International Journal of Applied Science; Vol. 8, No. 2; 2025
ISSN 2576-7240 E-ISSN 2576-7259
https://doi.org/10.30560/ijas.v8n2p1

Generative AI (GAI) Use for Cybersecurity Resilience: A Scoping Literature Review

Jessica Parker[1]

[1] Marymount University, United States

Correspondence: Jessica Parker, Marymount University, Virginia, United States. E-mail: j0p80903@marymount.edu

Received: February 20, 2025; Accepted: March 7, 2025; Published: March 9, 2025

Abstract

With cyberattacks increasing in volume and number, organizations are increasingly at risk of adverse financial and reputational impacts. Cyber attackers are quick to implement technologies like Generative Artificial Intelligence (GAI) to enhance attacks, while organizations have yet to fully benefit from GAI to improve cybersecurity defenses. This scoping literature review analyzes current research and identifies gaps in the literature about how Generative Artificial Intelligence (GAI) can be used to enhance cybersecurity resilience. The analysis includes an overview of GAI, ethical considerations and challenges, future directions and research opportunities, and a discussion of how this GAI research can be applied.

Keywords: Artificial Intelligence (AI), cybersecurity, Generative Artificial Intelligence (GAI), information security

1. Introduction

In 2023, over 350 malicious intrusion attempts were made on organizations every second, representing a 6% increase over the prior year (SonicWall, 2024). Nearly 9 out of every 10 U.S. organizations are at risk of experiencing a cyberattack within a year that will result in significant financial loss (Petrosyan, 2024). For an organization that experiences a cyberattack, not only is there a financial cost from the remediation activities, but there is also an adverse impact on the organization's reputation (Huang et al., 2023; Juma'h & Alnsour, 2020; Makridis, 2021). Costs and impacts are considerable, especially in the case of a data breach or ransomware attack.

Recovering from a data breach can cost a U.S. organization an average of $9.44 million (Huang et al., 2023), with higher costs found in the healthcare industry (Seh et al., 2020). Consider that between 2002 and September 2023, there were over 17,500 data breaches in the United States (Privacy Rights Clearinghouse, 2023). Near the end of 2023, the massive National Public Data breach exposed data, including Social Security numbers, for almost 170 million people (Microsoft, 2024), representing about one out of every three people in the U.S. (US Census Bureau, 2024). By October 2024, National Public Data's parent company filed for bankruptcy as the company was unable to pay for the costs associated with the breach (Rundle & Nash, 2024). While data breaches impact organizations and individuals financially, other types of cyberattacks can have more devastating consequences.

Ransomware, a type of cyberattack where an organization's technology systems are rendered inoperable and data inaccessible, impedes an organization's ability to maintain operations (Lee, 2024). For hospitals, this has meant delays in care when patients in ambulances are routed to other facilities, postponements of tests and procedures (Lee, 2024), and a reduction in access to technology that provides live-saving monitoring and care – allegedly causing the death of a newborn (Poulsen et al., 2021). The 2021 attack on Colonial Pipeline forced the organization to close the largest gasoline pipeline in the U.S. (Eaton et al., 2021), resulting in gas shortages and price increases (Rust & Ruiz, 2021). Water utilities have also been victims of ransomware attacks, causing one town's water system to overflow (Miller, 2024) and raising concerns over the stability and security of municipal water supplies (Lee, 2024; Lyngaas, 2023; Shipkowski, 2024). Both data breaches and ransomware can have significant negative impacts on individual lives as well as on the organizations that experience them.

Cyber attackers use the latest Generative Artificial Intelligence (GAI) tools to improve the quality of their social engineering activities and scale up the volume of attacks within or across organizations (Google Cloud, 2023). The National Institute of Standards and Technology (2024) identified 12 risks that are unique to or made worse by GAI and provides over 200 recommended actions to mitigate those risks. Given the power of GAI tools to mitigate risk and detect attacks, almost 70% of organizations surveyed by PricewaterhouseCoopers (2023) expect to use

GAI to improve their cyber defenses but have yet to make the most of GAI's capabilities to strengthen cybersecurity (Mamgai, 2023). With more than 1 in 4 surveyed organizations impacted by a cyber incident within a recent 12-month period (World Economic Forum & Accenture, 2024), over 55% of respondents believed that GAI would be more advantageous to cyber attackers than to defenders over the next two years. To improve cybersecurity resilience, organizations need to understand how to benefit from the new capabilities of GAI, including better detection of potential threats and improved automated responses to incidents (Gupta et al., 2023; Sai et al., 2023). This research analyzes the literature to understand what is currently known so that leaders can make an informed assessment about the benefits of GAI to cybersecurity resilience based on defined business use cases at an organization.

2. Method

Recognizing that GAI is an evolving research topic, a scoping review was chosen to explore the existing literature about cybersecurity and GAI rather than a systematic or narrative (traditional literature) review. Scoping reviews are used to map currently available evidence, identify knowledge gaps, understand how research has been conducted, and clarify definitions and concepts about a topic (Munn et al., 2018; Peters et al., 2024; Stratton, 2019; Verdejo et al., 2021). Contrast this focus with systematic reviews, which are often used for hypothesis testing and analyzing existing data for well understood topics, and narrative reviews, which are unstructured and used to frame a research focus (Munn et al., 2018; Peters et al., 2020; Snyder, 2019; Stratton, 2019). The flexibility to include different types of methodologies (qualitative and quantitative) along with other peer-reviewed literature, like conference papers and editorials, provides a breadth of sources for emerging areas of research (Munn et al., 2018; Peters et al., 2024; Stratton, 2019; Verdejo et al., 2021). The following section will detail the structure of the scoping review, including the research question, inclusion criteria, exclusion criteria, search strategy, and results analysis.

2.1 Research Question

The following research question was used to focus the scoping review: *"How can organizations benefit from the new capabilities of GAI to improve cybersecurity resilience?"* This question is designed to explore the existing knowledge of the topic, the potential applications, and identify knowledge gaps.

2.2 Inclusion Criteria

Peer-reviewed, full-text articles in the English language were selected. Keywords were combinations of "cybersecurity" or "cyber security" with any one of the terms "generative artificial intelligence," "generative AI," "genAI," or "GAI," found in the title, abstract, or keywords. As ChatGPT is one of the commonly referenced GAI tools, a reference to ChatGPT or other GAI tools in the title, abstract, or keywords was considered a reference to GAI. There were no limitations on the publication date as GAI is a recent term.

