

Countering Cross-Border Radicalization Pipelines: A Comprehensive Analysis of How Foreign Terrorist Ideologies Amplify Domestic Extremist Violence in the US

Juliana G. Popoola¹ and Clement Aryee²

¹Texas Tech University, USA

²Department of Sociology, Kwame Nkrumah University of Science and Technology, Ghana

Abstract: Online platforms have empowered foreign terrorist organizations to systematically spread ideologies across borders, creating radicalization pipelines that amplify domestic extremist violence in the United States. This comprehensive review examined empirical literature from the last five years to demonstrate how foreign terrorist narratives penetrate and amplify domestic extremism in the U.S. Findings reveal that foreign groups exploit online platforms and socio-political grievances to radicalize susceptible populations. Critically, reciprocal radicalization cycles emerge between disparate extremist movements, enabling ideological cross-pollination and tactical adaptation. Internet-facilitated contagion effects accelerate violence frequency and severity as celebrated foreign attacks inspire domestic imitations. Challenges to counter-terrorism efforts identified included the dynamic and adaptive nature of extremist groups, the rapid evolution of digital platforms, the continuous emergence of new communication technologies, the inherent difficulties in distinguishing between legitimate online discourses and radicalizing content, and the absence of a unified international legal framework. Effectively countering these transnational threats requires multifaceted approaches integrating international intelligence sharing, community resilience programs, and psychological understanding of radicalization pathways. Traditional counter-terrorism strategies prove insufficient against these evolving, decentralized threats demanding comprehensive, interdisciplinary interventions.

Keywords: Cross-border radicalization, domestic extremism, terrorist ideologies, online radicalization pipelines, United States.

INTRODUCTION

The rapid integration of digital technologies, comprising the internet, the Internet of Things, and various social media platforms, has fundamentally reshaped global connectivity, simultaneously creating unprecedented avenues for information dissemination and the spread of evolving cyber threats, particularly in the context of terrorism and extremism (Montasari, 2024). Digital landscape, characterized by an extensive array of extremist digital spaces, facilitates the amplification of radical ideologies and the incitement of political violence, often experimented by terrorist organizations, state actors, or individuals (Baele & Brace, 2025).

The interconnectedness unknowingly provides malicious actors, including extremist organizations, with sophisticated methods to access potential recruits and pass their agendas onto them, thereby expanding their reach beyond geographical boundaries (Montasari, 2024; Zahrah *et al.*, 2020). Particularly evident is the strategic shift by extremist organizations towards online platforms for radicalization and recruitment, transforming the internet into a crucial field for ideological warfare (Winter *et al.*, 2020; Montasari, 2024). For instance, the accessibility and anonymity offered by some of these digital platforms enable extremist narratives to transcend

borders, influencing domestic extremist groups and amplifying the potential for violence within nations, including the United States (Afzal *et al.*, 2024).

Digital transformation has fostered virtual extremism, where the boundaries between physical and digital radicalization processes become increasingly unclear. The 2017 London Bridge attacker case buttresses this view, as Youssef Zaghba, was radicalized through prolonged online contact before acting in the physical world (Monaghan, 2019). The pervasive influence is further entrenched by the deliberate use of social media influencers by terrorist groups to spread propaganda and recruit individuals, often targeting younger generations through engaging text, images, audio, and video content (Robinson, 2022; Lewinsky *et al.*, 2024). Such sophisticated online engagement has enabled extremist movements, particularly right-wing groups, to exploit digital communication tools for mobilization, sustenance, and propagation of their activities, gaining significant policy attention in recent years due to the amplified threat posed by groups like ISIS and Q-Anon (Marwick *et al.*, 2022).

This digital evolution has led to a media morphosis of terrorism, where the medium itself becomes an asymmetric weapon, enabling a much greater capacity for spreading radicalization and transforming the internet into a perpetual hub of hate and violence (Antinori, 2023). That is, the internet functions not only as a tool for propaganda but as a comprehensive operational infrastructure, enabling extremist organizers to communicate, plan attacks, secure funding, gather intelligence, and actively radicalize and train new supporters.

