Magna Scientia Advanced Research and Reviews
eISSN: 2582-9394
Cross Ref DOI: 10.30574/msarr
Journal homepage: https://msarr.magnascientiapub.com/

(REVIEW ARTICLE)

STRENGTHENING CRITICAL INFRASTRUCTURE RESILIENCE IN THE UNITED STATES: AN INTEGRATIVE REVIEW OF STRATEGIES FOR COUNTERING POLITICAL VIOLENCE AND EXTREMIST THREATS

Juliana Popoola *

Texas Tech University.
* Corresponding Author

Magna Scientia Advanced Research and Review, 2026, 18(01), 145–151

Publication history: Received on 02 August 2026; revised on 05 October 2026; accepted on 07 October 2026

Article DOI: https://doi.org/10.30574/msarr.2026.18.1.0182

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Domestic violent extremists and state-sponsored actors' intent on disrupting democratic processes and institutions through targeted attacks on critical infrastructure, including energy, water, communications, and nuclear power plants, are an increasingly diversified and growing threat in the United States. Whilst the number of documented plots targeting infrastructure has increased since 2016, the literature is still divided into sectors of threat-specific, technical and policy studies, without an integrated synthesis that examines how threat intelligence, technical hardening, governance and community-based approaches interact in determining infrastructure resilience outcomes in the United States. This review identified and compiled peer reviewed academic papers and institutional publications from 2020 to 2026 from various databases and was thematized according to four domains; the changing threat landscape and radicalization pathways, cyber-physical security and technical hardening, governance and policy frameworks, and community and communication-based resilience strategies. The review concludes that no single intervention can ensure long-term resilience, but rather a thoughtful combination of technical, governance, and human-based strategies and also, fragmentation among federal, state, private-sector, and community groups is a key vulnerability. A multi-layered approach that includes technical hardening and human-centered prevention, is best coordinated, most defensible, and has a unified evidence base for policy design and future research.

Keywords: Critical Infrastructure Resilience, Political Violence, Domestic Extremism, Cyber-Physical Security, Homeland Security, United States

1 INTRODUCTION

Critical infrastructure encompasses the physical and cyber systems whose incapacitation or destruction would have a debilitating effect on national security, public health, or economic stability (Val et al., 2024). In the United States, 16 designated sectors; from energy grids and nuclear plants to water systems and communications networks form the operational foundation of American society, and their deliberate targeting by extremist actors has emerged as a defining national security challenge of the current decade (Panful et al., 2025; Krill & Clifford, 2022). The threat environment has grown substantially more complex, encompassing not only foreign state-sponsored cyber operations but a rising tide of domestically motivated political violence explicitly targeting infrastructure as a vehicle for societal disruption (Val et al., 2024).

The scale and ideological diversity of this threat are well documented. Krill & Clifford (2022) catalogue 79 violent extremist attack plots against U.S. critical infrastructure between 2016 and 2022, spanning white supremacist accelerationism, anti-government militia movements, and anarchist environmentalism. This view has also been extended across fifty years of domestic infrastructure terrorism, demonstrating that infrastructure targeting is a structurally persistent strategic preference across ideologically diverse traditions because of its potential to trigger failures that expose the fragility of democratic governance (Humpal, 2026). Doxsee (2023) argues that domestic violent extremism is qualitatively distinct from the foreign terrorist organization threats that post-9/11 frameworks were designed to address, requiring purpose-built analytical and institutional responses. The technical dimensions of the threat compound this challenge: critical infrastructure sectors increasingly rely on cyber-physical systems including Supervisory Control and Data Acquisition (SCADA) systems and industrial control networks that create attack surfaces exploitable by both nation-state adversaries and technically capable domestic actors (Zografopoulos et al., 2021; Panful et al., 2025). The adversarial use of generative artificial intelligence (AI) has further accelerated radicalization pathways, enabling extremist content production at unprecedented scale and personalization (Suleiman & Donkor, 2025; Nabila & Thompson, 2025).