2.3 Exclusion Criteria

Articles where the full text was unavailable, the source was not peer-reviewed, not in English, or either pre-publication or pre-print were excluded. Also excluded were results that contained no research information: messages from organizing committees, lists of committee members, title pages alone, back matter, publishing information, grant awards with abstracts, and author indexes. Results that did not have both cybersecurity and GAI topics referenced within the abstract were also excluded.

2.4 Search Strategy

The following databases were searched on September 7, 2024: Ebook Central, EBSCO, IEEE Computer Society, Google Scholar, ProQuest Central, ProQuest Dissertations & Theses Global, ProQuest Historical Newspapers: The New York Times, ProQuest Historical Newspapers: The Washington Post, and Science Direct. Duplicates were removed.

2.4 Results Analysis

The following databases were searched on September 7, 2024: Ebook Central, EBSCO, IEEE Computer Society, Across all databases, 99 unique articles were found, all of which were published in 2023 or 2024. Of the unique articles, 59 met the exclusion criteria. The 40 sources included in the scoping review and a summary of methods and theories used in those sources can be found in Table 1. From the included research, 23 papers used some form of literature review of existing research as the methodology, and six articles were commentary, interview, or discussion of the topic. All 29 of these sources lacked theoretical models or frameworks. The remaining 11 articles used qualitative and quantitative approaches to evaluate their research and were generally focused on technical models or comparison of tool performance. Just three papers included theoretical models or frameworks: Jüttner

et al. (2024) used the Plan-Do-Check-Act framework to describe the cybersecurity lifecycle, Kam et al. (2024) applied grounded theory to qualitative analysis of online posts, and Ssetimba et al. (2024) defined and applied three technical theories - machine learning theory, natural language processing theory, and GAI theory. While there were multiple papers describing how GAI can be used to augment an organization's cybersecurity (Aldasoro et al., 2024; Alwahedi et al., 2024; Andreoni et al., 2024; Dhoni & Kumar, 2023; Guo et al., 2024; Gupta et al., 2024; Mahboubi et al., 2024; Mavikumbure et al., 2024; Palani et al., 2024; Pasupuleti et al., 2023; Renaud et al., 2023; Saddi et al., 2024; Sai et al., 2024; Shahid & Imteaj, 2024; Szmurlo & Akhtar, 2024; Takale et al., 2024; Teo et al., 2024; Vemuri et al, 2024; Wang, 2024), there is a lack of information about how organizations are integrating GAI into cybersecurity defense and response in practice. The subsequent sections will provide an overview of GAI, ethical considerations, challenges and limitations, followed by future directions and research opportunities.

3. Overview of GAI

Often using content in the public domain, GAI is a subset of AI that analyzes and categorizes large amounts of information using deep learning (DL) and generative modeling techniques to create new content (Jovanovic & Campbell, 2022). DL is a type of machine learning where a computer uses multi-layered artificial neural networks to learn patterns and relationships from large amounts of data instead of by rules programmed into it (Russell & Norvig, 2022). Generative modeling describes the statistical technique used by a machine to create new data, like images and text, similar to existing data it has analyzed (Gupta et al., 2024; Jovanovic & Campbell, 2022). A strength of GAI is its ability to learn from vast amounts of data, which improves the accuracy of the results and enables the tool to provide human-like responses (Banko et al., 2002; Sai et al., 2023; Wang, 2024). GAI is a subset of AI that distinguishes itself in how it uses data to provide outputs.

GAI is distinct from other types of AI in its use of generative models to create responses, while other AI applications use discriminative models (García-Peñalvo & Vázquez-Ingelmo, 2023). The discriminative models of AI are used to classify and categorize data for activities like trend analysis and predicting future outcomes (Kissinger et al., 2021). Contrast that with GAI, which creates new content based on the patterns learned in its existing data and statistical probabilities (Gupta et al., 2024; Jovanovic & Campbell, 2022). As a result of this capability, GAI has been used for a wide range of tasks, including creating text descriptions of images, writing software code from text prompts, and improving video resolution (Bandi et al., 2023).

3.1 GAI in Cybersecurity

GAI can be used to enhance cybersecurity capabilities for organizations and, given the power of GAI tools to mitigate risk and detect attacks, almost 70% of organizations expect to use GAI to improve their cyber defenses (PricewaterhouseCoopers, 2023). Using deep learning techniques to analyze and identify patterns in security data, a GAI tool is able to create simulations of future attacks along with suggestions to mitigate the attacks, enabling the organization to proactively strengthen its defenses (Dhoni & Kumar, 2023; Saddi et al., 2024; Sai et al., 2024; Vemuri et al., 2024). Deep learning brings the strength of analyzing vast amounts of data, both labeled and unlabeled, and working through multiple hidden layers, allowing for complex analysis (Torre et al., 2023). Cybersecurity techniques for attack detection that leverage deep learning include convolutional neural networks, autoencoder, deep Boltzmann machines, recurrent neural networks, generative adversarial networks, and deep reinforcement learning (Dixit & Silakari, 2021; Sarker, 2021; Torre et al., 2023). GAI models use deep learning to analyze patterns in historical network traffic data that support improved detection of abnormal behaviors that may indicate an intrusion or data breach (Alwahedi et al., 2024; Dhoni & Kumar, 2023; Saddi et al., 2024; Sai et al., 2024; Vemuri et al., 2024). Similarly, the authors note that GAI models can help detect malware and phishing emails, enabling identified threats to be isolated proactively and preventing systems from being compromised. Hardware scans automated by GAI tools are capable of identifying misconfigurations or outdated software and providing automated notification to key personnel of what the issue is and how to remediate the problem (Dixit & Silarki, 2021). By training a GAN tool on existing threats, the GAN can synthetically create variations that can then be used as an added layer of screening against future threat developments (Dhoni & Kumar, 2023; Hamouda et al., 2024; Saddi et al., 2024; Vemuri et al., 2024; Wang, 2024). Additionally, GAI can provide automated responses to security threats based on defined organizational rules, like sending an email alert when an anomaly is detected or disabling incoming messages from a particular domain (Dhoni & Kumar, 2023; Saddi et al., 2024). To support ongoing training and incident response readiness activities, GAI can be used to create simulated attack scenarios that teams can practice responding to in a controlled environment (Dhoni & Kumar, 2023; Gupta et al., 2024). Overall, GAI provides benefits to organizations for cybersecurity applications to analyze and assess large quantities of information related to threat intelligence, creating simulated attacks, training for phishing identification, secure code creation and analysis, conduct and report behavior analysis of systems and devices,

automation of cyber defenses, and analyzing information for evidence to determine authenticity (Gupta et al., 2023; Saddi et al., 2024; Sai et al., 2024). The previous examples describe the current capabilities of GAI, while the following section will focus on the direction going forward for GAI integrations with cybersecurity and include examples of available tools.

