Journal of Political Science and International Relationship (JPSIR)

ISSN: 3065-6125 (ONLINE)

VOLUME 2ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

Journal of Political Science and International Relationship (JPSIR)

Volume 2 Issue 1, Year 2025
ISSN: 3065-6125 (Online)
DOI: https://doi.org/10.54536/jpsir.v2i1.5799
https://journals.e-palli.com/home/index.php/jpsir

Social Media and the Spread of Global Terrorism and Criminal Activities: A Critical Review

Wilfred Oritsesan Olley[1*], Joseph Omoh Ikerodah[2]

Article Information

Received: July 24, 2025

Accepted: August 29, 2025

Published: September 23, 2025

Keywords

Crime, Cybercrime, Radicalization, Social Media, Terrorism

ABSTRACT

This paper is a critical analysis of how social media can be used to intensify terrorism and organized crime from 2020 to 2025. Although the transformation of international communication and sociopolitical practices through digital platforms has proven to be influential, unregulated, and immediate, along with boundary issues, has created new breeding grounds for harmful use. Terrorist groups and criminal organizations (such as cartels, trafficking networks, and cybercrime gangs) utilize artificial intelligence, deepfake technology, encrypted communications, and newer alt-tech platforms to carry out recruitment, spread propaganda, organize activities, and secure financing. Recent incidents of fraud show that synthetic media is being used in terror finance scams, impersonation, and psychological operations as tools of psychological warfare, as well as bots built on AI to amplify narratives automatically. The paper consolidates empirical evidence on the psychological and social effects of repeated exposure to inhumane content, with a particular focus on youth, noting correlations with anxiety, polarization, distrust, and susceptibility to radicalization. It also examines the potential for online hate campaigns to escalate into real-world violence, which erodes public trust and weakens democratic institutions. The available countermeasures, such as algorithmic content moderation, rapid removal policies, and the development of international regulatory frameworks, are evaluated, and it is determined that their effectiveness is limited due to cross-jurisdictional enforcement challenges, civil liberties concerns, and the migration of hostile actors to less traceable territories. Based on interdisciplinary research and institutional reports, the review underscores the need for comprehensive, stewardship-oriented efforts that avoid fragmentation, apartheid-inspired policies, or rights violations. The recommended priority actions include implementing evidence-based measures, enhancing cross-border cooperation, and adopting ethical governance approaches to address the evolving cyber-physical landscape without compromising democratic rights.

INTRODUCTION

Social media platforms like Facebook, X (formerly Twitter), YouTube, WhatsApp, Instagram, and Telegram now form the backbone of global digital life. With over five billion users worldwide, these platforms enable instant communication, economic transactions, social mobilization, and political action (Alnaqbi, 2025; Arcila Calderón *et al.,* 2024). However, the very qualities that drive social progress, openness, anonymity, transnational reach, and algorithmic amplification, are actively exploited by terrorist and criminal groups (Zeiger & Gyte, 2023; Yumitro, 2023). Recent years have seen a sharp rise in online radicalization, recruitment by violent extremist groups, organized cybercrime, coordinated hate speech resulting in real-world violence, and illicit fundraising through cryptocurrencies, all facilitated or heightened by social media's architecture and algorithms (Binder *et al.,* 2022; Zhou, 2024). The COVID-19 pandemic further accelerated these trends by shifting a larger share of social, economic, and ideological engagement into virtual spaces (Näsi *et al.,* 2021). At the same time, increasing legislative and technological challenges, such as encrypted messaging, deepfake media, and regulatory differences, have made it harder for governments, civil society, and tech companies to respond effectively. Overly aggressive interventions risk violating civil liberties and privacy, while too little regulation leaves societies vulnerable to evolving and more sophisticated threats (Gorwa, 2023; ICCT, 2023).

This article aims to provide a critical, evidence-based examination of the role of social media in the spread of terrorism and criminal activities. Specific objectives include:

1. Analysing how terrorists and criminal actors utilize social media for recruitment, propaganda, and operational secrecy.
2. Assessing the impact of emerging technologies (AI, deepfakes, encrypted communications) on the threat landscape.
3. Evaluating policy, technological, and community interventions.
4. Identifying ethical, legal, and research challenges.
5. Proposing concrete recommendations for governments, technology providers, law enforcement, and civil society.

