

<https://doi.org/10.59298/NIJLCL/2026/6.2.6672>

Online Radicalization Pathways: Network Dynamics and Intervention Syntheses

Kakungulu Samuel J.

Faculty of Education, Kampala International University, Uganda

ABSTRACT

The rapid expansion of digital communication networks has transformed the nature and mechanisms of radicalization, creating new pathways through which individuals encounter, engage with, and potentially adopt extremist ideologies. This study examines online radicalization through the lens of network dynamics, focusing on how digital platforms, algorithmic amplification, information cascades, echo chambers, micro-communities, cross-platform mobility, and transnational linkages contribute to the evolution of extremist engagement. While the internet does not independently cause radicalization, it functions as an accelerator that enhances exposure, interaction, identity formation, and mobilization within broader social and political contexts. The study synthesizes empirical evidence on online radicalization pathways across diverse platforms, including social media networks, encrypted communication channels, and alternative digital spaces, highlighting the importance of understanding user behavior, platform architecture, and network structures. It further evaluates intervention strategies targeting individuals, online content, platforms, communities, and educational environments. Findings indicate that effective prevention requires a multidimensional approach combining risk identification, responsible platform governance, digital literacy, counter-narratives, community resilience, and interagency cooperation. However, significant challenges remain regarding ethical concerns, evaluation metrics, privacy protection, and the development of evidence-based interventions adaptable to evolving digital environments. The study concludes that addressing online radicalization requires coordinated strategies that recognize the interaction between online and offline factors while balancing security objectives with fundamental rights and freedoms.

Keywords: Online radicalization; Network dynamics; Extremist networks; Digital platforms; Intervention strategies

INTRODUCTION

The emergence of online radicalization as a credible threat to national and global security grew considerably as terrorist organizations increased and pivoted their attention toward cyberspace in the early 2000s [1]. Given the global nature of the internet, the pervasiveness of online communication, and the rise of social media, digital counterterrorism became a priority for intelligence and law enforcement agencies, but there is much skepticism concerning online radicalization as a pertinent issue [2]. This chapter aims to demystify online radicalization by elucidating existing pathways of individual engagement with digital extremist networks, which can subsequently lead to more offline involvement with violent extremist organizations or other criminal activity [3]. While some scholars contend that online radicalization pathways cause terrorists to contemplate violence or terrorist acts, available evidence supports the idea that the Internet is merely a supplementary and not necessary factor in the radicalization process [5]. French National Police research noted that political context acts as decisive leverage, wherein online communication accelerates standard individual radicalization processes [1]. Radicalized violent Islamist offenders born outside of France require stronger contextual triggers than their French-born

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

counterparts. Prior to the 2015–2016 series of attacks, individuals with no physical links to the country sought entry through problematic digital communication pathways [1]. The broader evidence indicates that young people exposed to political attacks or religious images prior to violent acts canvassed and circulated information on online fora, although most later communicated separately through encrypted environments [2]. Anthony James M. Lawan, David M. Gonçalves, and Yeadal M. B. Amri explicate online radicalization models that enhance counter-online radicalization strategy formulation and implementation through understanding of associated phenomena [1].

Conceptual Frameworks

This section relies on a range of empirical studies to support theoretical discussions, examining how recent findings inform explanatory frameworks [1]. An extensive body of literature explores radicalization processes in digital contexts, identifying distinct facets such as ‘online radicalization’, ‘digital radicalization’, ‘digital jihadism’, and ‘internet radicalization’ [2]. Many scholars now consider these terms misaligned with radicalization’s core definition. Nevertheless, researchers increasingly study the role of online processes and digital environments in radicalization [3]. The focus thus shifts to useful concepts and models that clarify the online aspects of radicalization, leading to the adoption of digital radicalization alongside structurally integrated conceptual frameworks emphasizing the various degrees of focus on, or manifestations of, radicalization itself [2]. To pinpoint relevant online processes within broader radicalization pathways, network theory serves as a foundational approach describing interaction patterns and structural properties that shape radicalization [5]. Digital technologies profoundly alter how adherents, sympathizers, and organizations disseminate and broker ideas, opinions, claims, and identities [6]. Consequently, the role of digital environments, especially the internet, in radicalization receives increased scrutiny [1]. Network models elucidate the multifaceted, cumulative ways in which online processes, practices, and environments leverage networked digital communication technologies to enhance users’ engagement with extremist ideas, beliefs, narratives, and scripts [7].