Despite the documented severity and growth of this threat, the existing literature addresses the problem of critical infrastructure resilience in fragmented and disconnected ways. Cybersecurity studies examine threat modeling and technical hardening without integrating the human and organizational dimensions of resilience (Zografopoulos et al., 2021; Rajendran & Vyas, 2023). Extremism scholarship catalogues threat patterns without connecting them to operationally actionable protection strategies (Krill & Clifford, 2022; Doxsee, 2023). Counter-narrative and strategic communication research examines prevention interventions independently of technical hardening and governance frameworks (Bilazarian, 2020; Nabila & Thompson, 2025). Organizational and supply chain resilience literature contribute frameworks that are rarely applied to the infrastructure protection context (Adewumi et al., 2024). No existing integrative synthesis examines how threat intelligence, technical hardening, governance, and community-based strategies work or fail to work together in the specific context of extremist threats to U.S. critical infrastructure, despite growing evidence of the limitations of each stream in isolation (Krill & Clifford, 2022; Zografopoulos et al., 2021; Bilazarian, 2020; Adewumi et al., 2024). This gap is consequential; without a consolidated, integrated evidence base, policymakers design responses that address individual threat dimensions in isolation; infrastructure operators invest in technical controls without the governance and organizational culture conditions that make them effective; and community prevention programs are funded and evaluated independently of the technical and governance frameworks they must complement to produce durable resilience outcomes (Adewumi et al., 2024; Val et al., 2024; Panful et al., 2025).

This integrative review addresses that gap directly. It synthesizes evidence published between 2020 and 2026 across four thematic domains; the evolving threat landscape and radicalization pathways, cyber-physical security and technical hardening, governance and policy frameworks, and community and communication-based resilience strategies, to develop an integrated understanding of what strengthens critical infrastructure resilience against political violence and extremist threats in the United States.

2 LITERATURE SEARCH STRATEGY

This review adopted an integrative narrative approach to synthesize literature drawn from multiple academic and institutional databases, including Google Scholar, Scopus, IEEE Xplore, PubMed, the Homeland Security Digital Library, and the Program on Extremism at George Washington University. The search covered peer-reviewed journal articles, book chapters, institutional reports, and policy documents published between January 2020 and June 2026. Search terms were organized around the four thematic domains of the review and included combinations of the following: "critical infrastructure resilience," "domestic violent extremism," "political violence," "countering violent extremism," "infrastructure terrorism," "cyber-physical security," "SCADA attacks," "radicalization pathways," "counter-narrative," "strategic communication," "homeland security," "AI and extremism," "disinformation and national security," and "supply chain resilience." Retrieved sources were screened for relevance to the U.S. context and to the specific problem of politically motivated and extremist threats to critical infrastructure. International sources were included where they offered frameworks or evidence with direct applicability to the U.S. context. Sources focused exclusively on natural hazards, non-deliberate accidents, or cybersecurity incidents without a politically motivated violence dimension were excluded from the synthesis.

3 DATA SYNTHESIS

The evidence from the included literature is summarized in the following four subject sections, which are arranged according to the key domains that have been most frequently found to be indicators of critical infrastructure resilience against extremist threats and political violence. The literature was reviewed iteratively to identify each theme, and sources were assigned according to their main theoretical or empirical contribution.