3.2 State of GAI in Cybersecurity in 2024

GAI is capable of positively transforming cybersecurity by bolstering threat detection, automating security processes, and enabling proactive defense strategies, yet not all organizations are making the most of this powerful technology to reduce cybersecurity risk. While there are many opportunities to benefit from the enhanced capabilities of GAI, commercial software is still evolving to make the most of the new capabilities, as illustrated in Table 2. In the table, examples of GAI software are listed that assist with code vulnerability, identity management, incident response, phishing detection and reporting, remediation identification and guidance, and threat intelligence, yet there is a notable area of opportunity missing from the list: anomaly detection. Both generative adversarial networks and variational autoencoders have been used to generate test data in support of anomaly detection activities; however, these approaches have yet to be successful enough to move beyond the research phase (Li & Li, 2022; Lim et al., 2024). While there are software tools that address intrusion detection and identification of anomalies, these tools have not incorporated GAI capabilities (*Intrusion Detection and Prevention Systems Reviews and Ratings*, n.d.). Similarly, many tools support cybersecurity automation without using GAI, as organizations have integrated AI tools and automation with their cybersecurity defenses (Ponemon Institute & IBM Security, 2023). Software tools equipped with GAI offer promising capabilities to enhance cybersecurity functions. With this broad perspective of GAI use in cybersecurity, it is important to understand aspects of cybersecurity that were once the exclusive domain of human experts that can benefit from the integration of automation tools like AI and GAI, starting with cybersecurity risk assessment, followed by cybersecurity risk management and cybersecurity risk mitigation.

4. Ethical Considerations

GAI tools have made headlines for a variety of reasons – from new capabilities to ethical concerns about training and use. Responsible technology behaviors exist within the bounds of the law and in an ethical way that preserves security, privacy, and accuracy (Bengio et al., 2023; Kallonas et al., 2024; Panchamia et al., 2024). Used ethically, the positive capabilities of new technologies like AI would be maximized and negative features minimized (Russell & Norvig, 2022). While it would be ideal if all technologies were used ethically, that is unfortunately not the case for GAI.

There are no global standards governing data privacy and ethical use, nor are there restrictions on who has access to the free GAI tools (Caldwell, 2023; Shahid & Imteaj, 2024), resulting in many ethical issues that need to be considered around confidentiality, data security, and reliably factual information. For example, generated content may infringe on intellectual property rights or be used to intentionally misrepresent information in a convincing way, which can cause problems when attempting to use the information for cybersecurity tasks like remediation (Gupta et al., 2024; Sai et al., 2024; Teo et al., 2024). Sometimes GAI tools present false information as a response without indicating that it is fictional, leading to false positive or false negative results that can be problematic for cybersecurity tasks like threat evaluations (Caldwell, 2023; Gupta et al., 2024; Sai et al., 2024; Teo et al., 2024; Truong et al., 2020). Individuals using GAI tools may not have sufficient information about the risks and implications of using a particular tool, which may include using their data and queries for further training (Jovanovic & Campbell, 2022; Sai et al., 2024). When sensitive information is used for training, there is a risk that it will inadvertently reproduce that information and effectively leak that data (Caldwell, 2023; Gupta et al., 2024; Sai et al., 2024; Teo et al., 2024). Unfortunately, these GAI tools can also be used in unethical ways to do things like generate malicious code, create phishing emails, produce convincing deep fake videos used for illegal purposes, and provide suggestions about exploitable vulnerabilities (Bandi et al., 2023; Gupta et al., 2024; Shahid & Imteaj, 2024). From the ethical considerations of GAI in cybersecurity, the discussion moves into the challenges and limitations of GAI tools.

5. Challenges and Limitations

There are several challenges and limitations to AI tools, including GAI. For example, when the data quality of the learning dataset is poor due to problems with how the data is collected, structured, analyzed, or presented, the quality of the results provided by an AI tool will also be poor (Hassenstein & Vanella, 2022; Kaur et al., 2023; Parker, 2023). With AI models, the results coming from the model will reflect any biases contained within the learning dataset (Bandi et al., 2023; Gupta et al., 2024; Parker, 2023; Russell & Norvig, 2022; Sai et al., 2024; Teo et al., 2024; Turner Lee et al., 2019). Similarly, misinformation introduced into the training data – either

intentionally or unintentionally – can also lead to incorrect information outputs (Teo et al., 2024; Truong et al., 2020; Zhang et al., 2022). For organizations wanting to use their own training data for GAI cybersecurity systems, there will be a significant investment of time and cost (Bandi et al., 2023; Sai et al., 2024; Zhang et al., 2022). High quality data is no guarantee that the results can be reasonably interpreted by humans receiving the information, which can be of particular concern in cybersecurity applications (Sai et al., 2024). In addition, the logic used by GAI tools is opaque and not yet explainable, which can make it challenging to ensure that results are accurate (Bandi et al., 2023; Caldwell, 2023; Jovanovic & Campbell, 2022; Kaur et al., 2023; Sai et al., 2024; Teo et al., 2024; Zhang et al., 2022). Even with the most sophisticated tools and data, these tools cannot fully replicate or replace human intelligence (Zhang et al., 2022).

6. Future Directions and Research Opportunities

Based on the literature, there are many opportunities for additional research related to GAI in cybersecurity. First, a look at emerging trends with GAI use in cybersecurity.