Definitions and Scope of Online Radicalization

Radicalization is defined as the social process by which individuals or groups adopt extreme beliefs that advocate violence or other illegal activities to promote a political, ideological, or religious agenda [2]. The process is often illustrated as a “slippery slope” wherein individuals move progressively along the path, growing increasingly aligned with propagators of radical ideology and behavior [3]. Offline processes of radicalization have been documented and described extensively, but some experts contend that there is still considerable uncertainty regarding the online radicalization process, which entails different dynamics [4]. Online radicalization can occur in isolation, as users enter online spaces with little offline exposure or pre-existing views. However, few individuals constitute solely online radicals; ideological exposure and interaction is usually needed for radicalization to occur [5]. Moreover, the reciprocal influence between online and offline radicalization suggests that both processes matter and require consideration within a broader information environment framework [6]. Increasingly, research focuses on identifying online radicalization pathways mapped to platforms, networks, users, and languages in a given region [1].

Network Theory in Online Environments

The Internet is fundamentally changing the nature of interpersonal interactions. In many respects, the online world acts as a separate space where networked individuals engage in a range of interactions that shape their identities, intergroup attitudes and group-related behaviours [4]. Such on-line environments are a breeding ground for the identification of at-risk individuals. The pace of social interaction, augmentation of knowledge and experiences, and opportunity for reaching like-minded people far exceeds those in the physical world [5]. Social media, chat-rooms and other online platforms facilitate political and anti-political dialogue among everyday citizens. Internet-mediated radicalisation remains one of the most prominent and dangerous online activities today yet preliminary research on the phenomenon continues to grow [5]. Young individuals engage with radicalised content online in ways that often approximate without involvement in offline activities [6]. Radicalisation occurs through a series of interconnected pathways that determine how a person traverses from initial encounter to end state [1]. Two key components of the structure of the Internet impact this process, networked action and connective action. Online radicalisation proceeds along five broad pathways that describe the content an individual engages with, the eventual path taken differentiates the order in which these are traversed, direct contact, online and offline, or purely online [2].

Pathways of Radicalization in Digital Networks

The information environment has changed due to the emergence of new communication technologies. Radicalization processes have not changed; however, the online environment and digital social networks can facilitate and accelerate them [3]. Studies of online radicalization often employ temporal or sequential models to capture the evolution of radical views and behaviors. Internet-mediated processes can be described as pathways.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Pathways highlight the interrelated and reciprocal nature of online radicalization [4]. Radicalization on digital platforms has a dual nature. On the one hand, processes occur within core platforms such as social media; on the other hand, processes can occur across multiple platforms. Mobilization, networking, coordination, and recruitment processes can take place after initial radicalization. Pathways operate when the information or view shifts, and are related to the mechanism of potential radicalization [5]. Digital social networks alter the dynamics of how ideas propagate and influence. Patterns of interactions contribute to information cascades and echo chambers. Initial exposure to extreme material influences mutual engagement between individuals or small groups. Radicalization growth is closely connected to the notion of like-minded groups and micro-communities. Network structures undergoing change are conducive to the development of alternative sub-cultural or extremist jurisdictions [6]. Transnational connections and movements occur through interactions among digital networks across several platforms. The innovation of new communication technologies improves the connectivity of these disparate networks [7]. Radicalization progresses through cross-platform interactions while interest can remain on the core platform, promoting further cross-platform movement [1].