The article is organized into the following sections: (2) Literature Review, (3) Methodology, (4) Mechanisms of Exploitation, (5) Case Studies and Trends, (6)

[1] Department of Mass Communication, Edo State University, Iyamho, Nigeria
[2] Department of Journalism, University of Colorado, Boulder, United States
[*] Corresponding author's e-mail: olley.wilfred@edouniversity.edu.ng

Technological Developments, (7) Impact Analysis, (8) Discussion, (9) Recommendations, and (10) Conclusion.

LITERATURE REVIEW

Dual Nature of Social Media

Recent studies by Alnaqbi (2025) and Näsi *et al.* (2021) depict social media as a paradoxical force in modern society. These platforms have redefined the global public sphere, reducing barriers to political engagement and creating new spaces for civic participation. Social media provides marginalized and dissenting voices with channels to challenge power structures and spark grassroots movements, even within authoritarian regimes. Digital networks allow communities to form beyond traditional boundaries, fostering solidarities and alliances that would otherwise be unimaginable. Social media has contributed to overturning information monopolies in most cases, real-time mobilization and organization, and the creation of access to the public debate in many instances. Nevertheless, this two-sided organizational system also brings in weaknesses. Arcila Calderon *et al.* (2024) and Zeiger and Gyte (2023) describe the potential evil aims of the potent instruments that turn social media into a machine of democratization. The acceleration of information dissemination and the potential for content to go viral are used by criminal and extremist groups. Social media infrastructure allows these actors to use it as a weapon to target propaganda delivery, illegal activity coordination, and the recruitment of supporters beyond borders. Hate speech, incitement to violence, and disinformation are free to spread, amplified by algorithms that increase engagement.

So, what makes social media a revolutionary medium of democratic expression turns out also to be another ideal crop-land for developing security threats that develop at a quicker rate than regulatory and social adaptations. What emerges is the digital frontier full of hope and danger, as the instruments of freedom are also mills of bondage (Ate, *et al.,* 2024).

Online Radicalization

Since 2020, the importance of social media in the radicalization of the youth and marginalized groups has been a greater topic of research. According to Binder *et al.* (2022) and Bright *et al.* (2021), the nature of extremist recruitment and mobilization is also affected by social media because it makes access to radical ideologies in remote areas far easier. The platforms provide a sense of connection and community for those who feel excluded from mainstream society. Online networks serve as alternatives to the traditional social environments, and in the case of the younger generation, forums, messaging services, and video platforms are the places where exposure to and playing around with extremist ideologies becomes widespread.

Social media architecture also leads to the faster prevalence of these pathways. Yumitro (2023) points out that the echo chambers and filter bubbles have been created when the interactions of a user are facilitated by algorithms reflecting the useris existing thoughts and delivering their content to them. The repetition of the source restricts the exposure of the users to different views, further strengthening tightly-knit tendencies and reinforcing the in-group versus out-group differences. As Ghosh (2025) notes, the effects of algorithmic curation not only aggravate this aspect but also encourage more divisive or sensational (or polarizing) content being ranked higher, as this kind of material tends to have more engagement. In susceptible people, these digital echo chambers reinforce and feed prejudices and give them the feeling of legal legitimacy from their peers. This, in turn, excludes outsiders even more.

The sort of environment established favours radicalization. Individuals are engaged in groups that are closed online, in which extreme views are tolerated and violence might even be justified or heroic. The speed at which these mechanisms occur exceeds the majority of prevention measures, and society is scrambling to follow the continually evolving strategies of internet extremists. To sum up, there is a psychological vulnerability, social exclusion, and algorithmic reinforcement, which have treated social media as a trigger and accelerant of radicalization after 2020.