6.1 Emerging Trends in GAI for Cybersecurity

With GAI in its early stages of integration into cybersecurity, much of the literature examines possible use cases for the technology within the cybersecurity domain rather than actual use. Going forward, GAI may be integrated into automated reporting to further speed up analysis activities and leveraged by cybersecurity teams to predict future threats as well as support activities for tabletop exercises to prepare the organization to respond effectively to a cyberattack. Because threat intelligence sharing focuses on a common set of threats, there could be consolidation in this area into a few major players offering a comprehensive threat intelligence package with GAI integration that operates similarly to how antivirus software works today, in that organizations will receive regular local updates based on a centralized database from a vendor rather than trying to manage it at the organization level. While these are speculative ideas, the research gaps and opportunities are more clearly defined.

6.2 Research Gaps and Opportunities

Current research addresses technical aspects of using GAI tools and proposes ideas for how the technology can possibly be used; however, there are gaps identified by this scoping review concerning the practical aspects of organizational decision-making to determine whether or not to integrate GAI and the activities involved with implementing GAI technology into cybersecurity activities. Future research should explore business cases and decision criteria, implementation practices, benefits realized from integrating GAI with cybersecurity, impacts of the changing cybersecurity threat landscape, and challenges or additional risks identified during implementation and operations. Additionally, current studies are predominantly qualitative, so future quantitative studies could assist practitioners in understanding best practices, standards, benefits, and challenges with tools beyond theoretical possibilities. As GAI is still evolving as a technology, it is also possible that new capabilities will lead to additional research opportunities.

7. Discussion

While organizations have been integrating AI into cybersecurity and benefiting from automation that reduces the time to detect and respond to cyberattacks, GAI is in its early stages of exploration to identify capabilities and optimal utility. Because large amounts of data are required in order to effectively train and tailor GAI tools to organizational needs, organizations that have large amounts of proprietary data and technical teams capable of building and integrating that data into GAI tools are well-positioned to make the most of the technology. For organizations that do not have the resources, there are commercial tools that leverage large datasets of cybersecurity data and may be of use. An additional challenge is understanding which use cases make sense for each organization, given a lack of predefined criteria. In order to assess utility, organizations need to clearly define business cases and assess both the risks and benefits of various solutions. Based on the literature, use cases that seem to be most likely to be worth the investment are predicting and designing a defense against potential threats using GANs, enhancing research and reporting activities with GAI, and developing a chatbot to guide cybersecurity teams through remediation activities. Future research may discover additional use cases while also addressing the gap in understanding of real-world applications, processes that support effective use, and measurable outcomes to assess results.

References

Aceto, G., Giampaolo, F., Guida, C., Izzo, S., Pescapè, A., Piccialli, F., & Prezioso, E. (2024). Synthetic and privacy-preserving traffic trace generation using generative AI models for training network intrusion detection systems. *Journal of Network and Computer Applications, 229*, 103926. https://doi.org/10.1016/j.jnca.2024.103926

Alawida, M., Shawar, B. A., Abiodun, O. I., Mehmood, A., Omolara, A. E., & Hwaitat, A. K. A. (2024). Unveiling the dark side of ChatGPT: Exploring cyberattacks and enhancing user awareness. *Information*, *15*(1), 27. https://doi.org/10.3390/info15010027

Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T., & Whyte, D. (2024). Generative artificial intelligence and cyber security in central banking. *BIS Papers.* https://doi.org/10.1093/jfr/fjae008

Almeida, J., & Gonçalves, T. C. (2024). The AI revolution: Are crypto markets more efficient after ChatGPT 3? *Finance Research Letters*, *66*, 105608. https://doi.org/10.1016/j.frl.2024.105608

Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet of Things and Cyber-physical Systems, 4*, 167–185. https://doi.org/10.1016/j.iotcps.2023.12.003

Andreoni, M., Lunardi, W. T., Lawton, G., & Thakkar, S. (2024). Enhancing autonomous system security and resilience with Generative AI: A comprehensive survey. *IEEE Access*, *12*, 109470–109493. https://doi.org/10.1109/access.2024.3439363

Bandi, A., Adapa, P. V. S. R., & Kuchi, Y. E. V. P. K. (2023). The power of generative AI: A review of requirements, models, input–output formats, evaluation metrics, and challenges. *Future Internet*, *15*(8), 260. https://doi.org/10.3390/fi15080260

Banko, M., Brili, E., Dumais, S., & Lin, J. (2002). AskMSR: Question answering using the worldwide web. In *Proceedings of 2002 AAAI Spring Symposium on Mining Answers from Texts and Knowledge Bases,* 7-9. https://cs.uwaterloo.ca/~jimmylin/publications/Banko_etal_AAAI2002.pdf

Bartolo, A. (2023, February 16). GitHub Copilot update: New AI model that also filters out security vulnerabilities. *Educator Developer Blog*. https://techcommunity.microsoft.com/blog/educatordeveloperblog/github-copilot-update-new-ai-model-that-also-filters-out-security-vulnerabilitie/3743238

Bengio, Y., Hinton, G., Yao, A., Song, D., Abbeel, P., Darrell, T., ... & Mindermann, S. (2024). Managing extreme AI risks amid rapid progress. *Science*, *384*(6698), 842-845. https://doi.org/10.1126/science.adn0117

Caldwell, A. (2023). Novel cybersecurity challenges within Artificial Intelligence. *Journal of Internet Technology and Secured Transaction, 11*(1), 796–801. https://doi.org/10.20533/jitst.2046.3723.2023.0098

Dhoni, P. S., & Kumar, R. (2023). Synergizing generative Artificial Intelligence and cybersecurity: Roles of generative Artificial Intelligence entities, companies, agencies and government in enhancing cybersecurity. *Journal of Global Research in Computer Sciences. 14*(3). https://doi.org/10.4172/2229-371X.14.3.005

Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, *39*, 100317. https://doi.org/10.1016/j.cosrev.2020.100317

Drew, J. (2024). Tech roundtable: There's more to AI than ChatGPT: Our panel provides perspective on the potential, perils, and place of GenAI in the wider context of Artificial Intelligence and automation. *Journal of Accountancy*, *237*(4), 22–25.