Information Cascades and Echo Chambers

The online radicalization mechanism, while not entirely new, acquires a unique dimension in the digital arena. Within this space, users navigate via networked platforms populated by communities sharing their interests, concerns, and passions [1]. Users may be radicalized within any one of these platforms, and the risk of radicalization often grows when they are exposed to the content disseminated through these platforms [2, 3]. The digital landscape enables the rapid spread of information from one locality to another and from one platform to another, allowing for global outreach in seconds. Severing all ties virtually anywhere in the world becomes impossible [4]. Information cascades, echo chambers, algorithmic amplification, micro-communities, cross-platform mobility, and transnational linkages constitute the elements of the process [5]. Language and terminology are also factors involved. These elements emerge from content dissemination, monitoring, and engagement, and represent vectors or channels through which radicalizing content travels [6]. They synthesize evidence from online activity revolving around jihadist, white-supremacist and eco-extremist material on 4chan, 8chan, Gab, Instagram, Parler, TikTok, Telegram, Twitter, and YouTube [7].

Algorithmic Amplification and Content Curation

The algorithmic amplification of extremist content on YouTube and other social media platforms leads to a radicalization effect among viewers [4]. YouTube, as one of the largest video platforms with a diverse and global audience, is attractive for spreading radical views and hateful information. While people who share radical content meet in user-persistent forums, the algorithmic content curation on platforms has directed public attention toward extreme ideologies [5]. YouTube has been widely used to incite radicalization among its viewers, and the service is delivered both via user-persistent channels and algorithmic recommendation [6]. Even radical materials that have not been removed can be spread through recommendation channels based on patterns such as user contribution and content similarity. The mechanism of recommendation diffusion pushes extreme contents and incites radicalization [7].

Micro-Communities and Identity Formation

Changes in the political climate and online exposure to extremist material have been linked to the emergence of “micro-communities,” or small groups consisting of friends or like-minded individuals united around issues such as environmentalism, political violence, or other extreme views [4]. Group discussions within these tight private networks can generate radicalization-driving messages while at the same time constituting a mechanism to strengthen mutual social bonds and a sense of community [5]. Micro-communities can play a role in both rehabilitative and radicalization processes. These small groups provide a platform for identity-building before individuals make their way to larger communities [6]. Micro-communities provide a context for identity and description building and an avenue for help-seeking before bigger groups of extremists [2]. Further, these groups provide signals to the rest of the network as individuals bound together in smaller circles begin to cluster toward an outside set of groups directed toward rehabilitation or radicalization [7].

Cross-Platform Mobility and Transnational Linkages

Digital radicalization dynamics increasingly exhibit platform-transcending continuity as individuals transition across online venues, often linking site-specific encounters into overarching trajectories [5]. Such multi-site journeys facilitate transitions from milder discourses into more extreme positions and political violence options [6]. This movement is enhanced by the prospect of anonymity, platform interoperability, and compatible residue artefacts enabling selective recontextualization, the meshing of personal and group exchanges in one platform moulding the social-identity transmissions of likes or follows on another, the reconstruction of polarizing environmental narrativization from one pole into another, the adaptation of interest-based animations from non-government-organized-organization specific channels into those explicitly framed as belonging to such

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

advocacy[7]. Actors do not merely traverse venue-specific discourses, but connect interlocutions on different platforms [1]. Evidence from Youtube users switching to Telegram shows unaffected engagement, policy adaptations on the former still hold recontextualized valuation beyond notice [2]. Radicalization-preceding user profiles exchange framed positions across platform junctions, gradually coupling controversial tenets through “stepwise radicalization.” Similar trajectories thread Youtube and Instagram, Facebook and Telegram, and Discord and Telegram [3]. The movement of radicalization-enabling users across disparate sites presumes attendant sustainment or neural replacement at each point of dispersal, enabling both transitory flux and stable multi-locationality at radicalization-relevant profiles [4].