Despite the well-documented rapid spread of online extremism, a gap exists in the understanding of the specific mechanisms through which foreign terrorist ideologies, originating from established international terrorist organizations, state-sponsored actors, and transnational ideological movements directly and indirectly infiltrate and amplify domestic extremist violence within the United States. Considering this gap, the review investigates the mechanisms through which foreign terrorist ideologies are integrated into domestic extremist narratives within the United States, analysing the resulting amplification of violence and its implications for US national security.

METHODS

The review examined the relationship between cross-border radicalization and domestic extremist violence in the United States. It comprehensively searched academic databases using keywords like "cross-border radicalization," "foreign influence," "domestic extremism," "online radicalization," and "social media." Inclusion criteria prioritized empirical studies published within the last five years that addressed foreign terrorist ideological influence on U.S. domestic extremism. Following the initial screening, abstracts and full texts were evaluated against predetermined criteria by multiple reviewers to ensure relevance and minimize bias. Data extraction focused on methodologies, theoretical frameworks, and empirical findings. Synthesis involved thematic analysis to identify patterns, convergences, and gaps in the literature, with particular attention to studies employing content analysis to uncover latent meanings in radicalization narratives and behaviors.

FINDINGS

Pipelines of Foreign Terrorist Ideology Transmission

One primary mechanism by which foreign terrorists transmit their ideologies involves foreign

terrorist organizations strategically using online platforms to disseminate their ideological content, thereby transcending geographical boundaries and directly reaching susceptible individuals in the United States (Villa-Turek *et al.*, 2024). This digital propagation leverages social media, encrypted messaging applications, and dedicated online forums to share propaganda, recruitment materials, and tactical guidance, effectively creating a virtual pipeline for radicalization (Villa-Turek *et al.*, 2024; Meena *et al.*, 2025).

Foreign terrorist groups often exploit moral intuitions and existing sociopolitical grievances by employing compelling narratives and visual media to connect with potential recruits and justify violence (Akram & Nasar, 2023). The digital influence is often compounded by the rapid evolution of online communication technologies, which enable real-time interaction and personalized ideological brainwashing (Ibrahim & Attia, 2025). These tactics often leverage highly prominent socio-political issues, mirroring existing domestic right-wing extremist ideologies, which have seen a significant increase in violence since 9/11 (Bhangoo, *et al.*, 2024). The emotional arousal associated with these overseas conflicts, coupled with the presentation of extremist role models, further inspires emulation and offers practical examples that validate the necessity of armed resistance championed by extremist ideologies (Schuurman & Carthy, 2023). Moreover, the strategic framing of foreign conflicts as existential battles, often infused with religious or nationalistic passion, provides a compelling framework through which domestic extremists can rationalize their violent aspirations and actions (Lahnala *et al.*, 2025). Further complicating this process is the fact that the spread of such ideologies can traverse different movements, allowing for the diffusion of ideas and techniques that inspire or shape terrorist acts across various political leanings (Malthaner *et al.*, 2024). This cross-pollination of extremist narratives and operational tactics between different ideological camps presents a significant challenge to counter-radicalization efforts, as the boundaries between distinct extremist movements become increasingly obscured.

Pathways to Domestic Extremist Violence Amplification

Domestic extremist violence amplification often manifests through a process of reciprocal radicalization, where the rhetoric and actions of foreign terrorist groups are mirrored by domestic

extremists, eventually leading to a self-reinforcing cycle of violence and ideological escalation (Marwick *et al.*, 2022). This mechanism not only legitimizes violent acts but also intensifies the perceived threat, thereby fueling further radicalization within domestic contexts (Schumann *et al.*, 2022). For instance, despite their supposed opposition, far right and jihadi groups often utilize each other's destructive visions and actions to recruit members and justify violent escalation, illustrating a shared deceitful approach and a focus on an out-group enemy (Marwick *et al.*, 2022). This symbiotic relationship, wherein each extremist faction inadvertently bolsters the other's narrative of existential threat, creates a volatile environment ready for the amplification of domestic extremist violence (Kristinsdóttir *et al.*, 2025).