Dwivedi, R., & Elluri, L. (2024). Exploring generative Artificial Intelligence research: A bibliometric analysis approach. *IEEE Access*, *12*, 119884–119902. https://doi.org/10.1109/access.2024.3450629

Eaton, C., Rundle, J., & Uberti, D. (2021, May 9). U.S. pipeline shutdown exposes cyber threat to energy sector. *Wall Street Journal*. https://www.wsj.com/articles/u-s-pipeline-shutdown-exposes-cyber-threat-to-energy-sector-11620574464

Eze, C. S., & Shamir, L. (2024). Analysis and prevention of AI-Based phishing email attacks. *Electronics*, *13*(10), 1839. https://doi.org/10.3390/electronics13101839

García-Peñalvo, F., & Vázquez-Ingelmo, A. (2023). What do we mean by GenAI? a systematic mapping of the evolution, trends, and techniques involved in generative AI. *International Journal of Interactive Multimedia and Artificial Intelligence*, *8*(4), 7. https://doi.org/10.9781/ijimai.2023.07.006

Gill, S. S., & Kaur, R. (2023). ChatGPT: Vision and challenges. *Internet of Things and Cyber-physical Systems*, *3*, 262–271. https://doi.org/10.1016/j.iotcps.2023.05.004

Google Cloud. (2023). *Cybersecurity forecast 2024: Insights for future planning*. https://cloud.google.com/resources/security/cybersecurity-forecast

Guo, D., Chen, H., Wu, R., & Wang, Y. (2023). AIGC challenges and opportunities related to public safety: A case study of ChatGPT. *Journal of Safety Science and Resilience*, *4*(4), 329–339.

https://doi.org/10.1016/j.jnlssr.2023.08.001

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. *IEEE Access, 11*, 80218-80245. https://doi.org/10.1109/ACCESS.2023.3300381

Hamouda, D., Ferrag, M. A., Benhamida, N., Seridi, H., & Ghanem, M. C. (2024). Revolutionizing intrusion detection in industrial IoT with distributed learning and deep generative techniques. *Internet of Things, 26*, 101149. https://doi.org/10.1016/j.iot.2024.101149

Hassenstein, M. J., & Vanella, P. (2022). Data quality—concepts and problems. *Encyclopedia*, *2*(1), 498-510. https://doi.org/10.3390/encyclopedia2010032

Hu, M., Behar, E., & Ottenheimer, D. (2024). National security and federalizing data privacy infrastructure for AI governance. *Fordham Law Review*, *92*(5), 1829–1853.

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023). The devastating business impacts of a cyber breach. *Harvard Business Review. https://hbr. org/2023/05/thedevastating-business-impacts-of-a-cyber-breach*.

Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024). AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business. *AI and Ethics*, 1-14. https://doi.org/10.1007/s43681-024-00443-4

Intrusion detection and prevention systems reviews and ratings. (n.d.). Gartner. Retrieved October 4, 2024, from https://www.gartner.com/reviews/market/intrusion-prevention-systems

IRONSCALES. (2023, June 20). *IRONSCALES revolutionizes email security with powerful new generative AI capabilities*. https://ironscales.com/news/ironscales-announces-themis-copilot

Jovanovic, M., & Campbell, M. (2022). Generative Artificial Intelligence: Trends and prospects. *Computer, 55*(10), 107-112. https://doi.org/10.1109/MC.2022.3192720

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, *28*(2), 275-301. https://doi.org/10.1108/IJAIM-01-2019-0006

Jüttner, V., Grimmer, M., & Buchmann, E. (2024). ChatIDS: Advancing explainable cybersecurity using generative AI. *International Journal on Advances in Security, 17*(1), 2. https://www.researchgate.net/profile/Victor-Juettner/publication/382069889_ChatIDS_Advancing_Explainable_Cybersecurity_Using_Generative_AI/links/668bd697714e0b03154c15cb/ChatIDS-Advancing-Explainable-Cybersecurity-Using-Generative-AI.pdf

Kallonas, C., Piki, A., & Stavrou, E. (2024, May). Empowering professionals: a generative AI approach to personalized cybersecurity learning. In *2024 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1-10). IEEE. https://doi.org/10.1109/EDUCON60312.2024.10578894

Kam, H. J., Zhong, C., & Johnston, A. (2024). The impacts of generative AI on the cybersecurity landscape. In *ECIS 2024 TREOS*. 9. https://aisel.aisnet.org/treos_ecis2024/9

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2023). Machine learning for healthcare-IoT security: A review and risk mitigation. *IEEE Access*, *11*, 145869–145896. https://doi.org/10.1109/ACCESS.2023.3346320

Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2021). *The age of AI: And our human future* (1st ed.). Little, Brown and Company.

Kolochenko, I., & Heiskell, M. P. (2024). Generative AI, cybersecurity and cybercrime for lawyers: Myths, risks and benefits. Mealey's litigation report: *Artificial Intelligence, 1*(10). https://platt.law/Generative-AI-Cybersecurity-and-Cybercrime-for-Lawyers.pdf

Lee, D. (2023, June 15). Introducing SecureFrame Comply AI: Faster, tailored cloud remediation. *Secureframe*. https://secureframe.com/blog/secureframe-comply-ai

Lee, N. (2024). *Counterterrorism and cybersecurity: Total information awareness* (3rd ed.). Springer. https://doi.org/101007/978-3-031-63126-9

Li, H., & Li, Y. (2022). Anomaly detection methods based on GAN: A survey. *Applied Intelligence*, *53*(7), 8209–8231. https://doi.org/10.1007/s10489-022-03905-6

Lim, W., Chek, K. Y. S., Theng, L. B., & Lin, C. T. C. (2024). Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. *Computers & Security*, 103733. https://doi.org/10.1016/j.cose.2024.103733

Loh, E. (2023). ChatGPT and generative AI chatbots: Challenges and opportunities for science, medicine and medical leaders. *BMJ Leader*, *0*, 1–4. https://doi.org/10.1136/leader-2023-000797

Lyngaas, S. (2023, December 1). Federal investigators confirm multiple US water utilities hit by hackers. *CNN*. https://www.cnn.com/2023/12/01/politics/us-water-utilities-hack/index.html

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications, 232*, 104004. https://doi.org/10.1016/j.jnca.2024.104004

Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab021

Mamgai, A. (2023, October 16). *Generative AI with cybersecurity: friend or foe of digital transformation?* ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2023/generative-ai-with-cybersecurity-friend-or-foe-of-digital-transformation

Mavikumbure, H. S., Cobilean, V., Wickramasinghe, C. S., Drake, D., & Manic, M. (2024, July). Generative AI in cyber security of cyber physical systems: Benefits and threats. In *16th International Conference on Human System Interaction (HSI),* 1-8. https://doi.org/10.1109/HSI61632.2024.10613562

Microsoft. (2024). *National Public Data breach: What you need to know*. Microsoft Support. Retrieved October 2, 2024, from https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535

Microsoft. (n.d.). *AI for cybersecurity: Protect with AI*. https://www.microsoft.com/en-us/security/business/solutions/generative-ai-cybersecurity

Miller, K. (2024, April 18). *Rural Texas towns report cyberattacks that caused one water system to overflow*. AP News. https://apnews.com/article/texas-muleshoe-water-systems-cyberattacks-russia-5f388bf0d581fc8eb94b1190a7f29c3a

Munn, Z., Peters, M. D., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC medical research methodology*, *18*, 1-7. https://doi.org/10.1186/s12874-018-0611-x

National Institute of Standards and Technology. (2024). Artificial Intelligence risk management framework: Generative Artificial Intelligence profile. In *NIST.gov* (NIST AI 600-1). https://doi.org/10.6028/nist.ai.600-1

NVIDIA. (n.d.). *Spear Phishing Detection AI Workflow*. https://www.nvidia.com/en-us/ai-data-science/ai-workflows/spear-phishing/

Palani, K., Kethar, J., Prasad, S., & Torremocha, V. (2024). Impact of AI and generative AI in transforming cybersecurity. *Journal of Student Research*, *13*(2). https://doi.org/10.47611/jsrhs.v13i2.6710

Panchamia, V., Harchwani, A., & Momaya, T. (2024). Cybersecurity renaissance: Navigating threats, ethical hacking, and risk mitigation in the digital era. *International Journal of Scientific Research in Engineering and Management (IJSREM), 08*(01), 1–10. https://doi.org/10.55041/ijsrem28181

Parker, J. (2023, October). *Behind the scenes of AI: How data drives the intelligence. [Professional organization presentation].* Society for Information Management Las Vegas Chapter, Las Vegas, NV, United States.

Pasupuleti, R., Vadapalli, R., & Mader, C. (2023, November). Cyber security issues and challenges related to generative AI and ChatGPT. In *Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS),* 1-5. https://doi.org/10.1109/SNAMS60348.2023.10375472

Pattison-Gordon, J. (2024). *Michael Makstman*. GovTech. https://www.govtech.com/top-25/michael-makstman

Peters, M. D., Godfrey, C., McInerney, P., Munn, Z., Tricco, A. C., & Khalil, H. (2020). Chapter 11: Scoping reviews. *JBI manual for evidence synthesis*. https://doi.org/10.46658/jbimes-20-12

Petrosyan, A. (2024, September 26). *U.S. companies at risk of cyberattacks according to CISOs 2021-2024*. Statista. https://www.statista.com/statistics/1448307/companies-at-material-cyberattack-risk-us/#statisticContainer

Ponemon Institute & IBM Security. (2023). *Cost of a data breach 2023*. IBM Corporation.

Potti, S., & Joyce, S. (2024, May 6). *Introducing Google Threat Intelligence: Actionable threat intelligence at Google Scale.* Google Cloud Blog. https://cloud.google.com/blog/products/identity-security/introducing-google-threat-intelligence-actionable-threat-intelligence-at-google-scale-at-rsa/

Poulsen, K., McMillan, R., & Evans, M. (2021, September 30). A hospital hit by hackers, a baby in distress: The case of the first alleged ransomware death. *Wall Street Journal.* https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

PricewaterhouseCoopers. (2023). *The C-suite playbook: Putting security at the epicenter of innovation.* https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html?

Privacy Rights Clearinghouse. (2023, September). *Data breach chronology*. PrivacyRights.org. https://privacyrights.org/data-breaches

Quintero, B. (2023, April 24). *Introducing VirusTotal Code Insight: Empowering threat analysis with generative AI*. https://blog.virustotal.com/2023/04/introducing-virustotal-code-insight.html

Raman, R., Calyam, P., & Achuthan, K. (2024). ChatGPT or Bard: Who is a better Certified Ethical Hacker? *Computers & Security*, *140*, 103804. https://doi.org/10.1016/j.cose.2024.103804

Raman, R., Pattnaik, D., Hughes, L., & Nedungadi, P. (2024). Unveiling the dynamics of AI applications: A review of reviews using scientometrics and BERTopic modeling. *Journal of Innovation & Knowledge, 9*(3), 100517. https://doi.org/10.1016/j.jik.2024.100517

Renaud, K., Warkentin, M., & Westerman, G. (2023). *From ChatGPT to HackGPT: Meeting the cybersecurity threat of generative AI*. MIT Sloan Management Review.

Rundle, J., & Nash, K. S. (2024, October 16). For some companies, the real cost of a cyberattack is telling everyone about it. *Wall Street Journal*. https://www.wsj.com/articles/for-some-companies-the-real-cost-of-a-cyberattack-is-telling-everyone-about-it-735bee74

Russell, S. J., & Norvig, P. (2022). *Artificial Intelligence: A modern approach* (4th ed.). Pearson India Education Service Pvt. Ltd.

