World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Strengthening Homeland Security Preparedness against Adversarial Use of Generative AI in the United States: A Scoping Review

Aisha Mohammed Suleiman [1] and Alice Ama Donkor [2,*]

[1] *University of Iowa, Iowa, USA.*
[2] *Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana.*

World Journal of Advanced Research and Reviews, 2025, 28(02), 1169-1175

Publication history: Received on 20 September 2025; revised on 01 November 2025; accepted on 04 November 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.2.3658

Abstract

Generative artificial intelligence (GenAI) and large language models (LLMs) are transforming the U.S. security landscape, reshaping both its prospects and challenges. Their adversarial use, from deepfakes, synthetic disinformation, automated phishing, and cyberattacks on critical infrastructure, constitutes a considerable test for homeland security preparedness. Despite these urgent developments, the literature remains limited across law, policy, and security domains.

In line with this gap, this scoping review maps the current state of knowledge on three issues: (1) adversarial uses of GenAI with respect to U.S. homeland security, (2) defensive strategies that have been proposed or tried, and (3) the legal and government frameworks shaping American responses to these challenges. The review was guided by the Systematic Reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR).The evidence reveals that GenAI reduces the threshold of cyberattack, phishing, and ransomware penetration tests, which existing liability laws and regulatory frameworks struggle to capture. Defensive technologies such as adversarial training data, anomaly detection, and automated incident responses appear promising. Federal efforts like the 2023 Executive Order on AI show emerging policy alignments. However, there are struggles with implementation.

In conclusion, this paper argues that GenAI is both a threat and a resource for resilience. Therefore, effective preparation requires building bridges that bring together law, technology, and governance into a framework wherein homeland infrastructure can protect itself against new forms of adversarial use.

Keywords: Homeland Security; Generative AI; United States; Cybersecurity; Critical Infrastructure; Disinformation; Policy Preparedness

1. Introduction

From research labs to everyday applications, generative artificial intelligence (GenAI) has advanced quickly [1]. Large language models and video and picture generators are examples of tools that are now easily accessible and user-friendly (Pantano friendly) [2; 3]. Although these systems can help public services, businesses, and education, they also present new homeland security threats. For instance, studies have shown that generative artificial intelligence can generate persuasive text, images, voices, and software code at scale, unlike normal cyber programs [4; 5]. This implies that advanced attacks can now be launched by malicious actors without the need for advanced technological abilities.

The adversarial use of GenAI is a top priority for the U.S. Department of Homeland Security (DHS) and the Agency for Cybersecurity and Infrastructure Security (CISA). According to their most recent strategies and risk evaluations,

* Corresponding author: Alice Ama Donkor

adversaries have begun to experiment with GenAI to disseminate false information, produce convincing deepfakes, and create or modify cyberattacks [6]. These dangers are not merely imaginable but highly practicable. For instance, cybersecurity companies have identified ransomware groups investigating GenAI for more adaptable attacks, and law enforcement has already reported multiple frauds involving AI-generated voice recordings [7-9].

According to a study by Bellavita [10], Homeland Security comprises various groups, including federal agencies, state and local governments, and private companies, responsible for the protection of important state security infrastructure. Thus, it would be possible to target any of these agencies. For example, in instances of a national tragedy or disaster, a deepfake video could fool people, an AI-generated phishing email could get into a hospital system, or an AI-assisted malware could mess up energy grids [11-13]. This implies that GenAI not only poses technical risks, but it also makes people less likely to trust official communications, which are essential for handling emergencies effectively.

While people are becoming increasingly concerned, there is little research about adversarial use of GenAI and how prepared the U.S. is for homeland security [14; 15]. Most research has highlighted vulnerabilities [4; 8; 16], which underline big risks [6]. However, very few have examined specific ways to prepare for them. This division makes it problematic for decision makers and law enforcement agencies to see the whole picture.