Empirical Evidence on Network Dynamics

The existing empirical evidence supportive of the outlined online radicalization a pathway is reviewed across three axes [1]. The first describes the methodological approaches and data sources employed to document network dynamics on popular platforms. The second summarizes major findings reported in the studies [2]. The third details case studies concerning evidence of radicalization on two platforms used intensively by jihadist actors: the now-defunct video chat application Chatroulette, and the live streaming platform Twitch, which has emerged as a significant recruitment environment for the far-right and other extremist groups in recent years [3]. Since 2000, scholarly research on the internet as a tool for radicalization has increased steadily and expanded to encompass both theoretical and empirical work [1]. The earliest empirical investigations generally focused on the role of the internet in the radicalization process, the behaviour of radicalized users across social media platforms, and analyses of guidance documents on radicalization disseminated by extremist groups [4]. The research agenda subsequently broadened to include the collective dynamics observable within radicalized social media communities [5].

Methodological Approaches and Data Sources

Radicalization is a process through which individuals or groups undergo gradual changes in their political, social, or religious beliefs, often resulting in the endorsement of extreme ideologies and violence [1]. Existing academic literature indicates a strong social component in the radicalization process, particularly in the dissemination of extremist beliefs [1, 2]. In the digital age, an increasing number of studies are exploring the role of online environments in fostering extremist and radical ideologies [3]. It is essential to understand the specific mechanisms driving online radicalization and the different avenues of support sustaining radical movements in the digital age [2]. By analysing available studies, key dynamics of network and digital platforms that offer pathways for radicalization via online forums, social media or the general digital environment have been investigated. A ‘pathway’ is understood as the consistent micro-level user actions carried out within a defined time span to become influenced towards or joining a radical or extremist group [3]. The identified online radicalization pathways provide information and understanding of audience engagement where users are exposed to radical content [1].

Key Empirical Findings

Addressing online radicalization, a phenomenon reinforced by internet dynamics, necessitates a nuanced understanding of user engagement and dissemination pathways [3]. Hence, empirical insights into radicalization-related content propagation inform preventive measures. Studies span various ideologies from extremist, hate, and political agendas to ideological grooming [1].

Case Studies across Platforms

Specific social media platforms serve different radicalization purposes, resulting in distinct network dynamics. Telegram supports underground sharing and private communities, while scaling communities to over 10,000 members and allowing connections to public channels with tens of thousands of subscribers [5]. Twitter links reference-based micro-communities across ideologies, individuals transmit memes across unique micro-communities, amplifying their message to followers but never engaging with mainstream feeds [6]. TikTok appears to favour expression over exchange, enabling poor-quality content to attain massive reach via memes or popular songs. Polarized actors seem less active on TikTok[7]. The platform shapes content far less than others, aligning poorly with prevailing radicalization theories. Analysis of French-speaking far-right ideologies within Telegram and Discord indicates post-Gilets Jaunes groups shift online, seeking event-oriented, explanatory video content rather than a novel message. After the 2019–2020 incel phase, retention mechanisms increasingly emphasize social bonds; most channels invite further exploration rather than promote instantaneous alignment and conversion [1]. French-speaking radical Alt-Tech movement messaging has expanded through Telegram, Tinder, Discord, TikTok, etc., using humour and absurdity, focus on societal concerns, attack on digital control, statement of interests and frustrations [4]. Evidence from ISIS and New Zealand shows transnational connections prompt certain actors to experiment with other platforms for far-right discourse, seeking not to join but to observe and analyse[5]. These broadened studies of pathway features stratified by platform genre, user count, target audience, and technological architecture remain scarce and essential for developing generic models of radicalization, informing counter-measures according to expected dynamics [6].