Rust, M., & Ruiz, R. (2021, May 13). Why the Colonial Pipeline shutdown is causing gas shortages. *Wall Street Journal*. https://www.wsj.com/articles/why-the-colonial-pipeline-shutdown-is-causing-gasoline-shortages-11620898203

Saddi, V. R., Gopal, S. K., Mohammed, A. S., Dhanasekaran, S., & Naruka, M. S. (2024, March). Examine the role of generative AI in enhancing threat intelligence and cyber security measures. In *2nd International Conference on Disruptive Technologies (ICDT),* 537-542. https://doi.org/10.2209/ICDT61202.2024.10489766

Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). Generative AI for cyber security: Analyzing the potential of chatgpt, dall-e and other models for enhancing the security space. *IEEE Access. 12*, 53497-53516. https://doi.org/10.1109/ACCESS.2024.3385107

Sarker, I. H. (2021). Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective. *SN Computer Science*, *2*(3), 154. https://doi.org/10.1007/s42979-021-00535-6

SentinelOne. (2023, April 26). *Purple AI: Empowering cybersecurity analysts with AI-Driven threat hunting, analysis & response*. https://www.sentinelone.com/blog/purple-ai-empowering-cybersecurity-analysts-with-ai-driven-threat-hunting-analysis-response/

Shahid, A. R. B., & Imteaj, A. (2024). Sticks and stones may break my bones, but words will never hurt me!—Navigating the cybersecurity risks of generative AI. *AI & Society*, 1-2. https://doi.org/10.1007/s00146-024-01934-y

Shipkowski, B. (2024, October 7). *American Water, the largest water utility in US, is targeted by a cyberattack*. AP News. https://apnews.com/article/american-water-cyberattack-36423062dbce05c9aa70ef8aa07810cb

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, *104*, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Snyk. (n.d.). *SNYK Developer Security Platform*. https://snyk.io/platform/

SonicWall. (2024). 2024 SonicWall cyber threat report. In *SonicWall*. https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf

Ssetimba, I. D., Kato, J., Pinyi, E. O., Twineamatsiko, E., Nakayenga, H. N., & Muhangi, E. (2024). Advancing electronic communication compliance and fraud detection through machine learning, NLP and generative AI: A pathway to enhanced cybersecurity and regulatory adherence. *World Journal of Advanced Research and Reviews, 23*(2), 697-707. https://doi.org/10.30574/wjarr.2024.23.2.2364

Stratton, S. J. (2019). Literature reviews: Methods and applications. *Prehospital and disaster medicine*, *34*(4), 347-349. https://doi.org/10.1017/S1049023X19004588

Szmurlo, H., & Akhtar, Z. (2024). Digital sentinels and antagonists: The dual nature of chatbots in cybersecurity. *Information*, *15*(8), 443. https://doi.org/10.3390/info15080443

Takale, D. G., Mahalle, P. N., & Sule, B. (2024). Cyber security challenges in Generative AI technology. *Journal of Network Security Computer Networks, 10*(1), 28-34.

Teig, J., & Eiken, A. (2024). Use of Generative AI in Offensive Cybersecurity: A case study using PentestGPT with GPT-4 and Dolphin2. 5 *(Bachelor's thesis, NTNU)*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3139808

Tenable. (n.d.). *Tenable ExposureAI: Harness the power of generative AI for preventive security*. https://www.tenable.com/solutions/exposure-ai

Teo, Z. L., Quek, C. W. N., Wong, J. L. Y., & Ting, D. S. W. (2024). Cybersecurity in the generative Artificial Intelligence era. *Asia-Pacific Journal of Ophthalmology*, *13*(7), 100091. https://doi.org/10.1016/j.apjo.2024.100091

Torre, D., Mesadieu, F., & Chennamaneni, A. (2023). Deep learning techniques to detect cybersecurity attacks: A systematic mapping study. *Empirical Software Engineering*, *28*(3). https://doi.org/10.1007/s10664-023-10302-1

Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial Intelligence and cybersecurity: Past, presence, and future. In *Artificial intelligence and evolutionary computations in engineering systems* (pp. 351-363). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-0199-9_30

Turner Lee, N., Resnick, P., & Barton, G. (2019, May 22). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. Brookings. https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

US Census Bureau. (2024, September 3). *Population and housing unit estimates*. Census.gov. https://www.census.gov/programs-surveys/popest.html

Vemuri, N., Thaneeru, N., & Tatikonda, V. M. (2024). Adaptive generative AI for dynamic cybersecurity threat detection in enterprises. *International Journal of Science and Research Archive*. 11(01), 2259–2265. https://doi.org/10.30574/ijsra.2024.11.1.0313

Verdejo, C., Tapia-Benavente, L., Schuller-Martínez, B., Vergara-Merino, L., Vargas-Peirano, M., & Silva-Dreyer, A. M. (2021). What you need to know about scoping reviews. *Medwave*, *21*(02), e8144. https://doi.org/10.5867/medwave.2021.02.8144

Wang, M. (2024). Generative AI: A new challenge for cybersecurity. *Journal of Computer Science and Technology Studies*, *6*(2), 13-18. https://doi.org/10.32996/jcsts.2024.6.2.3

World Economic Forum & Accenture. (2024). *Global cybersecurity outlook 2024*. World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Yi, J.-K., & Yao, Y.-F. (2024). Advancing quality assessment in vertical field: Scoring calculation for text inputs to large language models. *Applied Sciences*, *14*(16), 6955. https://doi.org/10.3390/app14166955

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial Intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25. https://doi.org/10.3390/fi15090286

Appendix A

Tables

Table 1. Sources included in the scoping review with methods and theories summarized

