment of resilience to threats, and builds confidence in AI-driven decisions, which is key to broader adoption and reliable use in complex operational environments [61].

GenAI fuels innovation and adaptability in cybersecurity by enabling dynamic responses to emerging threats, training on real-time data to generate proactive threat-hunting queries, detecting advanced phishing attacks, scanning for malicious activity, and automating responses, surpassing the limitations of static systems [4]. However, GenAI's dual-use nature escalates the cyber arms race, as it empowers both defenders by simulating threats and generating training data and attackers, who can craft inputs to evade detection, demanding a more proactive and responsive security approach to counter emerging risks [62]. As generative AI evolves, continuous updates are essential. Still, they must be balanced with system stability and adherence to ethical and regulatory standards to ensure robust security against vulnerabilities, privacy breaches, jailbreaking, and prompt injection [63]. GenAI can enhance cybersecurity compliance by automating documentation and risk identification [63, 64]. However, while governance frameworks are vital for ensuring responsible and ethical use of GenAI within organizations, they cannot prevent malicious misuse such as AI-driven phishing or social engineering, which instead require dedicated defensive strategies like real-time AI-based threat detection [65].

5.1. Research Gaps and Recommendations

Our study identified additional areas of research that we recommend for further studies.

As GenAI enables low-skill actors to launch sophisticated attacks, future research must prioritize developing AI-powered systems to detect and counter AI-generated threats like phishing, malware, and ransomware while studying how adversaries innovate with GenAI to build adaptive, evolving defenses.

Future research should explore how GenAI can augment rather than replace cybersecurity profession-

als by optimizing human-AI workflows, enhancing training and skill retention, and ensuring automation is balanced with human oversight in critical decision-making.

Further research should focus on mitigating bias in GenAI models, developing transparent and auditable systems, and establishing ethical and legal frameworks to ensure trustworthy and responsible AI use in cybersecurity.

Future research should focus on developing affordable, accessible GenAI tools and shared cybersecurity models for smaller organizations, ensuring strong security without high resource demands to strengthen overall ecosystem resilience.

6. Limitations

This study, combining an SLR and Netnography to examine the opportunities, threats, and challenges of using GenAI in cybersecurity, proved to be a valuable tool for synthesizing the existing body of knowledge. However, it is essential to acknowledge that certain limitations can affect the scope, depth, and applicability of the findings associated with our review.

Since our study partly relied on academic and peer-reviewed publications, there is often a delay between when research is conducted and when it is published. In the context of a rapidly evolving field like GenAI, this time lag can result in findings that may fail to capture the latest developments. Further, while Netnography addresses this gap by analyzing current discussions in online communities, it may lack the technical rigor and depth found in formal research publications.

Additionally, netnography, conversely, is based on user-generated content from specific online forums or platforms, which may not represent the broader cybersecurity or AI community. The views expressed in these communities can be skewed or influenced by platform-specific cultures and norms.

Furthermore, both SLR and Netnography are primarily qualitative and descriptive. They can offer rich narratives and thematic insights, but lack empirical testing. As a result, findings may not be generalizable to real-world cybersecurity environments or suitable for drawing causal inferences about the effectiveness or risks of GenAI applications.

Contextual and cultural limitations also come into play, particularly with Netnography. Online discourse is often shaped by its participants' artistic and regional backgrounds. What is discussed, how it is framed, and which issues are prioritized may vary significantly across communities. Consequently, insights drawn from netnographic analysis may not be universally applicable or reflective of global trends.

Lastly, the dynamic nature of cybersecurity threats makes both SLR and Netnography vulnerable to becoming quickly outdated. Cyber threat landscapes change rapidly, and attackers continuously develop new tactics. When literature is reviewed or online discourse is analyzed, emerging threats or novel uses of GenAI may evolve beyond what was captured in the study.