Propaganda and Misinformation

Current studies clarify that the trend of AI-generated content, deepfakes, and the use of misinformation campaigns has become a severe issue in the present information environment. Engelmann (2022) and ICCT (2023) highlight the significant gap between authenticity and counterfeit material, eroding public trust in what they see and hear on the Internet. The applications of persuasion have moved way beyond mere text: artificially generated videos, audio recordings, and visually appealing memes are a common phenomenon. They are made to be genuine, appealing, and shareable.

Farid (2025) also highlights the technological mastery of such fakes, stating that synthetically created images can seem like the real ones, making it difficult to distinguish between accurate and fake information for both regular citizens and sometimes professionals. According to Gorwa (2023), the rapid cycle of digital propaganda means not only the speed with which narratives are spread but the adaptation of narratives in real-time to take advantage of a temporary trend or confusion during which related assertions are disproven. This dynamism adds to the challenges authorities are facing, not only finding it hard to investigate malicious actors, but also developing effective countermeasures in real time. Together, these trends have contributed to a climate of suspicion and instability. Public trust falters, and the institutions tasked with ensuring safety and factual integrity are forced into a reactive, often inadequate, posture against the deluge of manipulated media and disinformation.

Operational and Financial Uses

Encrypted platforms such as Telegram and WhatsApp have become vital tools for those seeking operational security in illicit enterprises. Zhou (2024) points out the ease with which encrypted messaging buffers communications from surveillance, allowing groups to plan, coordinate, and recruit beyond the reach of traditional law enforcement. The ability to control access, delete messages, and create private channels or groups has given actors a marked advantage, letting them structure hierarchies, issue commands, and cultivate communities of intent without fear of interception. Bright *et al.* (2021) further contend that these platforms, designed for privacy, inadvertently foster a sense of haven, promoting trust among users and enabling recruitment on a meaningful scale, particularly when physical convening is risky or impractical.

Meanwhile, the financial backbone of many illicit operations has shifted towards cryptocurrency and peer-to-peer payment tools. Gordon (2023) details how digital assets, prized for their anonymity and global reach, facilitate fundraising that is difficult to trace. Cryptocurrencies bypass conventional regulatory checks, making laundering and rapid cross-border transfers a matter of routine rather than exception. In this way, the communications of criminal and extremist networks, as well as the financing, are secured. Both operational schemes can be developed in the secrecy of encrypted chats, and funds are transferred invisibly across distances, disrupting logistics and the feasibility of modern unlawful activities.

Policy and Countermeasures

There has been a significant increase in recent years in regulatory action by the European Union, United Nations, OSCE, and single governments to address online extremist and cybercrime-related harms. The European Commission (2025) has been at the forefront in enacting sweeping legal frameworks that seek to establish global standards in digital transparency and content moderation, and UNESCO (2024) has been leading efforts in safeguarding freedom of expression and right to access to information, arguing that regulation should not be at the cost of the democratic approach. On the same note, sovereign nations like Australia have proposed national strategies, and this has comprised prevention, disruption, and alignment of industry in the quest for digital safety (Government of Australia, 2025).

Despite this proliferation, empirical studies are rather somber. Borelli (2023) concludes that the landscape is full of fragmentation: regulatory initiatives often are not well coordinated and create inconsistent standards among the jurisdictions, and have a patchwork effect on enforcement. As Gorwa (2023) points out, attempts to combat extremist content with the help of specific measures often lead to rather crude censorship, which is bound to catch legitimate discourse, giving rise to the discussion of fundamental rights. In addition, platform accountability can be mostly rhetorical instead of practical; ongoing loopholes enable large technology corporations to escape liability or postpone serious compliance, and point toward the difference between regulatory discourse and practical excellence. The international initiative can therefore be characterized more precisely as a Rorschach test in which the optimists and the pessimists both see what they want to see, but these flawed policies are aimed at ensuring that policymakers can keep pace with the fast-changing digital menace.