3.1 Theme 1: The Evolving Threat Landscape and Radicalization Pathways

The nature and trajectory of the threat of extremism to critical infrastructure is essential to any effective strategy on how to be more resilient. Over the last fifty years, the threat environment in the United States has changed greatly, and the nature, sophistication, and goals of domestic extremist actors have also changed dramatically, posing a threat to the traditional security paradigm (Humpal, 2026). The most thorough historical overview of this development is provided by Humpal (2026), who shows that domestic infrastructure terrorism has taken place in various campaigns throughout the 1970s and 1980s, accelerated in the far-right movements of the 1990s and 2000s, and continued as a consistent, strategic preference among ideologically divergent extremist traditions today precisely for this reason. But the historical perspective is highlighted by Krill & Clifford (2022), which comes from their documentation of 79 attack plots on U.S. critical infrastructure from 2016 to 2022 and their finding that white supremacist accelerationism, anti-government militia ideology, and anarchist environmentalism all contribute to a significant portion of documented plots; they suggest that the latter three categories together are sufficient to cover the majority of the documented plots, thereby challenging the idea that domestic infrastructure terrorism is a monolithic and ideologically homogeneous phenomenon.

The threat of domestic terrorism in the transnational terrorism literature, posits that the U.S. domestic terrorism threat is qualitatively unique, and that analysis and institutionalization need to be adapted for the domestic context (Doxsee, 2023). A legal and definitional overview of threats and political violence has been documented, explaining the differences between constitutionally protected speech, threats and political violence, which are crucial for developing effective prevention and prosecution tools that are legally defensible (Declan, 2026). There has also been an examination of the public face of the threat landscape in the present study, specifically, a comparison between the threat level of terrorism and the extent to which Americans fear it, and they find that through experimental evidence, targeted messaging interventions can measurably alleviate the fear of terrorism without reducing Americans' support of appropriate security measures, with direct implications for public communication strategy (Silverman et al., 2022).

Digital environments and new technologies have significantly changed the way people become radicalized for infrastructure targeting. A recent scoping review by Suleiman & Donkor (2025) reports that extremist actors are now exploiting generative AI to generate customized radicalization materials on an unprecedented scale, thereby greatly reducing the hurdles to ideological conversion and operational planning. In security applications, however, Lo Piano (2020) points out that ethical principles, such as fairness, transparency, and accountability, that are used to design systems that utilize AI and machine learning, will need to be applied in practice when designing AI-based detection and prevention systems, to avoid perpetuating or exacerbating existing biases in threat identification. Strategic narrative and storytelling are two key mechanisms of radicalization and counter-radicalization and have been shown to be central in both processes (Nabila & Djokoto, 2025). Countries with a clear positive national narrative have significantly higher public resistance to recruitment and disinformation by extremists. In looking at the policy documents, it is reviewed that gender-blind prevention frameworks repeatedly fail to consider the gendered aspects of the pathways to violent extremism, which has a direct impact on the design of prevention programs (Skjelsbæk et al., 2020).

3.2 Theme 2: Cyber-Physical Security and Technical Hardening

Technical hardening of critical infrastructure to defend against cyber-physical attack is a bottom-up element of resilience that needs to form the foundation for more holistic governance and community-based efforts. The most comprehensive threat modeling framework for cyber-physical energy systems found in the literature is presented by Zografopoulos et al., (2021), who have systematically classified the attack vectors, risk assessment methods, security metrics and case studies in energy sector infrastructure, concluding that effective cyber-physical security needs a combination of approaches that address both the cyber and physical aspects of infrastructure, not treating them as separate security domains. Their framework is especially significant given the fact that both nation-state and domestic extremist actors have been known to use the Internet as a tool to gain access to their physical targets, a phenomenon which has been documented as a force multiplier in attacks. This creates threat scenarios that cannot be addressed by purely physical or cyber security measures.

To substantiate their threat modeling, a case-study analysis of SCADA system attacks experienced in the U.S. utility sector during the last few years was used, demonstrating that the most important difference between organizations that contained incidents and those that caused a substantial operational disruption was that security awareness was distributed throughout the operational staff rather than limited to security teams (Panful, et al., 2025). The finding has important implications for technical hardening strategy, in that it indicates that expenditure on technology for resilience without corresponding expenditure on human and organizational conditions for the technology to be effective results in systematically sub-optimal resilience outcomes. Val et al., (2024) support this conclusion by analyzing security practices for U.S. critical infrastructure defense, which show that technical measures are not enough without governance frameworks, training programs and cross-functional communications that would enable them to be effective in actual practice.