7. Conclusion

This study examined the opportunities, threats, and challenges of using GenAI in cybersecurity through an SLR and Netnography. The findings reveal that while GenAI enhances cybersecurity capabilities such as threat detection, automation, and workforce support, it also introduces significant risks. These include the rise of AI-generated attacks, over-reliance on automation, loss of human expertise, and ethical and legal concerns. GenAI enables more efficient operations and faster threat response, but it also lowers the barrier for attackers to create sophisticated phishing, malware, and ransomware. This dual impact underscores the need for balanced strategies that integrate GenAI with human oversight, continuous training, and robust ethical safeguards. Future research areas include building AI defenses against AI-generated threats, improving human-AI collaboration, addressing model bias and transparency, and developing accessible, cost-effective AI tools for smaller organizations. These directions are critical for ensuring GenAI strengthens rather than destabilizes cybersecurity efforts.

While the combined SLR and netnographic approach provided both structured analysis and real-time community perspectives, limitations such as publication lag and potential source bias should be noted. Despite these constraints, the study offers a strong foundation for guiding responsible and effective GenAI adoption in cybersecurity. Furthermore, we recommend that ethical governance of GenAI be a key focus for future research to help manage its associated risks. There is a clear need for a holistic framework that guides the responsible and secure use of GenAI in cybersecurity.

Declaration on Generative AI

During the preparation of this work, the authors utilized ChatGPT and Grammarly for grammar and spelling checks, sentence polishing, and rephrasing. After using ChatGPT and Grammarly, the authors reviewed and edited the content as needed, and take full responsibility for the publication's content.

References

[1] L. V. Huy, H. T. Nguyen, T. Vo-Thanh, N. H. T. Thinh, T. Thi Thu Dung, et al., Generative ai, why, how, and outcomes: A user adoption study, AIS Transactions on Human-Computer Interaction 16 (2024) 1–27.

[2] S. Feuerriegel, J. Hartmann, C. Janiesch, P. Zschech, Generative ai, Business & Information Systems Engineering 66 (2024) 111–126.

[3] V. S. Santos Gabriel, Generative ai: A literature review on business value, AMCIS 2024 Proceedings, Paper 27, 2024. URL: https://aisel.aisnet.org/amcis2024/ai_aa/ai_aa/27.

[4] S. Sai, U. Yashvardhan, V. Chamola, B. Sikdar, Generative ai for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space, IEEE Access (2024).

[5] A. Golda, et al., Privacy and security concerns in generative ai: A comprehensive survey, IEEE Access (2024).

[6] R. Sen, G. Heim, Q. Zhu, Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for MIS academics, Communications of the Association for Information Systems 51 (2022) 28.

[7] J. Chavan, C. Mankar, V. Patil, Opportunities in research for generative artificial intelligence (GenAI), challenges and future direction: A study, International Research Journal of Engineering and Technology 11 (2024) 446–451.

[8] IBM, What is artificial intelligence (AI)?, 2025. URL: https://www.ibm.com/think/topics/artificial-intelligence, [Accessed 16 February 2025].

[9] D. L. Poole, A. K. Mackworth, Artificial Intelligence: Foundations of Computational Agents, Cambridge University Press, 2010.

[10] N. Capodieci, C. Sanchez-Adames, J. Harris, U. Tatar, The impact of generative ai and LLMs on the cybersecurity profession, in: 2024 Systems and Information Engineering Design Symposium (SIEDS), IEEE, 2024, pp. 448–453.

[11] F. Kalota, A primer on generative artificial intelligence, Education Sciences 14 (2024) 172.

[12] A. Nguyen-Duc, et al., Generative artificial intelligence for software engineering—a research agenda, arXiv preprint arXiv:2310.18648 (2023).

[13] M. Gupta, C. Akiri, K. Aryal, E. Parker, L. Praharaj, From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy, IEEE Access (2023).