Thus, a gap exists in the availability of many documented real-life examples of GenAI being used against U.S. security interests. Also, while federal agencies like DHS and CISA have started red-teaming and providing guidance, local responders and infrastructure operators often do not have the training and needed tools to identify AI-enabled threats [17]. Furthermore, the way governments respond to technological evolutions is still slower than the rate at which technology itself changes. For instance, RAND and other analysts have noted that adversaries can adapt and utilize open-source GenAI models more quickly than U.S. institutions can develop defenses [18].

It is in light of the above, that the current review maps and synthesizes what is currently known about the adversarial use of GenAI and how the United States is preparing to counter it by (1) Identifying documented or anticipated GenAI-enabled threats relevant to homeland security (2) Examining preparedness and mitigation strategies described in the literature, including technical, operational, and policy measures. (3) Highlighting evidence gaps where further research and actions are needed.

2. Methods

The review adhered to the guidelines set forth by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR). Thus, the process ensured that the principles of transparency, reproducibility, and completeness were followed.

2.1. Eligibility Criteria

Table 1 Outlines the eligibility domains and operational definitions

Domain	Operational definitions	Samples from selected sources
Population	Studies addressing adversarial or malicious uses of generative AI relevant to national/homeland security	Cybersecurity, disinformation, terrorism, critical infrastructure
Concept	Applications, threats, or preparedness strategies linked to generative AI	Deepfakes, LLM-enabled cyberattacks, policy frameworks, resilience models
Context	U.S. homeland security or comparable national security settings	DHS/CISA reports, U.S. executive orders, peer-reviewed U.S.-focused studies
Types of evidence	Peer-reviewed journal articles, government/agency reports, think tank papers, industry white papers (2020–2025)	PRISMA-ScR eligible sources

2.2. Table 1 outlines the eligibility domains and operational definitions applied to this review.

A literature search was conducted in Google Scholar, Scopus, Web of Science Core Collection, and PubMed/MEDLINE, with grey literature also included in the search on U.S. government and agency websites (e.g., DHS/CISA, NIST, DOE CESER, DOT, EPA, HHS/ASPR) and selected U.S. think tanks and research organizations (e.g., RAND, CSIS, MITRE).

Keywords and controlled vocabulary were combined to capture work on Generative AI, large language models, agentic AI, cybersecurity, homeland security, and critical infrastructure protection in the United States. Search strategies were also adapted to each database. The search results were managed using a citation program, and all duplicates were removed. Screening of titles and abstracts was conducted independently by two reviewers, with full texts reviewed by a third reviewer to resolve any disagreements. In addition, reasons for exclusion were recorded in a table. Data extraction was conducted using a pre-tested form, which captured information on study details; definitions of the infrastructure sector(s); demographics or system characteristics where relevant; the type of AI model (generative AI, LLM, or agentic AI); the specific application domain (cybersecurity task such as anomaly detection, phishing defense, incident response, resilience testing, or evaluation/benchmarking); barriers and challenges (e.g., trust, privacy, availability, appropriateness, governance); performance measures used; and the main findings and implications.

Synthesis involved descriptive mapping of study designs, critical infrastructure sectors, and AI models, as well as thematic analysis of barriers and opportunities. Findings were grouped by security framework domains (e.g., NIST CSF functions: Identify, Protect, Detect, Respond, Recover) and by types of AI application (generative, evaluative, or agentic). Where possible, findings were contextualized in terms of their implications for U.S. homeland security and critical infrastructure resilience, linking challenges and opportunities in generative AI/LLM use to broader national security outcomes.

3. Results

The included U.S. focused Studies ranged from analyses of cybersecurity risks in generative AI to resilience-focused frameworks for critical infrastructure.

Table 2 Study Characteristics of U.S.-Focused Literature on Generative AI and Homeland Security Preparedness