Also, an important but challenging subfield of the cyber-physical security field was explored: AI-assisted fault detection and diagnostics of nuclear power plant control systems (Bonsu & Adeoye, 2025). Their review reveals that AI-based monitoring significantly improves the time to detection of anomalous activity, including activities that could signal sabotage or insider threat, over traditional monitoring methods, and can also decrease false alarms, thus lowering the likelihood of operator alert fatigue. It works to show how the right technical hardening using AI can achieve both enhanced detection sensitivity and a more efficient operational security monitoring workload, as long as there is adequate human oversight of AI-generated alerts through governance. Rajendran & Vyas (2023) expand this research to the larger cybersecurity arena, examining the use of AI in critical infrastructure protection, and conclude that explainability, bias mitigation, and continuous model monitoring are the most important technical governance principles to achieve the success of an AI-driven security system, findings that are directly applicable to Lo Piano's (2020) ethical considerations for the use of AI in sensitive contexts.

3.3 Theme 3: Governance and Policy Frameworks

Governance mechanisms that integrate action across the disjointed federal agencies, state and local governments, private-sector infrastructure owners and community organizations are necessary to create effective resilience against these threats faced by critical infrastructure. The governance challenge is especially pronounced in the United States, where about 85% of critical infrastructure is privately owned, meaning that more robust voluntary coordination arrangements are invariably needed, and there is a structural dependency on public-private partnership (Val et al., 2024; Panful et al., 2025). The governance attributes that are most likely to predict resilience outcomes, identified by Adewumi et al., (2024) in their systematic review of pharmaceutical supply chain resilience strategies, can be directly applied to the context of critical infrastructure protection: relationship quality, information sharing norms and cross organizational trust have been shown to be the most predictive of resilience outcomes.

The governance of emerging technology for critical infrastructure protection has unique challenges and opportunities. Similar to the problem of threat detection in physical infrastructure, there has been the use of machine learning models for the task of pattern identification for terrorist financing in the U.S. financial industry, noting that ML-based models can detect a number of patterns that significantly outperforms manual attempts, and that the use of the models poses governance questions regarding transparency of the models, false positive management, and accountability for automated decisions (Boateng et al., 2025). Regulatory standards and mandatory minimum-security requirements are relevant governance mechanisms that have been seen to consistently outperform voluntary approaches in moving up the energy sector's cybersecurity baselines, which further underscores the need for regulatory mandates over industry self-regulation in high-consequence infrastructure domains (Zografopoulos et al., 2021).

Skjelsbæk et al., (2020) highlight the gender dimension of governance frameworks for violent extremism prevention, finding that policy documents in several national contexts systematically marginalize gender considerations, as opposed to mainstreaming them, when it comes to preventing terrorism and violent extremism, despite evidence that the gendered dimension is central to radicalization, recruitment and community-level prevention. The impact of this governance ‘blind spot' on the operation is that prevention programs that are not gender-informed reach a smaller group and address fewer pathways to radicalization than the evidence base indicates. Bringing a complementary legal governance point of view, Broughton (2026) examines the present constitutional and statutory context for handling threat-based political violence, and the potential for governmental overreach in implementing proactive security measures, which is in tension with civil liberty protections, as the most important governance challenge regarding infrastructure protection policy in a democratic setting.

3.4 Theme 4: Community and Communication Based Resilience Strategies

Technical hardening and governance frameworks will not be enough to create long-term resilience to politically motivated violence. The findings presented here continue to highlight the importance of complementary community-level and communication-based interventions, including counter-narrative programs, strategic communication, public resilience building, and a gender-sensitive approach to prevention. Based on lessons learned from the offline countering violent extremism (CVE) practice, Bilazarian (2020) offers foundational evidence on the effectiveness of counter-narrative interventions in the online space by examining characteristics of offline counter-narrative methods. Building on lessons learned from offline countering violent extremism (CVE) practice, Bilazarian (2020) explores characteristics of offline counter-narrative methods to assess digital counter-narrative programs, concluding that the most effective practice shares similarities with offline interventions, such as addressing legitimate grievances, using credible messengers, and delivering counter-narratives through channels that reach the ideology radicalization vulnerable population before radicalization hardens.