Research Gaps

Bagchi (2025) highlights the significant research gaps in the existing studies, especially as a new digital environment regularly shows up in the form of new platforms aligned with the so-called alt-tech philosophy and metaverses. Such fast-fluxing landscapes can lie outside the scope of even major policy and academic research, posing unanswered questions about the spread of extremism, misinformation, and harmful content in places that do not even entirely exist as yet, or are under sufficient control. The fact that they give rise to unique cultures and lines of communication makes it difficult to generalize the findings of better-established social media platforms. According to Taylor (2025), as algorithmic moderation has grown much sophisticated, limited longitudinal studies are determining the long-term effectiveness of such moderating strategies. There is little clarity over whether automated interventions deter malign behaviour or merely prompt it to migrate and morph elsewhere. Algorithmic opacity and the evolving arms race with those intent on evading moderation only add layers of uncertainty to the policy debate.

Both Bagchi and Taylor highlight the paucity of research into the social psychological consequences of persistent exposure to synthetic media—especially the subtle, cumulative impacts on memory, belief formation, and interpersonal trust. The long-term repercussions of blurring the line between factual and fabricated experience remain poorly understood. As a result, scholars are left grappling with more questions than answers about the nature and depth of these emerging risks.

MATERIALS AND METHODS

This research is grounded in a qualitative thematic literature review, drawing on a carefully curated selection of literature published between 2020 and 2025. Priority was given to peer-reviewed studies and authoritative institutional reports, with relevance to the themes of social media, terrorism, cybercrime, AI, deepfakes, and digital governance guiding the inclusion process. Selection criteria focused not just on topical alignment but placed weight on methodological integrity and the reputation of the publisher, thereby seeking to secure both rigour and currency in the evidence base.

To identify sources, advanced search strategies, such as Boolean queries, were executed across major scholarly databases, including Web of Science, Scopus, Sage,

Springer, and Taylor & Francis Online. The resultant corpus comprises empirical insights from a mix of bibliometric analyses, content reviews, cross-national crime studies, and reports by prominent institutions. This ensures that the synthesis is not only theoretically informed but also empirically substantiated.

Nevertheless, there are acknowledged limitations. Chief among these is the restricted availability of proprietary big data, which can constrain the depth of analysis regarding certain phenomena, especially those unfolding in less accessible corners of digital platforms. Furthermore, given the pace at which digital threats and technologies evolve, even the most recent peer-reviewed literature may lag behind contemporary realities, leaving an unavoidable gap between research and rapidly shifting practice.

RESULTS AND DISCUSSIONS

Mechanisms of Social Media Exploitation

Recent studies highlight how more advanced methods are used by terrorists and criminal networks to recruit, radicalize, and mobilize vulnerable individuals. These campaigns can run across various platforms, including mainstream social media, encrypted messaging apps, and niche online forums—using curated content, private chat rooms, and gamification to keep users engaged and aligned with the ideology (Yumitro, 2023; Zeiger & Gyte, 2023; Raharjo, 2025). When aided by AI-based profiling, such campaigns become highly customized to an individual's psychological traits and are amplified by algorithmically generated content feeds, which encourage subjects to spend more time exposed to extremist ideologies (Binder *et al.,* 2022; Taylor, 2025).

The face of propaganda has shifted entirely toward ideological messaging, supported by eye-catching media, AI-generated texts, and deepfake videos that can create convincing yet false events or messages from leaders (Engelmann, 2022; Farid, 2025). Empirical evidence increasingly links online hate campaigns to a rise in offline violence, illustrating how digital platforms fuel notorious hate crimes through online radicalization (Arcila Calderon *et al.,* 2024). During the spreading phase, bots and organized online campaigns, such as so-called Twitter storms, are used to inflate extremist views, boosting their visibility artificially and perceived popularity (ICCT, 2023; Gorwa, 2023). Secure communication channels, including encrypted messaging systems and other dark social platforms, are commonly employed to plan attacks, coordinate logistics, and facilitate illegal trade (Bright *et al.,* 2021; Zhou, 2024; Holt, 2025). This use of channels presents a significant challenge to law enforcement and sparks ongoing debates about privacy rights, lawful access to communications, and appropriate government monitoring (Metrick, 2025).