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Intervention Strategies and Synthesis

Radicalization is a continuum from non-extremist to extremist views and is targeted at potential future extremists [7]. The internet does not automatically push users to radicalisation; societal challenges such as exclusion, marginalisation, loneliness, vulnerability, and identity crises encourage individuals to engage with extremist content. These are often presented through content that does not necessarily contain hatred for other groups [1]. Large platforms increasingly put measures for user safety, resulting in shifts towards the Dark Web [4]. Involvement in extremist discourse generates brand-new struggles and the threat of arrest, yet the desire for belonging remains. Drawing on radicalisation models, 200 multi-ethnic youngsters in Canada were engaged in multi-staged focus groups to explore healthy expressions across cultural, racial and religious identities that could lead to attachment to pro-social relationships [5]. As a result, it was found that group exclusion, family-parental neglect and unemployment are factors that would invite the young towards radicalisation. In familial settings, a good family structure would avert radicalisation. Research has also investigated content analysis on toxic discourse targeting children and adolescents using Hatecheck, cleaned contained corpus of MFC-19, and concept of humour [6]. In tackling the problem of preventing online radicalisation, three levels of intervention focusing on individuals, content, and communities have been identified either for entire platforms or for specific cases. Individual-level intervention seeks to detect and avert possible radicalisation through profiling users by defining reference profiles and possible trajectories of engagement with radical content [7]. Differently from toxic comments, monitoring radicalisation is not supported by standard tools.

At-Risk User Identification and Risk Profiling

Online radicalization is a pervasive threat to society, prompting interest in identifying individuals at risk of committing extremist acts. Programs across different countries, such as the 'Prevention Programme' based on Big Data analysis and the 'I Guy programme', aim to assess and intervene in social media radicalization [7]. Definitions of radicalization have included the adoption of extremist beliefs or ideologies for change, and the shift to exclusionary in-groups [1]. Profiling at-risk users is necessary to design tailored preventive actions and closely monitor their online behavior for intervention when risk increases. An initial framework suggests indicators of degree and kind of radicalization: [1] vulnerable account ownership compared to other users, [2] vulnerable smartphone integration or accessibility compared to other devices, [3] selective exposure to extremist content across platforms, [4] potential exposure to different degrees of extremist content across platforms, [5] subscription to or engagement with specific accounts posing potential influence, and [6] consumption or engagement with scripts explicitly supporting user participation. Preventive measures should target both the digital and socio-psychological environments that nurture radicalization. In existing frameworks, account vulnerability linked to fragile identity and social endorsement facilitates entry into violent extremist arenas. Importantly, community approaches should be explored to foster resilience and refrain from minimizing the privilege of intimate offline settings in favor of online counterparts [7].

Platform-Level Interventions and Design

A discerning analysis of intervention strategies targeting online radicalization, focusing on user-level, platform-level, community-level, and educational-level measures, underscores the utility of a systemic framework that incorporates pathways of online radicalization and their accompanying network dynamics [5]. While numerous grid-based or typological analyses of interventions are available, employing a systematic framework that provides comprehensive insight into the interplay between pathways and corresponding interventions remains a gap in the literature [6]. Such a framework can thus inform the design of evidence-based interventions capable of addressing online radicalization's multifaceted challenges [6]. Whereas user-level measures (e.g., pro-social content, counter-speech, social media commentary) directly target at-risk individuals, platform-level measures influence the overall context in which users interact. Algorithms are central to content promotion, yet applicable algorithmic interventions remain nebulous [7]. Existing guidelines for pro-social content promotion [7] tackle the challenge indirectly by suggesting content types likely to engage at-risk users, but do not identify intervenable algorithmic features themselves. Values-based design provides a framework for designing algorithmic prompts and nudges reflecting community-approved values, yet does not specify criteria for identifying pro-social or harmful content [2]. Likewise, an overview of algorithmic content-harm interventions offers a distinction between identifying harmful content and detecting harmful content consumption, omitting criteria for a broad set of pro-social content. Consequently, additional research is needed on the theoretical foundations, pathways, or characteristics of content that merit algorithmic intervention across multiple platforms and user groups [1]. Addressing such gaps can facilitate the design of effective interventions via pro-social audience targeting.