Furthermore, the propagation of foreign terrorist ideologies often provides domestic extremists with a sophisticated operational framework, including tactics, targets, and methods, which can then be adapted to the local context (Gaibulloev & Sandler, 2023). This adaptation frequently involves the reinterpretation of foreign narratives to align with domestic grievances, thereby making these imported ideologies more noticeable and compelling to a local audience (Malthaner *et al.*, 2024). The interplay between these global and local narratives can lead to an acceleration of radicalization processes, as individuals are exposed to a broader spectrum of justifications and perceived mandates for violence. Moreover, this transnational exchange has been shown to foster a contagion and copycat effect, where successful foreign attacks are celebrated online and inspire similar acts of violence domestically, thereby escalating the frequency and severity of extremist incidents (Kupper *et al.*, 2022). This underscores the critical role of the internet in mobilizing, sustaining, and propagating extremist activity in the U.S.

Evolution of Radicalization Pipelines

The convergence of tactics and narratives between disparate extremist groups, such as white supremacists and jihadists, makes efforts to disrupt radicalization pipelines difficult, as they increasingly copy each other's organizational structures and propaganda modules (Koch *et al.*, 2024). Indeed, the ideological similarities between Salafi-jihadism and white supremacist extremism, particularly in their shared traits and political outlooks, present a significant challenge to conventional counter-terrorism frameworks

(Clifford & Meleagrou-Hitchens, 2022). This necessitates a comprehensive approach that recognizes the interconnectedness of these threats and addresses the underlying grievances and ideological currents that fuel both domestic and foreign extremist movements.

Understanding the pathways through which individuals become radicalized, whether through online exposure to foreign ideologies or direct engagement with transnational networks, is crucial for developing effective prevention and intervention programs (Ging *et al.*, 2025). This requires acknowledging that threats can dissociate from their agents, interacting to form a broader threat without requiring central leadership, and that these threats often socialize, creating complex, multi-layered networks (Zamir & Kaunert 2025). A nuanced understanding of this dissociation is essential for developing targeted interventions that address the specific vulnerabilities and influences driving individuals towards extremist ideologies, thereby fortifying societal resilience against cross-border radicalization. Such an approach must therefore integrate advanced data science techniques to unravel the complex connections underpinning these modern movements, especially as many Western powers often over-focus on foreign Islamic threats while neglecting homegrown fascist threats veiled as the Alt-Right (Hughes *et al.*, 2022).

According to Hoverd *et al.*, (2022) this disparity in often overlooks how online platforms and recommendation algorithms contribute significantly to radicalization, sometimes inadvertently connecting individuals to existing hate groups through suggested content. This underscores the critical need for interdisciplinary research combining computational analyses of online behavior with psychological theories of vulnerability to extremism, thereby enabling a more robust understanding of radicalization pathways. It will involve mapping the intricate networks of ideological transmission and identifying critical junctures where interventions can most effectively disrupt the radicalization process, particularly through proactive counter-narratives and strategic de-platforming initiatives.

Challenges in Identifying and Disrupting Pipelines

A crucial challenge is the dynamic and adaptive nature of extremist groups, which includes their sophisticated use of encrypted communication platforms and the legal and ethical complexities

associated with monitoring online activities across international borders (Herath & Whittaker, 2023). The rapid evolution of digital platforms and the continuous emergence of new communication technologies also present an ongoing cat-and-mouse game for authorities attempting to keep pace with extremist innovation (Winkler, 2025).

Additionally, the inherent difficulties in distinguishing between legitimate online discourses and radicalizing content, coupled with civil liberty concerns, frequently impede proactive intervention efforts (Farrand, 2023). Another persistent challenge is the absence of a unified international legal framework for prosecuting individuals involved in cross-border radicalization, hindering coordinated efforts to dismantle these pipelines effectively (Magaji, 2024; Emmanuel *et al.*, 2025).