The economic aspects of such operations have also changed. The ability to send funds anonymously using cryptocurrencies like Bitcoin, or through digital crowdfunding on social media, is now widespread, often disguised as charitable donations or routed through fake organizations (Gordon, 2023; Adewopo, 2025). This international flow of capital makes detection and prosecution more difficult. Also, fake identities, machine-generated stories, and automated interactions help extremist and criminal groups quickly expand recruitment, harassment, and propaganda efforts. Deepfakes pose serious risks, including fake calls to action by leaders and counterfeit hostage or ransom videos, adding a new challenge in digital manipulation (ICCT, 2023).

Case Studies and Trends

Terrorist organizations like ISIS have proven to be highly adaptable by leaving traditional social media and turning to encrypted communication platforms like Telegram and Signal, especially as mainstream social media platforms continue to remove and moderate content (Yumitro, 2023; Arcila Calderon *et al.,* 2024). These platforms offer security, minimal oversight, and the ability to support both broad propaganda and secure communication with targeted individuals. This shift has enabled extremists to expand their communication strategies using more advanced digital tools to recruit members, coordinate activities, raise funds, and share operational techniques that are much harder for security agencies to detect and interfere with. This trend is mirrored in organized crime syndicates such as drug cartels, human trafficking rings, and ransomware groups. These groups are increasingly blending real-world crime with traditional cyber deception, using platforms like Discord and Telegram, as well as gaming and metaverse environments to find, groom, and recruit operatives (Zhou, 2024; Bagchi, 2025). Coupled with their global reach, payment systems, and communication facilities, the relative anonymity of these virtual spaces creates an ideal environment for criminal networking, money laundering, and trading activities.

Robust multi-country studies provide evidence of a clear and statistically confirmed link between spikes in coordinated online hate campaigns—such as tweets, memes, or viral hashtags, and subsequent increases in hate crimes, mob violence, and terrorist attacks (Arcila Calderon *et al.,* 2024; Ghosh, 2025; social media + Society, 2025). These data underscore the catalytic role of digital extremism and highlight online hate outbreaks as early indicators of real-world violence. The COVID-19 pandemic further accelerated this shift toward radicalization, propaganda dissemination, and recruitment within the digital space. Factors like social mobility restrictions, lockdowns, increased internet use, and social isolation created fertile ground for extremist and criminal exploitation. Reports from international organizations such as the UNODC, OECD, and scholarly research (Nhesi *et al.,* 2021; UNODC, 2025; OECD, 2020) reveal a significant rise in cyber-enabled crimes, internet fraud, and extremist mobilization during the pandemic, demonstrating how hostile actors adapt to global crises. These trends show that criminal and extremist groups are leveraging emerging technologies and alternative platforms to evade regulation, expand their influence, and

operationalize online networks, posing an ongoing and evolving threat to global security.

Technological Developments

Artificial intelligence is also being used to assist both criminal and defense actors in their pursuit of digital threats, as well as to protect their technology. Proven instances have shown that deepfakes—hyper-realistic synthetic audio and video—have been actively used in terror finance scams, identity theft, and psychological manipulation efforts, expanding the scope and impact of malicious activities (Engelmann, 2022; Farid, 2025; ICCT, 2023; Taylor, 2024). AI-powered bots used to spread propaganda automate the process of narrative dissemination, allowing extremist organizations to exponentially increase the number of targets and memes promoted across different platforms (Gorwa, 2023). To counteract this, large internet sites have incorporated advanced algorithmic technologies, such as natural language processing (NLP) and image analysis, to identify, filter, and neutralize harmful content in real time. However, despite these innovations, efforts at content moderation often struggle with the cleverness and adaptability of emerging threat methods. Through obfuscation, coded language, and the continually advancing rhetorical tools, such malicious content consistently evades detection systems, exploiting the fact that computers are not easily fooled by the ever-changing tactics of adversaries (Metrick, 2025; Borelli, 2023).