In the United States, Nabila & Thompson (2025) describe the importance of strategic communication in national security policy and how coherent and well-resourced strategic communication programs impact the government's ability to effectively respond to foreign influence operations and sustain public backing for legitimate security measures. They further show al. (2026) al., (2026) demonstrates that digital storytelling and visual rhetoric are effective at

enhancing public resilience to misinformation, as they show that narrative-based communication has a significant effect on creating a more enduring resistance to disinformation that substantially outperforms fact-correction approaches when it comes to public communication strategies for critical infrastructure security.

In a study that is missing from the literature on security, Silverman et al. (2022) provides experimental evidence related to the management of public fear of terrorism, which is one of the aspects of community resilience that is overlooked. Their findings show that messaging interventions that focus on threats can help lower disproportionate terrorism-related fear without eroding either support for security measures or public trust in the government, indicating that resilience communication programs need to go beyond factual content on threats to focus on the psychological and emotional aspects of public perceptions of security. There is also the need for inclusive community engagement by showing that gender-blind prevention approaches systematically exclude aspects of the radicalization process (and community assets) that would be accessed by gender-sensitive approaches (Skjelsbæk et al., 2020). These analyses collectively suggest a community resilience framework that is both technically informed, communicatively complex, and psychologically nuanced, and that accounts for and embraces the entire diversity of community members and pathways to radicalization.

3.5 Conceptual Framework

The four thematic domains synthesized in this review: the evolving threat landscape, cyber-physical security and technical hardening, governance and policy frameworks, and community and communication-based resilience strategies do not function as independent pillars but as an interdependent system in which the effectiveness of each domain is conditioned by the strength of the others. To capture this interdependency and provide an organizing structure that is actionable for policymakers and practitioners, an integrated conceptual framework was developed from the evidence base of this review. As illustrated in Figure 1, the framework positions the four thematic domains around a central commitment to critical infrastructure resilience; defined across three operational imperatives of prevention, protection, and recovery with continuous learning, intelligence sharing, and adaptive governance as the connective mechanisms that sustain the system over time. The outer feedback loop reflects the evidence that resilience is not a static condition achieved through one-time investment but a dynamic capability requiring continuous adaptation as the threat landscape, technology environment, and governance context evolve.