Source	Methods and theories
Aceto et al., 2024	Empirical study comparing different types of data models for training synthetic data generators.
Alawida et al., 2024	A narrative review of ChatGPT and cyberattacks with quantitative analysis of a user awareness survey of how ChatGPT relates to cyberattacks.
Aldasoro et al., 2024	A narrative review of GAI and how it relates to cyber risk for the banking industry with quantitative analysis from a survey about AI and cyber security for the banking sector.
Almeida & Gonçalves, 2024	Adjusted Market Inefficiency Magnitude (AMIM) is used to quantitatively analyze market efficiency.
Alwahedi et al., 2024	Semi-structured literature review focusing on cyber threat detection, machine learning techniques, Intrusion Detection Systems (IDSs), open issues, and the future with GAI.
Andreoni et al., 2024	A narrative review focusing on the use, issues, and advancements of GAI for securing autonomous systems (e.g., self-driving cars, robotic arms).
Dhoni & Kumar, 2023	GAI tool exploration and literature review (narrative) focusing on benefits, issues, and issue mitigation with the topics of GAI and cybersecurity.
Drew, 2024	Expert panel discussion of risks, opportunities, and applications of GAI, along with automation and AI tools for accounting applications.
Dwivedi & Elluri, 2024	Bibliometric analysis of published research about GAI using quantitative analysis of characteristics, research themes, social network, and performance.
Eze & Shamir, 2024	Empirical evaluation of multiple methods of automated classification of AI-generated phishing emails from known datasets using statistical analysis.
Gill & Kaur, 2023	Semi-structured literature review of ChatGPT, including background, capabilities, beneficial uses, integration with IoT, trends, and research opportunities.
Guo et al., 2023	A narrative review of AI-generated content (AIGC), security challenges and mitigations, and security applications.
Gupta et al., 2023	Semi-structured literature review of GAI applications for cybersecurity, including risks and beneficial uses for both attackers and defenders.
Hamouda et al., 2024	Experiments were conducted with the introduced FedGenID security framework, with results quantitatively analyzed to assess efficacy using a known dataset that can generate synthetic data to augment the dataset.
Hu et al., 2024	An essay discussing security and AI governance benefits of integrating data infrastructure into an overall infrastructure strategy.
Humphreys et al., 2024	Semi-structured literature review of cybersecurity and AI concerns using a blend of principlist ethics and framework for a Good AI society as a framework to identify and analyze ethical obligations and risks.
Jüttner et al., 2024	Plan-Do-Check-Act cycle applied to cyber security. Research conducted experiments to evaluate the ability of a GAI tool to provide actionable and accurate explanations of home security alerts to non-technical individuals.
Kam et al., 2024	Grounded theory qualitative analysis of public Reddit posts to represent interactions between human cognition and GAI then from cybersecurity professionals via online panel discussions to understand how GAI was perceived. Open, axial, and selective coding were used.
Khatun et al, 2023	Structured review of healthcare IoT devices and the importance of monitoring the devices along with an overview of cybersecurity risks and mitigations.
Kolochenko & Heiskell, 2024	Commentary focusing on impacts and risks for lawyers from GAI, cybersecurity, and cybercrime.
Loh, 2023	A narrative review of ChatGPT and GAI chatbots that explores risks and benefits for healthcare.
Mahboubi et al., 2024	A systematic review of cyber threat hunting techniques and challenges to understand best practices, hypothesis models, challenges, and how challenges can be addressed.

Mavikumbure et al., 2024	A systematic review of GAI and cybersecurity of Cyber-Physical Systems (CPS) focusing on history, risks, beneficial uses, and risk mitigations.
Palani et al., 2024	Semi-structured review of AI technologies and cybersecurity to explore concepts, trends, uses, impacts, and prevalence of usage.
Pasupuleti et al., 2023	A narrative review of cybersecurity risks and challenges that exist as a result of GAI and ChatGPT.
Pattison-Gordon, 2024	Profile of Michael Makstman, CISO for the city of San Francisco, and his work on cybersecurity.
Raman, Calyam et al., 2023	An experiment was conducted with ChatGPT and Bard to evaluate their performance on a Certified Ethical Hacking Exam, with the results analyzed quantitatively to assess which tool performed better.
Raman, Pattnaik et al., 2023	A systematic review using the PRISMA protocol to review other AI review papers to identify themes and categories.
Renaud et al, 2023	High-level information about cybersecurity risks from ChatGPT and what organizations and individuals can do to mitigate the risks.
Saddi et al., 2024	An experiment was conducted to quantitatively evaluate the effectiveness of a new GAI algorithm compared to four existing ones to improve cyber security and threat intelligence in organizations.
Sai et al, 2024	A narrative review of GAI used for cybersecurity applications along with capabilities and limitations.
Shahid & Imteaj, 2024	Commentary about GAI cybersecurity risks and suggestions to address them.
Ssetimba et al., 2024	Application of machine learning (ML) theory, natural language processing (NLP) theory, GAI theory, and compliance theory to quantitatively analyze case studies and existing data sources. The analysis provides positive impacts of using tools with ML, NLP, and GAI to improve fraud detection and compliance for financial services companies.
Szmurlo & Akhtar, 2024	Structured review of chatbots, providing definitions, history, functionality, technical overviews, uses and impacts, attacks on and with chatbots, defenses for and with chatbots, limitations, and examples of chatbots used for cyberattacks.
Takale et al., 2024	A structured review of GAI cybersecurity risks and mitigations for text-based, media-based, and code-based GAI tools.
Teig & Eiken, 2024	Case study of the integration of large language models with PentestGPT to evaluate the impact on penetration testing. Quantitative analysis of penetration testing results and qualitative thematic analysis of researcher observations were conducted.
Teo et al., 2024	Semi-structured review of risks and mitigations for cybersecurity in GAI applications and as a tool to support cybersecurity for healthcare organizations.
Vemuri et al., 2024	Semi-structured review of GAI use for detecting and mitigating cybersecurity threats, including pros and cons of different adaptive GAI approaches.
Wang, 2024	A systematic review of GAI in the cybersecurity field, identification of issues and challenges, ethical aspects, and strategies to address security risks
Yi & Yao, 2024	An empirical study to test the relationship between proposed evaluation criteria (vertical field score) and the generated text quality for a set of input questions designed for five distinct cybersecurity problems, using the Chinese language.

Table 2. Cybersecurity functions supported by GAI in commercial software

Cybersecurity Function	**Commercial Software (with GAI)**
Code vulnerability identification and analysis	• Microsoft GitHub Copilot (Bartolo, 2023) • Snyk Developer Security Platform (Snyk, n.d.) • VirusTotal Code Insight (Quintero, 2023)
Identity management	• Microsoft Copilot for Security (Microsoft, n.d.)
Incident response	• Microsoft Copilot for Security (Microsoft, n.d.)
Phishing detection and reporting	• IRONSCALES Themis Copilot for Microsoft Outlook (IRONSCALES, 2023) • NVIDIA Spear Phishing Detection AI Workflow (NVIDIA, n.d.)
Remediation identification and guidance	• Secureframe Comply AI (Lee, 2023) • Tenable ExposureAI (Tenable, n.d.)

Threat intelligence	• Google Threat Intelligence (Potti & Joyce, 2024) • Microsoft Copilot for Security (Microsoft, n.d.) • SentinelOne PurpleAI (SentinelOne, 2023) • Tenable ExposureAI (Tenable, n.d.) • VirusTotal Code Insight (Quintero, 2023)

Note. Commercial software was identified in October 2024; the list is a sample and not intended to be exhaustive.