©NIJCIAM
Publications Online

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770

NEWPORT INTERNATIONAL JOURNAL OF CURRENT ISSUES IN ARTS AND MANAGEMENT (NIJCIAM)

Volume 7 Issue 1, Page 1-9, 2026



https://doi.org/10.59298/NIJCIAM/2025/71.1900

# Online Radicalization Pathways: Social Network Dynamics and Interventions

**Asuman Banywana**

**Humanities Education Kampala International University Uganda**

**Email** asuman.banywana@studmc.kiu.ac.ug

## ABSTRACT

Online radicalization is a complex, multi-stage process in which individuals adopt extremist ideologies through digital channels, often reinforced by social network dynamics and algorithmically curated content. Unlike offline radicalization, online pathways are shaped by the unique affordances of digital platforms, including rapid information dissemination, echo chambers, homophily, and the influence of automated agents or bots. Exposure to extremist content, reinforcement of grievances, and identity formation are central mechanisms driving online radicalization, while recommendation systems and algorithmic personalization amplify engagement with radical narratives. Empirical studies highlight the interplay between online and offline environments, the role of social networks in information diffusion, and the potential for intervention strategies at platform and community levels. Effective countermeasures include digital literacy programs, narrative-based interventions, platform-level design adjustments, and policy frameworks that balance safety, privacy, and free expression. Despite advances, gaps remain in understanding causal mechanisms, the interaction between online and offline networks, and comparative patterns across ideological groups, underscoring the need for further multidisciplinary research.

**Keywords**: Online radicalization, Social network dynamics, Echo chambers, Algorithmic personalization, and Counter-radicalization interventions.

## INTRODUCTION

Radicalization is a process through which individuals adopt extreme political, social, or religious ideologies that advocate for violence [1]. Pathways are the distinct routes observed during the radicalization process. Online radicalization refers to radicalization that occurs in digital environments, rooted in the notion that not all radicalization takes the same form, and that understanding the common pathway is essential for the effective prevention of radicalization. Online radicalization is widely regarded as an important and dangerous security threat [1]. Online processes can differ substantially from those observed offline [1]. The online arena introduces new spaces for information sharing, discussion, and deliberation that were largely absent prior to the Internet. Information can now be easily, rapidly, and cheaply disseminated across large distances [2]. Online platforms serve as central points for the mobilization and interaction of interested individuals. Social media platforms heavily influence the content an individual engages with, and can expose them only to messages that reinforce, rather than challenge, their existing viewpoints [2]. Radicalization has been widely studied, yet little is known about the processes that characterize radicalization through online channels. Most research has focused on the radicalized individual their personal history, beliefs, and social milieu, rather than the social networks that determine the flow of influence and the diffusion of information [3]. Few studies examine the connections between individuals who become radicalized online, the structures of those social networks, and the changes that occur during the radicalization process. Even less attention has been paid to how online radicalization differs from offline

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770


radicalization [3]. Online radicalization is believed to follow a different trajectory from offline radicalization, but specific differences remain unspecified.

**Theoretical Foundations of Online Radicalization**

Radicalization is a multi-step process leading from values and beliefs that accept radical means of dealing with grievances to support for a change in the existing political, social, or religious order as violent as terrorism. Factors and mechanisms that have been associated with radicalization include the interaction with (perceptions about) radical peers and networks, social identity change, exposure to radicalizing narratives, grievance amplification, and support for radical behavior [3]. While these processes have mainly been studied in offline contexts, online channels are especially relevant given the observed increase in extremist discourse. Among the factors that could contribute to radicalization in online environments, echo chambers that emphasize messages favoring or opposing particular groups, social network structures that experience a surge in such messages, and social media algorithms that promote increasingly polarizing content are especially prominent [4]. By focusing on the mechanisms driving radicalization dynamics rather than on empirical accounts of online radicalization itself, it is possible to delineate both the nature of radicalization in online contexts and the conditions under which it occurs [6]. Within the online literature, exposure, reinforcement, and identity formation constitute three distinct but interrelated processes and are examined in terms of how they relate to escalating support for antisocial attitudes and their antecedents. Taken together, the accounts suggest that the radicalization of attitudes during social-media use relies on a self-reinforcing mechanism–it is not merely an inevitable outcome of such use but typically requires specific types of exposure to content, groups, and networks[5].