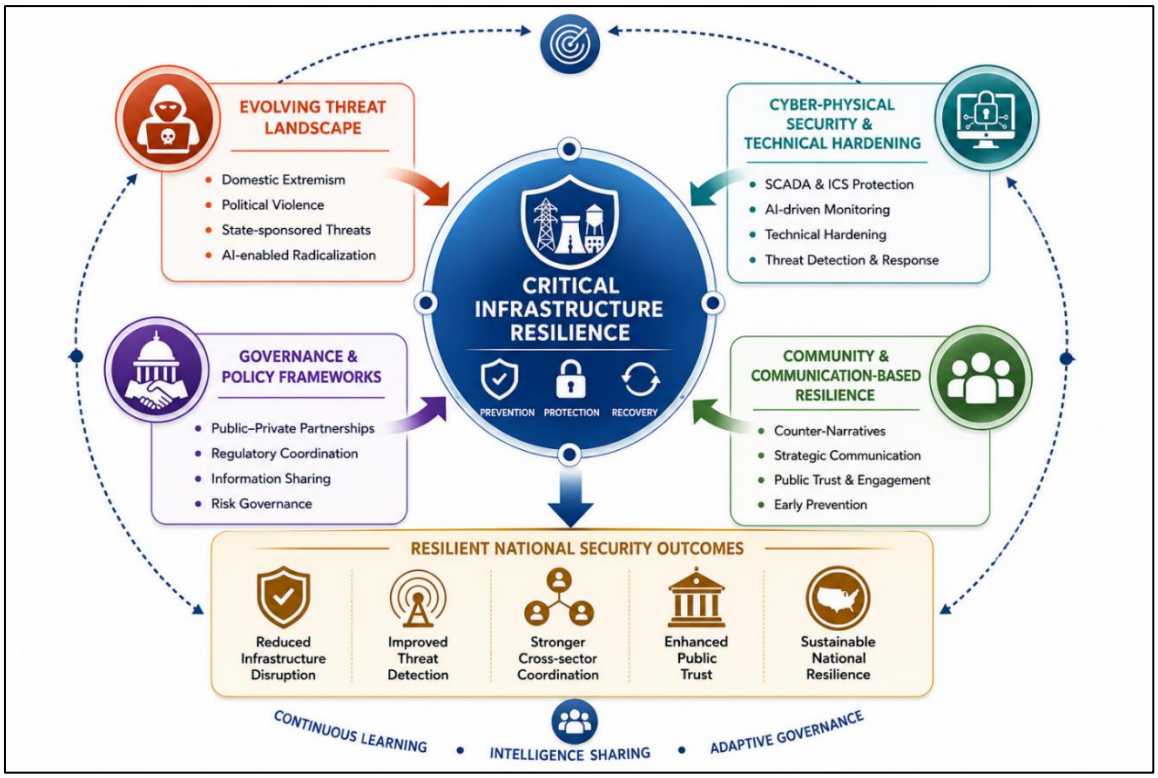


Figure 1: An Integrated Framework for Critical Infrastructure Resilience Against Political Violence and Extremist Threats in the United States

Source: Author's construct (2026).

Figure 1 demonstrates that the resilience of critical infrastructure in the U.S. against political violence and extremism necessitates simultaneous alignment across four thematic domains. To properly guide technical hardening, governance, and community measures, the ever-changing threat picture necessitates ongoing intelligence updates. For cyber-physical security measures to be operational rather than just compliant, they must be ingrained in company culture. Governance frameworks established through public-private partnerships and coordination are essential for the coherent execution of both technical and community strategies. Community resilience strategies address human factors that cannot be reached solely through technical and governance measures, particularly against extremist disinformation. Collectively, these domains yield national security outcomes aimed at minimizing infrastructure disruption and enhancing resilience. The framework's emphasis on continuous learning and adaptive governance fosters ongoing improvements in resilience rather than isolated successes.

4 CONCLUSION

This integrative review clarifies the imperative that the enhancement of critical infrastructure resilience in the United States, particularly in the face of political violence and extremist threats, necessitates the implementation of a meticulously coordinated, multi-layered strategic approach. This approach must recognize and treat threat intelligence, cyber-physical fortification, governance mechanisms, and community-oriented communication as interconnected and interdependent components, rather than as isolated or parallel issues that can be addressed independently. It is crucial to acknowledge that no singular domain is adequate on its own: for instance, the existence of technical defenses devoid of effective governance coordination inevitably results in a landscape characterized by fragmented vulnerabilities; conversely, governance efforts that lack active community involvement are ill-equipped to tackle the complex human radicalization pathways that ultimately give rise to various threats; further, communication strategies that are not grounded in technical expertise ultimately suffer from a lack of operational credibility, which is essential for fostering durable public resilience against potential threats. The fragmentation evident across different agencies, sectors, and academic disciplines stands out as the principal vulnerability that undermines efforts to enhance resilience, and thus, the imperative to address and close this fragmentation through a cohesive, integrated, and evidence-informed strategic framework emerges as the foremost priority in this endeavor. The extensive evidence base that has been systematically compiled and presented in this review serves as a consolidated foundation that is critical for informing the design of relevant policies, guiding organizational investments, and directing future research initiatives, all of which are essential for effectively meeting the multifaceted challenge posed by political violence and extremist threats

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

[1] Adewumi, G., Dada, S., Azai, J. S., & Oware, E. (2024). A systematic review of strategies for enhancing pharmaceutical supply chain resilience in the US. International Medical Science Research Journal, 4(11), 961–972.