[14] A. N. Jaber, L. Fritsch, COVID-19 and global increases in cybersecurity attacks: review of possible adverse artificial intelligence attacks, in: 2021 25th International Computer Science and Engineering Conference (ICSEC), IEEE, 2021, pp. 434–442.

[15] A. Kumari, I. Sharma, Securing vulnerabilities: Fuzzer detection with machine learning classification, in: 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), IEEE, 2024, pp. 1–6.

[16] C. E. Whyte, Machine expertise in the loop: Artificial intelligence decision-making inputs and cyber conflict, in: 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), IEEE, 2022, pp. 135–154.
[17] N.-M. Aliman, L. Kester, Malicious design in AIVR, falsehood and cybersecurity-oriented immersive defenses, in: 2020 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), IEEE, 2020, pp. 130–137.
[18] K. Sjoberg, Artificial intelligence and vehicles [connected and automated vehicles], IEEE Vehicular Technology Magazine 19 (2024) 103–105.
[19] H. S. Mavikumbure, V. Cobilean, C. S. Wickramasinghe, D. Drake, M. Manic, Generative AI in cyber security of cyber physical systems: Benefits and threats, in: 2024 16th International Conference on Human System Interaction (HSI), IEEE, 2024, pp. 1–8.
[20] M. Maldonado, C. Johnson, M. Gulati, T. Jaspers, P. F. Roysdon, Advanced cyber deception framework (ACDF): A comprehensive study, in: 2024 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2024, pp. 203–208.
[21] L. A. Garcia-Segura, The role of artificial intelligence in preventing corporate crime, Journal of Economic Criminology 5 (2024) 100091.
[22] M. J. Page, et al., The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, International Journal of Surgery 88 (2021) 105906.
[23] R. T. Watson, J. Webster, Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0, Journal of Decision Systems 29 (2020) 129–147.
[24] G. Schryen, Writing qualitative IS literature reviews—guidelines for synthesis, interpretation, and guidance of research, Communications of the Association for Information Systems 37 (2015) 12.
[25] T. Anne-Marie, N. Chau, K. K. Kai, Ethical questions related to using netnography as research method, The ORBIT Journal 1 (2017) 1–11.
[26] M. Shahbazi, B. Tan, D. Bunker, Netnography for crisis management and information systems research, 2024.
[27] I. Jeacle, Navigating netnography: A guide for the accounting researcher, Financial Accountability & Management 37 (2021) 88–101.
[28] R. Holanda Filho, D. Colares, A methodology for risk management of generative AI based systems, in: 2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE, 2024, pp. 1–6.
[29] J. Dwight, Collaborate, design, and generate cybercrime script tabletop exercises for cybersecurity education, in: International Conference on Computers in Education, 2023.
[30] N. Shenoy, A. V. Mbaziira, An extended review: LLM prompt engineering in cyber defense, in: 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET), IEEE, 2024, pp. 1–6.
[31] K. Jabbarova, AI and cybersecurity-new threats and opportunities, Journal of Research Administration 5 (2023) 5955–5966.
[32] M. Loupasakis, G. Potamos, E. Stavrou, Revolutionizing social engineering awareness raising, education and training: generative AI-powered investigations in the maritime domain, in: International Conference on Human-Computer Interaction, Springer, 2024, pp. 70–83.
[33] P. Burgstaller, The use of AI and its legal boundaries in the EU, in: 2023 1st International Conference on Optimization Techniques for Learning (ICOTL), IEEE, 2023, pp. 1–5.
[34] M. A. Ferrag, et al., Revolutionizing cyber threat detection with large language models: A privacy-preserving BERT-based lightweight model for IoT/IoT devices, IEEE Access 12 (2024) 23733–23750.
[35] Y. Yoo, D. Na, S. Nathanson, Y. Cao, L. Watkins, Disinformation at scale: Detecting AI-human composite images via convolution ensembles, in: MILCOM 2024–2024 IEEE Military Communications Conference (MILCOM), IEEE, 2024, pp. 621–626.
[36] R. Wang, AI-powered predictive cybersecurity in identifying emerging threats through machine learning, in: 2024 IEEE 3rd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), IEEE, 2024, pp. 819–825.
[37] K. Kumar, B. Bhushan, et al., Augmenting cybersecurity and fraud detection using artificial