Consequently, a deeper understanding of the societal, psychological, and technological factors that contribute to radicalization is essential for developing effective countermeasures. For instance, the widespread use of digital technologies, including social media platforms, has significantly transformed the landscape of terrorism and extremism, necessitating novel approaches to counter these evolving threats (Montasari, 2024). This includes addressing the challenges of tracking the dynamic spread of extremist ideologies across disparate platforms and understanding how users become involved through algorithmic, ideological, and psychosocial radicalization processes.

DISCUSSION

The literature reveals that the narratives from international terrorist groups, such as ISIS or al-Qaeda, are reinterpreted and adopted by domestic extremist groups to legitimize their grievances and justify violence within the U.S context (Motta & Succi Junior, 2024). This adaptation often involves tailoring universalistic ideological tenets to resonate with specific local issues, such as racial tensions, anti-government sentiments, or economic anxieties, thereby creating a powerful hybrid ideology that appeals to a broader base of disaffected individuals.

Furthermore, the online dissemination of these adapted foreign ideologies through social media platforms and encrypted channels accelerates their reach and influence, allowing for rapid ideation and mobilization among geographically dispersed domestic extremists (Kupper *et al.*, 2022; Marwick

et al., 2022). The pervasive nature of the internet, coupled with the advanced use of propaganda, has enabled a decentralized approach to radicalization, making traditional counter-terrorism strategies less effective against these evolving threats (Kaur, 2025). This dynamic interplay between foreign narratives and domestic grievances necessitates a robust analytical framework capable of discerning the causal links and feedback loops inherent in the radicalization process.

Indeed, effective counter-radicalization programs require a nuanced understanding of these internet and social media components of violent extremism, moving beyond superficial interpretations to address the complex interplay of digital and physical spaces. This includes examining how collective grievance, amplified by online radicalization, serves as a significant driver for the propagation and adoption of extremist ideologies, subsequently leading to acts of violence (Binder & Kenyon, 2022; Corner *et al.*, 2023). Specifically, it is imperative to investigate how individuals' exposure to narratives of group victimization, even if not directly experienced, can evolve into personal grievances that fuel violent behavior, especially when amplified by online echo chambers.

Policy Implications for Counter-Radicalization Efforts

The findings of this review call for enhancing international intelligence sharing and cybersecurity measures to implement community-based resilience programs that address the root causes of radicalization. This requires a comprehensive understanding of factors leading to exposure to extremist content, including social influence, social selection, and self-selection, to effectively disentangle the causes of political aggression.

Furthermore, given the increasing political polarization globally, policymakers must contend with stronger partisan social identities that impede reconciliation and amplify the risk of negative trigger events facilitating support for aggressive politics. Therefore, interventions should consider both dispositional factors, such as an individual's openness to new experiences, and situational elements, like the availability of propagandistic narratives, to develop targeted strategies that reduce vulnerability to radicalization.

Additionally, effective policies must acknowledge the epistemological challenges in studying radicalization, focusing on observable shifts towards extreme ideologies and support for violent actors rather than solely on engagement in violence itself.

CONCLUSION

This review has highlighted the complex interplay between foreign terrorist ideologies and domestic extremist violence in the US, underscoring the transnational nature of radicalization pipelines. It highlighted the critical need for a multifaceted approach that transcends traditional counterterrorism measures to effectively mitigate this evolving threat. This involves not only technological solutions but also a deep understanding of the psychological and sociological underpinnings of violent extremism.