Author(s), Year	Study Design / Type	Domain / Focus	Data Source / Methods	Population / Setting	Key Findings Relevant to Homeland Security
[19]	Interdisciplinary legal and technical analysis	AI law and liability	Hypothetical scenarios; expert consultation	U.S. constitutional and civil rights framework	Current U.S. law struggles to assign liability for AI harms; it proposes a "Responsible AI Legal Framework.
[20]	Narrative survey /scoping	Security & privacy of generative models	Literature synthesis	AI/ML security landscape	Generative AI can automate attacks (phishing, spoofing, and malware) but also aid defenses.
[21]	Comparative regulatory analysis	Global regulatory responses (U.S., EU, UK, China)	Policy review	International focus with U.S. component	The U.S. approach continues to lag behind the EU, where a resilience-oriented regulatory model has been proposed.
[6]	U.S. federal policy document	Responsible AI development and governance	Policy directive (Executive Order 14110)	Federal government, industry, civil society	Sets principles for AI safety, civil rights, innovation, and competition; frames AI as a national priority.
[22]	Applied cybersecurity case study	GenAI in cyber offense/defense	Analysis of attacks (jailbreaks, prompt	U.S. cybersecurity ecosystem	Identifies vulnerabilities in ChatGPT and outlines the use of GenAI for

			injection, phishing)		both attack and defense purposes.
[22]	Qualitative research article; conceptual and scenario-based analysis	Generative AI and cybersecurity: roles of AI entities, companies, agencies, and government	Four-part methodology: AI-driven code scanning, phishing email simulation, malicious domain generation, structured literature review	U.S.-based organizational and national security context (Five Below Inc., Innova Solutions) with a focus on CISA's role and critical infrastructure protection.	GenAI lowers the barrier to cybercrime, enabling phishing, ransomware, and DDoS by low-skilled actors. Highlights GenAI's defensive applications (anomaly detection, malware simulation, and automated incident response) and advocates for a U.S. AI policy framework, public–private partnerships, CISA coordination, and the establishment of a national Cyber Force.

4. Thematic Synthesis of Key Findings

4.1. Applications of Generative AI in homeland security preparedness

The literature shows that GenAI is already being used in several domains. In cybersecurity, it is applied both offensively and defensively, such as in generating phishing campaigns, automating malware, and strengthening detection capacity through synthetic training datasets [22].

In the protection of critical infrastructure, we found that large language models and agentic AI can support anomaly detection and resilience in energy, water, and transportation systems [23]. At the policy level, the U.S. government has recognized these risks and opportunities through the 2023 Executive Order on safe, secure, and trustworthy AI, which sets principles for safety, civil rights, innovation, and competition [6].

These applications highlight how homeland security actors are beginning to adopt GenAI as a potential threat vector and a preparedness tool.

4.2. Threats and barriers associated with adversarial use of GenAI

Across the studies, one clear theme that emerged was the lowered entry barrier for malicious actors. For instance, it was found that even individuals with limited technical expertise can now generate phishing emails, ransomware demands, or synthetic voices and images with relative ease [22].

Legal scholars also noted that U.S. constitutional and civil rights law, as well as liability frameworks, are poorly suited to address harms caused by AI outputs, particularly intangible harms such as discrimination, reputational damage, or privacy violations [19]. Further, deepfakes and synthetic media were identified as major risks to election security and public trust [20].

4.3. Opportunities and countermeasures

The findings show that the same capabilities that enable adversarial uses of generative AI can also be used defensively. Generative AI can help defenders improve detection systems, simulate realistic adversarial scenarios for training, as well as enhance cyber defense mechanisms and automation [23].

Policy frameworks can emphasize the importance of standardisation, such as aligning AI risk assessments with the NIST Cybersecurity framework, and strengthening partnerships between federal agencies, private industry, and research institutions [6; 21].

These measures were proposed as ways to build resilience and ensure responsible integration of GenAI into homeland security practices.

Generally, the evidence shows that while generative AI introduces new vulnerabilities to law, policy, cybersecurity, and critical infrastructure, it also presents opportunities for strengthening homeland security preparedness. Thus, the balance between these two aspects will depend on how effectively the U.S. develops adaptive regulatory frameworks, builds technical defense systems, and integrates AI into resilience and homeland security planning.

5. Discussion of key findings

This review highlights how generative AI is reshaping homeland security preparedness in the United States. The findings show a dual character of these technologies; thus, they create new vulnerabilities for law, policy, and critical systems while simultaneously offering tools for defensive innovation.