intelligence advancements, in: 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), IEEE, 2023, pp. 1207–1212.
[38] A. M. Shibli, M. M. A. Pritom, M. Gupta, AbuseGPT: Abuse of generative AI chatbots to create smishing campaigns, in: 2024 12th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2024, pp. 1–6.
[39] A. Gurtu, D. Lim, Use of artificial intelligence (AI) in cybersecurity, in: Computer and Information Security Handbook, Elsevier, 2025, pp. 1617–1624.
[40] V. R. Saddi, S. K. Gopal, A. S. Mohammed, S. Dhanasekaran, M. S. Naruka, Examine the role of generative AI in enhancing threat intelligence and cyber security measures, in: 2024 2nd International Conference on Disruptive Technologies (ICDT), IEEE, 2024, pp. 537–542.
[41] C. Koukou, E. Stavrou, The potential of generative AI chatbots as career advisors in cybersecurity: Professionals' perspectives, in: IFIP World Conference on Information Security Education, Springer, 2024, pp. 191–206.
[42] R. Nowrozy, GPTs or grim position threats? the potential impacts of large language models on non-managerial jobs and certifications in cybersecurity, in: Informatics, MDPI, 2024, p. 45.
[43] L. Peters, G. Gkoktsis, Generative AI and game theory for the development and deployment of honeypots to enhance the security of industrial automation and control systems, in: INFORMATIK 2024, Gesellschaft für Informatik eV, 2024, pp. 1905–1916.
[44] A. Patwardhan, V. Vaidya, A. Kundu, Automated consistency analysis of LLMs, in: 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), IEEE, 2024, pp. 118–127.
[45] E. Moyakine, T. van Ede, T. Mulder, Interdisciplinary research project "AI Shield,", 2024.
[46] B. Lodge, RAGe against the machine with BERT for proactive cybersecurity posture, in: 2024 IEEE International Conference on Big Data (BigData), IEEE, 2024, pp. 3579–3588.
[47] E. B. Blancaflor, R. M. Abaleta, L. M. D. Achacoso, A. C. C. Amper, P. I. R. Ampiloquio, Emerging threat: The use of AI voice cloning software and services to deceive victims through phone conversations and its potential effects on the filipino population, in: Proceeding of the 2024 5th Asia Service Sciences and Software Engineering Conference, 2024, pp. 137–146.
[48] Y. Usman, A. Upadhyay, P. Gyawali, R. Chataut, Is generative AI the next tactical cyber weapon for threat actors? unforeseen implications of AI generated cyber attacks, arXiv preprint arXiv:2408.12806 (2024).
[49] M. Andreoni, W. T. Lunardi, G. Lawton, S. Thakkar, Enhancing autonomous system security and resilience with generative AI: A comprehensive survey, IEEE Access (2024).
[50] R. S. Shah, The power of generative artificial intelligence: Revolutionizing cybersecurity, marketing, and creative industries, IEEE Potentials (2024).
[51] R. Vadisetty, A. Polamarasetti, Generative AI for cyber threat simulation and defense, in: 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA), IEEE, 2024, pp. 272–279.
[52] S. Metta, I. Chang, J. Parker, M. P. Roman, A. F. Ehuan, Generative AI in cybersecurity, arXiv preprint arXiv:2405.01674 (2024).
[53] C. Kallonas, A. Piki, E. Stavrou, Empowering professionals: a generative AI approach to personalized cybersecurity learning, in: 2024 IEEE Global Engineering Education Conference (EDUCON), IEEE, 2024, pp. 1–10.
[54] G. S. Nadella, et al., Generative AI-enhanced cybersecurity framework for enterprise data privacy management, Computers 14 (2025) 55.
[55] Z. L. Teo, C. Q. W. Ning, J. L. Y. Wong, D. Ting, Cybersecurity in the generative artificial intelligence era, Asia-Pacific Journal of Ophthalmology (2024) 100091.
[56] D. G. Takale, P. N. Mahalle, B. Sule, Cyber security challenges in generative AI technology, Journal of Network Security Computer Networks 10 (2024) 28–34.
[57] N. Vemuri, N. Thaneeru, V. M. Tatikonda, Adaptive generative AI for dynamic cybersecurity threat detection in enterprises, International Journal of Science and Research Archive 11 (2024) 2259–2265.