Community and Educational Interventions

Radicalization is a process that can occur through either online or offline interactions, or a combination of both. The mechanisms of engagement and the content consumed differ markedly between offline processes and those

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

that are exclusively online [2]. There is a need to consider the context and culture of online environments when assessing radicalization through these processes [2]. Nonetheless, the Internet plays a central role in enabling and amplifying various key topics and grievances [3]. Most research treats the Internet as an enabler rather than analysing how radicalization can develop solely online. Engagement is considered to be asymmetric between entities involved [1]. Youth are reportedly more vulnerable to radicalization than the general public. This at least partially stems from impressionability, cognitive distortion, personality traits unique to youth, a lack of mature coping strategies, a greater search for identity, and a generally broader range of experiences during youth [4]. The shift towards online radicalization has sparked significant concern and generated a multitude of perspectives, but community-level- and educational strategies remain widely underrepresented within intervention frameworks [5]. Yet both youth and young adults today have a much more significant online presence than past generations, with community and educational interventions activated 0–5 [7]. Researchers steadily emphasise that intervention efforts must engage broader audiences beyond those already radicalised or exposed to radical content [6].

Policy Implications and Interagency Collaboration

Recognizing the intersections among the different synthesis categories, interventions should also be designed and regarded as a comprehensive set rather than as a selection of independent measures [4]. Policy initiatives focused on a single intervention type are generally unlikely to achieve sustainable outcomes; in many cases, users do not engage sufficiently with available information to benefit from the intervention, and the presence of multiple risk indicators, such as online exposure alongside real-life grievances, suggests the importance of longer pathways with cumulative effects [1]. An integrated understanding of the catalyzing role of user risk profiles, channel characteristics and design features proprietary to each platform, and affinities for discourse and wayfinding among risk and protective agents permeating radical communities and sub-cultures is thus essential for deriving concerted strategies [5]. Assessing interventions from a policy perspective calls for considering especially the need for interagency collaboration on the respective strategies [6]. An interconnected interplay characterizes the phenomenon of online radicalization, with channels independently liberating yet actively strengthening one another, and careful attention to profile constellations and channel affordances permits identifying the most conducive and protective links in the system [7]. Certain digital channels facilitate information exchanges that enable access to attention-capacity-hungry spaces anchored within physical venues or gatherings of audience and actors alike, and the strategic undertaking of intervention activities over multiple platforms can support common objectives, such as countering grievances, reaffirming commitment, instilling doubt, and disrupting protective bonds [1].

Evaluation Metrics and Evidence Gaps

Radicalization has caused serious concern among scholars and authorities. However, available measures to combat it have not been investigated sufficiently [6]. A major issue is the lack of evaluation metrics to determine, before and after the implementation of measures or media campaigns, whether at-risk users have been indeed contacted, still continue to engage with content at-risk, or have checked at-risk content after an intervention. Research indicates that the network structure of potential targets' online activity is relevant [1] but attention to the subject is still very limited and the body of evidence regarding appropriate metrics remains scant [7].

Ethical, Legal, and Societal Considerations

Grounded on empirical evidence, the concept of a “pathway” provides a robust way to measure the relative likelihood of online radicalization [3]. Discrete steps along a pathway can be identified based on patterns in online behaviour. For example, establishing multiple social connections and communicating directly with existing fringe members are strong indicators of the potential to fall deeper into those extreme ideologies [1].

Synthesis and Recommendations

Online radicalization is a dynamic and evolving phenomenon, driven by the continuous development of digital platforms and networked interactions [2]. The pathways introduced in this study provide a foundation for understanding the links between online activities and the spectrum of beliefs or actions associated with radicalization. Adverse community responses to online radicalization pathways remain a topic for additional empirical study [6]. While the various intervention strategies examined capture the complexities associated with the problem, they represent only a subset of potential responses [2]. Future intervention-oriented knowledge synthesis should remain attentive to additional developments in the landscape of online radicalization that may inform strategies relevant to diverse platforms, spaces, communities, and belief systems. Global and cross-platform cases provide a useful insight concerning the dynamics of online radicalization pathways and inform relevant intervention strategies [7]. Recent data and empirical information regarding these platforms, communities, and movements remain limited. Continued efforts to gather and analyse such additional information represent a vital step toward a more complete picture of the phenomenon [1]. Frameworks, models, and responses that remain

cognisant of platform-specific and community-related patterns and developments, while nevertheless focused on bridging different spaces, also represent an important avenue for further elaboration and design [7].