**Social Network Dynamics Driving Radicalization**

The social and political phenomenon of radicalization towards violent extremism is closely linked to information exchanged within social networks. A social network consists of individual entities, or nodes, that are connected through one or more relationships [4]. Its structure, therefore, defines the flow of information and resources, including ideas, memes, and emotional appeals. These processes control how agents influence and are influenced by others. Social networks can be segmented into communities that are more densely connected within themselves than with the rest of the network. These communities can also act as echo chambers, reinforcing a shared worldview. Agents may also cluster toward specific identity groups, usually based on social and cultural attributes, thereby amplifying in-group favoritism and out-group hostility [5]. Depending on the overall structure of the network, these processes may lead to a strategic separation of opinion and increasingly polarized opinions. Patterns of influence may vary between groups. Some may exert a major influence on the direction of the group's views and choose the most relevant moment to express their opinion, while others may interact more to trigger or reinforce the choice without actually determining it [7]. These differences are critical to determine the evolution of group opinions. Other patterns may involve networks of bots that support specific opinions and in-group activities both during and before important events. Bots may also coordinate to interact with and influence specific agents of the network, extend the reach of a tweet, and change the perceived importance of a topic or opinion[3].

**Network Structure and Information Diffusion**

Understanding how online radicalization occurs involves knowing online radicalization pathways, the context in which information travels, and the role social media plays in transmitting discourse associated with radicalization or violent extremism[5]. Efforts to grasp online radicalization have often modeled the Internet as a resource or an infrastructure for propagating other ideas. However, specific patterns can emerge within networks of individuals over time [5]. Online radicalization occurs when individuals progress toward extremist views or behaviors. Pathways describe the dynamics and interactions that occur over time [2]. Radicalization depends partly on the transmission of discourse related to extremism. Understanding network structure and how information disseminates across networks is essential to clarifying online radicalization. Structure encompasses persistent geographic patterns and shapes interactions and the nature and reach of exposure. Information diffusion indicates how ideas and content spread online, including shared posts, retweets, or memes. The focus is on those seeking extremist content and those exposed to it through networks [6]. Starting from an information diffusion perspective, radicalization has occurred in various online interaction forms, from informal chats in Internet Relay Chat rooms to live-streamed terrorist attacks. Each platform has different affordances, norms, and moderation practices that shape engagement and dissemination [6]. Online discourse around radicalization or violence spans platforms such as YouTube, 4chan, Reddit, Twitter, Telegram, and Discord. Radicalization can reach audiences beyond initial recipients through network structure and information diffusion pathways. Online platforms alter how context, meaning, or normative legitimacy relate to content [3].

**Echo Chambers, Polarization, and Homophily**

The tendency to associate with similar others is a fundamental phenomenon in social and communication science known as homophily. Social networks exhibit a clear preference among individuals for connections with others like

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770


themselves [3]. Substantial evidence suggests that individuals are more likely to connect with others who resemble them in terms of demographic attributes, opinions, and values. As a result, characteristics such as political orientation tend to influence who individuals follow and with whom they interact, leading online discussion spaces to segment along the lines of shared beliefs. Segregation of this sort is one of the elements of social polarization [4]. Polarization encompasses the distribution of attitudes and opinions over a given range where agents are ultimately either pro- or anti-a position 3. Polarization arises when political disputes in society escalate to the point where consensus among the majority is no longer possible, and individuals begin to segregate in terms of their beliefs and values. Underlying mechanisms that drive the emergence of polarization are a hotly debated subject among academia [4]. The emergence of pocketing or echo is not confined to the online debate and has also been observed in offline discussions. By contrast, polarization tends to be much more conspicuous in online platform discussions. Such behaviors take place at a faster pace, allowing rapid catch-up among the trends to evolve away from public demands [5].