Regulatory frameworks at the EU, UN, and OECD emphasize the need for the quick removal of terrorist information and coordinated governance. However, these frameworks are weakened by complex cross-jurisdictional implementation issues, compounded by ongoing disagreements over the importance of personal protection and civil liberties, as well as how to manage these in cross-border cases (European Commission, 2025; UNESCO, 2024; ICCT, 2023). Efforts to balance strong platform oversight with protecting individual rights hinder the development of unified solutions across global platforms. As moderation increases on major platforms, bad actors are shifting to encrypted messaging services and less popular "alt-tech" platforms like Gab, as well as decentralized areas of the metaverse. These environments present new, larger challenges for intelligence collection and law enforcement efforts to track threats and respond effectively (Zhou, 2024; Holt, 2025). Overall, these trends highlight an ongoing competition between offenders and protections, where technological progress continually reshapes the landscape of digital safety and vulnerability.

Impact Analysis

Viewing hateful, violent, or edited messages on social media has profound psychological and social effects, especially increasing anxiety, mistrust, polarization, and susceptibility to radicalization, which is particularly evident in younger audiences (Baelanger, 2025; Arcila Calderon *et al.,* 2024; Mohammadi, 2023). Repeated exposure to graphic violence or radical speech can dull sensitivity to violence and foster an overall sense of danger, making peer pressure more likely to push individuals toward joining radical groups. Such a digital hate environment often deepens social divisions, weakens resilience, and hampers constructive participation in the public sphere. Online messages of uncertainty, propaganda, and calls for violence spread doubt among people and erode trust in democratic institutions, risking political destabilization and disruption of the democratic process (Engelmann, 2022; Stohl, 2020). Distrust in election credibility, judicial impartiality, or media fairness threatens civil society, risking democratic decline and political stagnation.

Government reactions in the form of heavy-handed regulation or blanket restrictions on the internet often worsen the situation. These interventions can increase anxiety among the population instead of supporting their intended goals, suppress reasonable discussion within the country, and trigger frustrations or feelings of disregard from authorities (Borelli, 2023). Additionally, strict content moderation measures by companies have not only caused undesirable effects but have also prompted malicious parties to move to encrypted or decentralized sites, where they are harder to police and where collateral blocks on legal, dissenting speech are more likely (Binder *et al.,* 2022; Gorwa, 2023). The effort to combat toxic online content becomes increasingly complex since national regulation systems vary, and digital information flows freely (OECD, 2020; UNESCO, 2024; Olley, & Ikerodah, 2025).). Regulation frameworks must carefully balance protecting vulnerable groups and democracy while navigating legal complexities across international jurisdictions. Unless more coordinated and nuanced interventions are implemented, there are concerns that the digital space will continue to fragment and that more harmful elements will take root and divide society further.

Discussion

The fast evolution of social media further challenges the digital societies asymmetrically. Enemies and those on defense are fast to change their strategies with the current types of technologies, including artificial intelligence, deepfakes, and encrypted communications, often before regulators and law enforcement can act upon them. With the emergence of AI-generated content and complicated deepfakes since 2020, propaganda techniques have radically evolved, and the risk of disinformation campaigns has grown. Radicalization acts and hate speech have turned out to be more flexible, including the boundaries between online activities and real social contacts. A concerted plan of action among various spheres, such as governments, scholars, experts in technology, and civil rights advocates, is needed to fight the same through core rights. Efforts to use policies that are more universalist, i.e., one size fits all, have turned out to be inadequate since the dynamics of threats are so flexible and technology-oriented. There are also substantial empirical holes related particularly to whether synthetic media will produce real-world effects,

the psychological aftermath of algorithmic radicalization, and whether existing initiatives in global governance work. Since countermeasures, policy, and regulatory responses are evolving, iteratively, and at a scale and complexity to which they have never been subjected, there is a premium on evidence-based and subtle countermeasures that strike a balance between societal security and the essential protections of digital freedoms.