REFERENCES

1. Afzal, J., Yongmei, C., Fatima, A., and Noor, A. "Review of Various Aspects of Digital Violence." *Journal of Engineering, Science and Technological Trends* 1.2 (2024).
2. Akram, M., and Nasar, A. "Systematic Review of Radicalization through Social Media." *Ege Academic Review* 23.2 (2023): 279–296.
3. Antinori, A. "Online Research Techniques and Methodologies in the Study of Left-Wing Extremism." In *The Palgrave Handbook of Left-Wing Extremism, Volume 1*. Cham: Springer International Publishing, 2023. 157–169.
4. Baele, S. J., Brace, L., and Naserian, E. "More Is More: Scaling up Online Extremism and Terrorism Research with Computer Vision." *Perspectives on Terrorism* 19.1 (2025).
5. Bhangoo, A. S., Cho, S., and Hashmi, R. S. "Understanding the Rise of Right-Wing Crimes, and Intergroup Threat Theory: Global Perspective & Case Studies." *Advanced Journal of Social Science* 13.1 (2024): 88–102.
6. Binder, J. F., and Kenyon, J. "Terrorism and the Internet: How Dangerous Is Online Radicalization?" *Frontiers in Psychology* 13 (2022): 997390.
7. Clifford, B., and Meleagrou-Hitchens, A. "Imitators or Innovators? Comparing Salafi-Jihadist and White Supremacist Attack Planning in the United States." (2022).
8. Corner, E., McEwan, T., and Logan, C. "Grievance-Fueled Violence: Conceptual and Empirical Developments." *Frontiers in Psychology* 14 (2023): 1177705.
9. Emmanuel, O. K., Aria, J., Jose, D., and Diego, C. "Blurring Boundaries: The Interplay between Terrorism and Organized Crime in Global Security." (2025).
10. Farrand, B. "'Is This a Hate Speech?' The Difficulty in Combating Radicalisation in Coded Communications on Social Media Platforms." *European Journal on Criminal Policy and Research* 29.3 (2023): 477–493.
11. Gaibulloev, K., and Sandler, T. "Determinants of Home-Base Attacks by Terrorist Groups." In *On Terrorist Groups*. Routledge, 2023. 8–27.
12. Ging, D., Baele, S., Brace, L., Long, S., and Murphy, S. "Aesthetics of Misogyny and the Repulsive Gaze: Worldview, Affect, and Ideology in Incel Imagery." *New Media & Society* (2025).
13. Herath, C., and Whittaker, J. "Online Radicalisation: Moving beyond a Simple Dichotomy." *Terrorism and Political Violence* 35.5 (2023): 1027–1048.
14. Hoverd, W., den Heyer, G., and de Terte, I. "Religion and Terrorism: What Can We Learn from the State Policy Responses to the Christchurch Mosque Shootings?" In *Crime, Criminal Justice and Religion*. Routledge, 2022. 208–221.
15. Hughes, B., Jones, D., and Amarasingam, A. "Ecofascism: An Examination of the Far-Right/Ecology Nexus in the Online Space." *Terrorism and Political Violence* 34.5 (2022): 997–1023.
16. Ibrahim, N. T., and Attia, N. A. "The Impact of Disinformation Generated by AI on Democracy Case Studies: The US Presidential Elections in 2016 & 2024." *Review of Economics and Political Science* (2025): 1–16.
17. Kaur, H. "The Evolution of Terrorism in Digital Age: Cyber Jihad and Emerging Threats." *International Journal of Multidisciplinary Education Research* 14.1 (2025): 3.
18. Kaur, H. "The Evolution of Terrorism in Digital Age: Cyber Jihad and Emerging Threats." *International Journal of Multidisciplinary Education Research* 14.1 (2025): 3.
19. Koch, A., Nahon, K., and Moghadam, A. "White Jihad: How White Supremacists Adopt Jihadi Narratives, Aesthetics, and Tactics." *Terrorism and Political Violence* 36.7 (2024): 919–943.
20. Kristinsdottir, K., Ebner, J., and Whitehouse, H. "Extreme Overvalued Beliefs and