[2] Bilazarian, T. (2020). Countering violent extremist narratives online: Lessons from offline countering violent extremism. Policy & Internet, 12(1), 46–65.

[3] Boateng, V., Amoako, E. K., Bonsu, M. A., & Oman-Amoako, M. Assessing the impact of machine learning model on identifying terrorism financing patterns within the US financial industry.

[4] Bonsu, J. O., & Adeoye, M. B. (2025). AI-driven fault detection and diagnostics in nuclear power plant control systems: A review. Journal of Engineering and Computer Sciences, 4(9), 552–559.

[5] Broughton, J. R. (2026). Threats and political violence. Nevada Law Journal, 26(3), 685.

[6] Doxsee, C. (2023). The heightened threat of US domestic terrorism. In Routledge handbook of transnational terrorism (pp. 197–207). Routledge.

[7] Humpal, J. (2026). From earth liberation to accelerationism: A high-level review of fifty years of domestic infrastructure terrorism. CTC Sentinel, 19(3), 26–34.

[8] Krill, I., & Clifford, B. (2022). Mayhem, murder, and misdirection: Violent extremist attack plots against critical infrastructure in the United States, 2016–2022. Program on Extremism at George Washington University.

[9] Lo Piano, S. (2020). Ethical principles in machine learning and artificial intelligence: Cases from the field and possible ways forward. Humanities and Social Sciences Communications, 7(1), 9.

[10] Nabila, M. H., & Djokoto, N. K. (2025). Narratives that build nations: Storytelling as a strategic tool against disinformation in the United States. Journal of Education and Sociology, 4(10), 29–37.

[11] Nabila, M. H., & Thompson, M. (2025a). Countering foreign influence: The role of strategic communications in national security policy making in the United States. Journal of Arts Humanities and Social Sciences, 4(9), 22–30.

[12] Nabila, M. H., & Thompson, M. (2025b). The impact of disinformation on national security policymaking: A review. EPRA International Journal of Multidisciplinary Research, 11(6), 1893–1894.

[13] Okai, A., Ohemeng, A., & Thompson, M. (2026). The role of digital storytelling and visual rhetoric in national security communication: Strengthening public resilience against misinformation in the United States.

[14] Panful, B., Apaflo, B., & Hutchful, N. (2025). Cyber-physical systems under threat: A case-study review of recent SCADA attacks in the US utility sector. Journal of Engineering and Computer Sciences, 4(12), 104–117.

[15] Rajendran, R. M., & Vyas, B. (2023). Cyber security threat and its prevention through artificial intelligence technology. International Journal for Multidisciplinary Research, 5(6), 1–18.

[16] Silverman, D., Kent, D., & Gelpi, C. (2022). Putting terror in its place: An experiment on mitigating fears of terrorism among the American public. Journal of Conflict Resolution, 66(2), 191–216.

[17] Skjelsbæk, I., Hansen, J. M., & Lorentzen, J. (2020). Hopes and misguided expectations: How policy documents frame gender in efforts at preventing terrorism and violent extremism. Politics, Religion & Ideology, 21(4), 469–486.

[18] Suleiman, A. M., & Donkor, A. A. (2025). Strengthening homeland security preparedness against adversarial use of generative AI in the United States: A scoping review. World Journal of Advanced Research and Reviews, 28(2), 1169–1175.

[19] Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening cybersecurity measures for the defense of critical infrastructure in the United States. Asian Journal of Research in Computer Science, 17(11), 25–45.

[20] Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775–29818.