The first theme is the legal and regulatory gap. Existing liability and constitutional frameworks struggle to address the harms of AI-generated content, particularly those that are intangible or diffuse, such as discrimination, reputational damage, or misinformation [19]. This gap is compounded by the complexity of proving causation and accountability in AI systems, which are often opaque in their functioning. Without updated legal frameworks, affected individuals and organizations remain inadequately protected. This aligns with broader calls for resilience-based governance that prioritises adaptability, swift response, and recovery mechanisms [21].

Second, cybersecurity risks are increasing as generative AI lowers the barrier for malicious actors. For instance, the studies of both Dhoni & Kumar [23] and Krishnamurthy [22] revealed how phishing, ransomware, and synthetic content creation are no longer the domain of highly skilled hackers, noting how average users can now exploit GenAI tools to launch damaging attacks. This democratization of cyber capabilities poses a significant challenge to homeland security, particularly in protecting critical infrastructure. The analysis of critical national infrastructures further confirms the urgency, with Krishnamurthy [22] reporting that high-impact attacks on essential systems such as energy, water, and transport have surged in recent years. These vulnerabilities suggest that preparedness must account not only for state-sponsored actors but also for increasingly capable non-state actors.

Third, there are opportunities for countermeasures and defensive uses. Generative AI can enhance cybersecurity resilience by producing synthetic adversarial data for training, supporting anomaly detection, and automating incident response [23].

At the federal level, the Biden Administration's Executive Order (2023) provided a coordinated national policy that balances safety, innovation, and equity while advancing standards through agencies such as NIST [6]. If effectively implemented, these measures could foster collaboration between government, industry, and academia, creating the ecosystem needed for adaptive resilience.

Together, these findings suggest that the U.S. is at a crossroads, and thus, without robust legal frameworks and defensive adaptation, generative AI could amplify existing vulnerabilities. At the same time, if properly governed, these tools can strengthen preparedness, enhance the resilience of homeland security infrastructure, and build public trust.

Limitations

The review has several limitations. First, it was restricted to studies published between 2020 and 2025, which may have excluded earlier foundational work on AI and security. Second, while the focus on U.S.-based literature provides national relevance, it limits the generalizability of the findings to other geopolitical contexts where regulatory and technological landscapes differ. Third, many of the included studies relied on conceptual analysis, scenario-based exploration, or policy commentary rather than empirical testing, which constrains the strength of causal claims. Finally, given the fast pace of AI development, some insights may already be outdated by the time of publication. This further buttresses the need for continuous research and evidence updates.

Future Research

Future research should focus on empirically testing the defensive potential of generative AI tools in operational homeland security contexts. For instance, studies could evaluate how synthetic adversarial data improves resilience in intrusion detection systems or how generative models can simulate realistic cyberattack scenarios for training exercises. More interdisciplinary research is also needed to bridge the gaps between law, ethics, and technology,

particularly in refining liability frameworks and accountability mechanisms. Policy-orientated studies should explore how federal initiatives, such as the 2023 Executive Order on AI, translate into measurable improvements in preparedness and resilience across critical infrastructure sectors.

6. Conclusion

Generative AI presents both risks and opportunities for homeland security preparedness in the United States. On the one hand, it enables adversarial actors to exploit vulnerabilities in law, policy, and critical infrastructure. On the other hand, it can be used to strengthen defensive systems, support resilience planning, and automate responses to emerging threats. The U.S. government, through initiatives such as the 2023 Executive Order on AI, has begun to chart a path forward, but significant efforts are needed to close regulatory gaps and ensure the safe and responsible integration of GenAI into homeland security infrastructure. As this technology evolves, homeland security strategies must strike a balance between vigilance against misuse and proactive investment in defensive innovation.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Reddy, P., Ch, K., Sharma, K., Sharma, B., & Sharma, S. (2025). Evolution of Generative Artificial Intelligence: A Review of the Developed and Developing. Engineered Science, 35, 1529.

[2] Pantano, E., Serravalle, F., & Priporas, C. V. (2024). The Form Of AI-Driven Luxury: How Generative AI (GAI) And Large Language Models (LLMs) are transforming the Creative Process. Journal of Marketing Management, 40(17-18), 1771-1790.