- Identities: Revisiting the Drivers of Violent Extremism." *Frontiers in Psychology* 16 (2025): 1556919.
21. Kupper, J., Christensen, T. K., Wing, D., Hurt, M., Schumacher, M., and Meloy, R. "The Contagion and Copycat Effect in Transnational Far-Right Terrorism." *Perspectives on Terrorism* 16.4 (2022): 4–26.
 22. Lahnala, A., Varadarajan, V., Flek, L., Schwartz, H. A., and Boyd, R. L. "Unifying the Extremes: Developing a Unified Model for Detecting and Predicting Extremist Traits and Radicalization." In *Proceedings of the International AAAI Conference on Web and Social Media* 19 (2025): 1051–1067.
 23. Lewinsky, D., Te'eni, D., Yahav-Shenberger, I., Schwartz, D. G., Silverman, G., and Mann, Y. "Detecting Terrorist Influencers Using Reciprocal Human-Machine Learning: The Case of Militant Jihadist Da'wa on the Darknet." *Humanities and Social Sciences Communications* 11.1 (2024): 1–11.
 24. Magaji, B. M. "Strengthening Cross-Border Legal Frameworks: Collaborative Approaches to Enhancing Security and Addressing Humanitarian Challenges in North-East Nigeria." *Islamic University in Uganda Journal of Comparative Law* 8.1 (2024): 51–56.
 25. Malthaner, S., O'Connor, F., and Lindekilde, L. "Scattered Attacks: The Collective Dynamics of Lone-Actor Terrorism." *Perspectives on Politics* 22.2 (2024): 463–480.
 26. Marwick, A., Clancy, B., and Furl, K. "Far-Right Online Radicalization: A Review of the Literature." *The Bulletin of Technology & Public Life* (2022).
 27. Meena, G., Raha, S., Selvakumar, P., Satyanarayana, P., and Vats, C. "The Role of AI in Combatting Extremism and Radicalization on Social Media." In *Ethical AI Solutions for Addressing Social Media Influence and Hate Speech*. IGI Global Scientific Publishing, 2025. 63–90.
 28. Monaghan, A. "The Rise of Low-Tech Terrorist Attacks in Europe." In *Organized Crime and Terrorist Networks*. Routledge, 2019. 78–99.
 29. Montasari, R. "Machine Learning and Deep Learning Techniques in Countering Cyberterrorism." In *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses*. Cham: Springer International Publishing, 2024. 135–158.
 30. Montasari, R. "The Impact of Technology on Radicalisation to Violent Extremism and Terrorism in the Contemporary Security Landscape." In *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses*. Cham: Springer International Publishing, 2024. 109–133.
 31. Motta, B., and Succi Junior, D. P. "Legitimation through Collectivization: Al Qaeda and U.S. Discourses on the Use of Force." *Studies in Conflict & Terrorism* 47.3 (2024): 301–320.
 32. Robinson, M. M. "Social Media Recruitment and Online Propaganda by Extremist Groups." (2022).
 33. Schumann, S., Rottweiler, B., and Gill, P. "Assessing the Relationship between Terrorist Attacks against Ingroup or Outgroup Members and Public Support for Terrorism." *Frontiers in Psychology* 13 (2022): 778714.
 34. Schuurman, B., and Carthy, S. L. "Understanding (Non) Involvement in Terrorist Violence: What Sets Extremists Who Use Terrorist Violence Apart from Those Who Do Not?" *Criminology & Public Policy* 23.1 (2024): 119–152.
 35. Villa-Turek, E., Abhari, R., Nisbet, E. C., Xu, Y., and Lokmanoglu, A. D. "Transnational Network Dynamics of Problematic Information Diffusion." *arXiv Preprint* (2024): arXiv:2404.01467.
 36. Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., and Fürst, J. "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counterstrategies." *International Journal of Conflict and Violence* 14 (2020): 1–20.
 37. Winkler, C. "Gaming and Extremism. *The Radicalization of Digital Playgrounds* by Linda Schlegel and Rachel Kowert." Routledge, 2024.
 38. Zahrah, F., Nurse, J. R., and Goldsmith, M. "#ISIS vs #ActionCounterTerrorism: A Computational Analysis of Extremist and Counter-Extremist Twitter Narratives." In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2020): 438–447.
 39. Zamir, M., and Kaunert, C. "Radicalisation and Counter-Terrorism—Reviewing the Problems in Strategic Communications Role in Counterterrorism." In *Strategic Communications' Role in Counterterrorism*:

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Popoola, J. G. and Aryee, C " Countering Cross-Border Radicalization Pipelines: A Comprehensive Analysis of How Foreign Terrorist Ideologies Amplify Domestic Extremist Violence in the US." *Sarcouncil journal of Arts humanities and social sciences* 5.2 (2026): pp 5-11.