CONCLUSION

Online radicalization represents a complex and continuously evolving phenomenon shaped by the interaction between digital technologies, social networks, individual vulnerabilities, and broader political and social conditions. Although online environments do not inevitably produce extremist beliefs, they provide powerful mechanisms for accelerating radicalization processes by facilitating exposure to extremist narratives, strengthening identity-based communities, amplifying harmful content, and enabling connections across geographical boundaries. Network dynamics such as echo chambers, algorithmic recommendation systems, micro-communities, and cross-platform migration demonstrate that radicalization pathways are increasingly decentralized, adaptive, and difficult to address through traditional security approaches alone. The evidence reviewed highlights that effective responses must move beyond content removal and surveillance-based interventions toward comprehensive strategies addressing the social, psychological, technological, and community dimensions of radicalization. Individual-level interventions, including early identification of risk indicators and support for vulnerable users, must be complemented by platform-level measures that promote responsible algorithmic design, transparency, and meaningful content moderation. Similarly, community and educational interventions remain essential in strengthening resilience, improving digital literacy, reducing social exclusion, and providing alternative sources of belonging and identity. Despite significant progress in understanding online radicalization pathways, important gaps remain. Limited access to platform data, inconsistent evaluation frameworks, ethical concerns surrounding monitoring practices, and the rapidly changing nature of digital spaces continue to challenge researchers and policymakers. Future approaches should prioritize evidence-based, cross-platform, and context-sensitive interventions that recognize the diversity of extremist movements and online communities. Ultimately, combating online radicalization requires a balanced and collaborative framework involving governments, technology companies, civil society organizations, researchers, educators, and communities. Sustainable prevention depends not only on disrupting extremist networks but also on addressing the underlying grievances, vulnerabilities, and social conditions that allow radical narratives to gain influence. A comprehensive understanding of network dynamics therefore provides a critical foundation for developing effective, rights-respecting strategies to reduce the risks associated with digital radicalization.

REFERENCES

1. Binder JF, Kenyon J. Terrorism and the internet: How dangerous is online radicalization? *Front Psychol.* 2022;13:997390.
2. Vidino L, Kilberg J, Lefkowitz J, Kohlmann E. *Terrorist Chatter: Understanding What Terrorists Talk About*. Washington (DC): Program on Extremism, George Washington University; 2015.
3. Törnberg P. Echo chambers and viral misinformation: Modeling fake news as complex contagion. *PLoS One.* 2018;13(9):e0203958.
4. Ledwich M, Zaitsev A. *Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization* [Internet]. 2019 [cited 2025 Jul 21]. Available from: <https://arxiv.org>
5. Pansanella V, Rossetti G, Milli L. From mean-field to complex topologies: Network effects on the algorithmic bias model. *Appl Netw Sci.* 2022;7(1):67.
6. Valentini D, Lorusso AM, Stephan A. Onlife extremism: Dynamic integration of digital and physical spaces in radicalization. *Front Psychol.* 2020;11:524.
7. Mughal R, DeMarinis V, Nordendahl M, Lone H, et al. Public mental health approaches to online radicalisation: An empty systematic review. *Front Public Health.* 2023;11:1172927.

CITE AS: Kakungulu Samuel J. (2026). Online Radicalization Pathways: Network Dynamics and Intervention Syntheses. NEWPORT INTERNATIONAL JOURNAL OF LAW, COMMUNICATION AND LANGUAGES, 6(2):66-72
<https://doi.org/10.59298/NIJLCL/2026/6.2.6672>