[3] Salierno, G., Leonardi, L., & Cabri, G. (2025). Generative AI and Large Language Models in Industry 5.0: Shaping Smarter Sustainable Cities. Encyclopedia, 5(1), 30.

[4] Anny, D. (2025). Adversarial Attacks on Generative AI Models in Cloud Platforms: Detection and Mitigation Strategies.

[5] Yang, A., & Yang, T. A. (2024, June). Social Dangers of Generative Artificial Intelligence: Review and Guidelines. In Proceedings of the 25th Annual International Conference on Digital Government Research (pp. 654-658).

[6] Biden, Joseph R. "Executive order on the safe, secure, and trustworthy development and use of artificial intelligence." (2023).

[7] Joshi, S. (2025). Gen AI in Financial Cybersecurity: A Comprehensive Review of Architectures, Algorithms, and Regulatory Challenges. International Journal of Innovations in Science Engineering and Management, 4(3), 73-88.

[8] Zucca, M. V., & Fiorinelli, G. (2025). Regulating AI as a Cybersecurity Defense: Fighting the Misuse of Generative AI for Cyber Attacks and Cybercrime. Technology and Regulation, 2025, 247–262.

[9] Zucca, M. V., & Gaia, F. (2025). Regulating AI to combat tech-crimes: Fighting the misuse of generative AI for cyber-attacks and digital offenses. Technology and Regulation, 2025(1), 247–262.

[10] Bellavita, C. (2008). Changing Homeland Security: What is Homeland Security? Homeland Security Affairs, 4(02).

[11] Aad, S. S., & Hardey, M. (2025). How GAI Works: Fundamentals. In After Generative AI (pp. 31-53). Emerald Publishing Limited.

[12] Wach, K., Duong, C. D., Ejdys, J., Kazlauskaitė, R., Korzynski, P., Mazurek, G., & Ziemba, E. (2023). The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. Entrepreneurial Business and Economics Review, 11(2), 7-30.

[13] Yoon, S. H., Yang, S. B., & Lee, S. H. (2025). Unveiling the Pros and Cons of Generative AIServices: A Mixed-Methods Approach. Available at SSRN 4770620.

[14] Pyżalski, J. (2024, November). Challenges for Education Based on Empirical Model of GAI in Schools–What Are the Concerns of Polish Primary School Teachers? In International Conference on New Media Pedagogy (pp. 192-204). Cham: Springer Nature Switzerland.

[15] Zhou, J., Lu, Y., & Chen, Q. (2025). GAI Identity Threat: When and Why Do Individuals Feel Threatened? Information & Management, 62(2), 104093.

[16] Suleiman, A. M. (2024). Enhancing the United States Counterterrorism Policy Through Artificial Intelligence: A Comprehensive Analysis of Machine Learning Applications, Challenges, and Strategic Implications. *International Journal of Scientific Research and Modern Technology, 3*(5), 21–34.

[17] Deshpande, A. S., & Gupta, S. (2023, December). GenAI in the Cyber Kill Chain: A Comprehensive Review of Risks, Threat Operative Strategies, and Adaptive Defense Approaches. In 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-5). IEEE.

[18] Mobilio, S. B. (2024). Utilizing Generative AI to Counter Deceptive Messaging.

[19] Cheong, I., Caliskan, A., & Kohno, T. (2025). Safeguarding Human Values: Rethinking US Law for Generative AI's Societal Impacts. AI and Ethics, 5(2), 1433-1459.

[20] Bauer, L. A., & Bindschaedler, V. (2021). Generative models for security: Attacks, defenses, and opportunities. arXiv preprint arXiv:2107.10139.

[21] Bodini, M. (2024). Generative Artificial Intelligence and Regulations: Can We Plan a Resilient Journey Toward the Safe Application of Generative Artificial Intelligence? Societies, 14(12), 268.

[22] Krishnamurthy, O. (2023). Enhancing Cyber Security Enhancement through Generative AI. International Journal of Universal Science and Engineering, 9(1), 35-50.

[23] 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).