CONCLUSION

It is evident that social media sites serve two functions in society: they facilitate communication and cause dysfunction. Although it has transformed communication in many ways, providing this platform has also led to the emergence of several terrorist acts and crimes, especially with the recent advent of AI and Deepfake technology. Malicious actors use these new tools to create engaging yet misleading content that can spread virally across global networks and cause harm. Resolving this issue requires a complex approach. The government can support the creation of boundaries, but government actions often remain limited, particularly when it comes to issues like freedom of speech and international jurisdiction. While platform intervention plays an important role, it has so far been unsuccessful in preventing the spread of harmful material or discouraging the misuse of new technologies. Civil society plays a vital role in raising awareness, promoting moral values, and emphasizing the responsibility of tech development by governments and corporations.

Such individual efforts, however, are not sufficient on their own. A unified effort that involves government regulation, platform responsibility, and active civil society participation is the only way to address these complex issues. More importantly, these actions should protect rights and safety without infringing on fundamental freedoms like free speech and privacy. Additionally, the strategies chosen should be flexible and adaptable, as technology is constantly evolving. Only through broad, collaborative efforts can societies hope to build a safer digital culture while safeguarding these fundamental principles.

RECOMMENDATIONS

1. Harmonize digital governance across borders, ensuring proportionality, accountability, and transparency in all interventions.
2. Invest in digital/critical literacy, early warning systems, and community resilience.
3. Enhance transparency and auditability of algorithmic moderation, prioritize explainability, and facilitate research access.
4. Improve user-reporting tools, especially for at-risk populations.
5. Build technical capacity in AI and forensic analysis of manipulated media, ensure oversight and proportionality in surveillance.
6. Foster cross-sector and international information sharing.
7. Promote proactive counter-narratives and mental health support for those targeted by extremist grooming.
8. Advance interdisciplinary research, focusing on new technology platforms and emergent vectors.

REFERENCES

Adewopo, V. A. (2025). Comprehensive analytical review of cybercrime and cyber security in West Africa. *Journal of Engineering Science and Technology Review, 18*(1), 216–232. https://doi.org/10.1186/s43067-025-00216-x

Alnaqbi, H. H. (2025). Social media impact on societal security. *Frontiers in Sociology*. https://www.frontiersin.org/journals/sociology/articles/10.3389/fsoc.2025.1508542/full

Arcila Calderón, C., Sánchez Holgado, P., Gómez, J., Barbosa, M., Qi, H., Matilla, A., ... & Fernández-Villazala, T. (2024). From online hate speech to offline hate crime: The role of inflammatory language in forecasting violence against migrant and LGBT communities. *Humanities and Social Sciences Communications, 11*(1), 1-14.

Ate, A. A., Akpor, E. D., Olley, W. O., Omosotomhe, S. I., Chukwu, O. J., Dauda, J. A., & Isah, A. (2024). Rethinking social media ethics in Nigeria. *International Research Journal of Multidisciplinary Scope (IRJMS), 5*(2), 27-34. https://doi.org/10.47857/irjms.2024.v05i02.0177

Bagchi, K. (2025). Cyber crime or technological epidemic? Intersecting the dark web, AI, and deepfake identities. *Open Journal of Social Sciences, 14*(4), 67–92. https://doi.org/10.4236/jss.2025.142856

Bélanger, J. J. (2025). Beyond radicalization: The 3N model and its application to criminal attitudes. *Frontiers in Psychology, 16*, Article 1498936. https://doi.org/10.3389/fpsyg.2025.1498936

Binder, J. F., & Kenyon, J. (2022). Terrorism and the internet: How dangerous is online radicalization?. *Frontiers in psychology, 13*, 997390. https://doi.org/10.3389/fpsyg.2022.997390

Borelli, M. (2023). Social media corporations as actors of counter-terrorism. *New Media & Society, 25*(8), 2765–2783. https://doi.org/10.1177/14614448211035121

Bright, D., Brewer, R., & Morselli, C. (2021). Using social network analysis to study crime: Navigating the challenges of criminal justice records. *Social Networks, 66*, 92–103. https://doi.org/10.1016/j.socnet.2021.01.002

Engelmann, S. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media change politics and law. *AI & Society, 37*(4), 1739–1754. https://doi.org/10.1007/s44206-022-00010-6

European Commission. (2025). *Prevention of radicalisation*. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation_en

Farid, H. (2025). Mitigating the harms of manipulated media: Confronting deepfakes and cheapfakes.