[58] S. Ankalaki, A. A. Rajesh, M. Pallavi, G. S. Hukkeri, T. Jan, G. R. Naik, Cyber attack prediction: From traditional machine learning to generative artificial intelligence, IEEE Access (2025).
[59] Y. Yigit, W. J. Buchanan, M. G. Tehrani, L. Maglaras, Review of generative AI methods in cybersecurity, arXiv preprint arXiv:2403.08701 (2024).
[60] L. Vaishnav, S. Singh, K. A. Cornell, Transparency, security, and workplace training & awareness in the age of generative AI, arXiv preprint arXiv:2501.10389 (2024).
[61] I. H. Sarker, H. Janicke, A. Mohsin, A. Gill, L. Maglaras, Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects, ICT Express (2024).
[62] A. O. Almagrabi, R. A. Khan, Optimizing secure AI lifecycle model management with innovative generative AI strategies, IEEE Access (2024).
[63] S. Wen, The power of generative AI in cybersecurity: Opportunities and challenges, Applied and Computational Engineering 48 (2024) 31–39.
[64] R. Changala, S. Kayalvili, M. Farooq, L. M. Rao, V. S. Rao, S. Muthuperumal, Using generative adversarial networks for anomaly detection in network traffic: Advancements in AI cybersecurity, in: 2024 International Conference on Data Science and Network Security (ICDSNS), IEEE, 2024, pp. 1–6.
[65] C. S. Veluru, Responsible artificial intelligence on large scale data to prevent misuse, unethical challenges and security breaches, Journal of Artificial Intelligence & Cloud Computing (2024) 2–6. SRC/JAICC-349.

A. Web Pages and Blogs

- Generative AI: opportunities, risks, and challenges | Epthinktank | European Parliament
- A CEO's guide to scaling the Generative AI Enterprise | Deloitte US
- A new arms race: cybersecurity and AI | World Economic Forum
- 3 key ways business leaders can adopt GenAI successfully | World Economic Forum
- Generative AI (Artificial Intelligence): Benefits and Challenges - Explained | ForumIAS Blog
- AI and cybersecurity: Navigating the risks and opportunities | World Economic Forum
- Discover this week's must-read cybersecurity news and stories | World Economic Forum
- Why cybersecurity is on the frontline of our AI future | World Economic Forum
- 4 ways data and AI tip the cybersecurity scales towards the defenders | World Economic Forum
- AI News & Artificial Intelligence | TechCrunch
- Generative AI adoption surpasses early PC and internet usage, study finds | VentureBeat
- Artificial Intelligence | The Verge
- What is AI? Here's everything you need to know about artificial intelligence | ZDNET
- Artificial Intelligence | WIRED
- The most innovative AI companies of 2024 | Fast Company
- What is AI? Artificial Intelligence Explained | TechTarget
- Artificial intelligence | MIT Technology Review
- How do you spot a deepfake? This is what the experts say | World Economic Forum
- The new AI imperative is balancing innovation and security | World Economic Forum
- What are some potential future applications of generative AI in offensive cyber operations? | Quora
- How can generative AI be used to fuel innovation while minimizing cyber threats? | Quora
- How can generative AI be used to fight against novel cyberattacks? | Quora