PNAS, 122(31), Article 12305536. https://www.pnas.org/doi/full/10.1073/pnas.2407673121

Gordon, A. (2023). Social media and terrorist financing. In *The Routledge Handbook of Counter Terrorism and Law* (pp. 181–195). Routledge. https://doi.org/10.4324/9781003092216-9

Gorwa, R. (2023). Benefits, risks, and regulation of generative AI screen technologies. *Media International Australia, 191*(1), 65–78. https://doi.org/10.1177/1329878X241288034

Government of Australia. (2025). *Australia's counter-terrorism and violent extremism strategy*. https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/australias-counter-terrorism-violent-extremism-strategy.pdf

Holt, T. J. (2025). An assessment of the harms associated with ideologically motivated cybercrime. *Crime & Delinquency, 71*(3), 860–889. https://doi.org/10.1177/00111287241271221

ICCT. (2023). *The weaponisation of deepfakes*. International Centre for Counter-Terrorism. https://icct.nl/sites/default/files/2023-12/The%20Weaponisation%20of%20Deepfakes.pdf

Metrick, S. (2025). Deepfake detection in generative AI: A legal framework proposal to tackle criminal and societal risk. *Computer Law & Security Review, 48*, Article 105971. https://doi.org/10.1016/j.clsr.2025.105971

Mohammadi, S. (2023). Effectiveness of educational programmes to prevent and counter violent extremism. *Public Health Reviews, 44*(2), 211–228. https://doi.org/10.1186/s40985-022-00160-8

Näsi, M., Tanskanen, M., Kivivuori, J., Haara, P., & Reunanen, E. (2021). Crime news consumption and fear of violence: The role of traditional media, social media, and alternative information sources. *Crime & Delinquency, 67*(4), 574-600.

OECD. (2020). *Current approaches to terrorist and violent extremist content among the global top 50 online content-sharing services*. https://www.oecd.org/en/publications/2020/08/current-approaches-to-terrorist-and-violent-extremist-content-among-the-global-top-50-online-content-sharing-services_5b85c74d.html

Olley, W. O., & Ikerodah, J. O. (2025). Emotional and social barriers to engaging in misinformation correction on social media: A qualitative study. *American Journal of Arts and Human Science, 4*(3), 142–148. https://doi.org/10.54536/ajahs.v4i3.5683

OSCE. (2023). *The role of civil society in preventing and countering violent extremism and radicalisation*. https://www.osce.org/files/f/documents/2/2/400241_1.pdf

Petrosino, A. (2025). Prevalence and risk and protective factors for extremism: A meta-analytic review. *Campbell Systematic Reviews, 21*(1). https://doi.org/10.1002/cl2.12018840

Social Media + Society. (2025). Sage Publications. https://journals.sagepub.com/home/sms

Stohl, M. (2020). *The politics of terrorism* (3rd ed.). Taylor & Francis. https://doi.org/10.4324/9781003065876

Taylor, F. X. (2024). *Impact of artificial intelligence (AI) on criminal and illicit activities*. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf

UNDP. (2021). *Prevention of violent extremism*. https://www.undp.org/sites/g/files/zskgke326/files/2022-08/UNDP-PVE-2021-Annual-Report-V2.pdf

UNESCO. (2024). *Preventing violent extremism*. https://www.unesco.org/en/preventing-violent-extremism

Yumitro, G. (2023). Bibliometric analysis of international publication trends on social media and terrorism. *Frontiers in Communication, 8*, Article 1140461. https://doi.org/10.3389/fcomm.2023.1140461

Zeiger, S., & Gyte, J. (2023). Prevention of radicalization on social media and the internet. *International Centre for Counter-Terrorism*. https://icct.nl/sites/default/files/2023-01/Chapter-12-Handbook_0.pdf

Zhou, Y. (2024). Metacrime and cybercrime: Exploring the convergence. *AI & Society, 39*, 771–783. https://link.springer.com/article/10.1007/s11417-024-09436-y