**Influence Agents and Coordinated In-Group Activities**

Classifying nodes based on their activity patterns provides insight into the roles of various actors within a network and helps in identifying possible areas of intervention or disruption [6]. Influence agents have been shown to lead trends and interact with non-radical users to initiate their transition toward extremism. Social bots can exploit this vulnerability , although they mostly RP content, and the scale of the amplification contributes less toward content engagement[3]. The impact of bots is also mediated by the level of engagement of their followers, suggesting that disinformation campaigns by bots might thrive in the lack of interaction among human users [5]. The consideration of bots as a non-human resource might also be valid when observing how, on certain occasions, part of their activity is synchronized to increase the reach of in-group activity. When this strategy of cross-feeding within the group is stable and recurrent, the bots should actually be constituted as nodes with a special status in the network infrastructure. The role of automated users, thus, is twofold: they act essentially as a megaphone for the group, but also connect different content producers and amplify in-group activity[4]. In general, the patterned roles undertaken by the community supporters – different profiles linking different user behaviors are mirrored in the clearly divergent information dynamics developed by pro-ISIS and anti-ISIS communities [5]. In both cases, such asymmetry serves to amplify different narratives and confirm viewers' prejudices. The evidence of in-group RPs in the pro-ISIS setting, where insider influence agents' RPs are either followed by others or are the only followers, adds the dimension of complementarity and possible coordination to the interactive segregation detected by other analyses[6].

**Mechanisms of Radicalization in Online Contexts**

Exposure to extremist content and group narratives is the starting point for an online radicalization journey, which consists of radicalization but stops short of verification and operation [1]. The online dimension is distinct because individuals can enter the radicalization pathway without any social interaction (Neo, 2019). Instead, grievance and immersion are identified as important factors that can operate or advance radicalization alone [3]. Algorithms personalize exposure by predicting the content and accounts to which users will pay attention, which moulds their perspectives, attitudes, and behaviours. The cycles of exposure and reinforcement thereby prevent users from acquiring or being exposed to contrary or diverse information [5]. In addition, group-polarized deliberation further modulates attitudes, which can radically evolve within a few weeks of exposure.

**Exposure, Reinforcement, and Identity Formation**

Online content exposes individuals to radical ideas and movements, potentially catalysing a sequence of events leading to exposure and acceptance of extremist ideas: these include increased consumption of risk content, reinforcement of grievances, transformative grievance narratives, and collective identity framing, but few empirical studies assess such processes [3]. Prior research identifies focus mechanisms within online settings: grievance framing is critical in radicalisation. Exposure to radical ideas leads individuals to situations where risk-reinforcement occurs. Identity framing mechanisms include collective identity narratives that may facilitate escalation to ideological extremism in risk contexts [1].

**Algorithmic Personalization and Recommendation Systems**

Radicalization mechanisms often exploit platforms' algorithmic personalization, with feed-driven attention loops intensifying impact. Algorithmic personalization shapes online experience based on inferred preferences, intent, and behavior metrics [7]. While central for effective information delivery, factors such as user settings, behavioral signals, and interactions with specific content also inform "predictive" selection processes employed by social networks [4]. Repeat engagement, combined with positive feedback through likes, shares, or new followers, amplifies dissemination, resulting in attention-driven "popularity signals." Recommendation systems develop interest-based sequences through information channels offering tailored suggestion features [3]. Content similarities form the basis for link-strength estimation, channeling user attention toward likely applicable

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770


information. Channel popularity signals leverage aggregate user behavior and activity levels to direct attention toward potentially captivating posts, videos, or image messages [5]. Content producers strategically time activity to maximize reach through feed-driven diffusion, while active followers enhance proximity to the suggestion logic [2]. Unlike Twitter and YouTube, Facebook feeds operate based on a customization model that remains economically opaque. The personalized nature of the Facebook news feed can lead to the social reinforcement of unwarranted beliefs or unfounded fears[4]. Evidence demonstrates that valid health information recommended by others, sequentially bolstering similar posts, may backfire and lead users toward misdiagnosis of appreciated symptoms [5]. Despite early marketing strategies portraying Facebook as a representation of a social graph, survey data reveal prevalent exposure to content coined as soft news. Because the content selection process is based on a custom-tailored logic, actual post engagement levels play a minimal role in feeding exposure moderation [3]. In addition to platform recommendation algorithms, the attention mechanism entails algorithmically driven feed loops across online social networks. Information naturally flocks to and consolidates within a selected location, guiding follower exposure and stimulating repetition in the information experience. These processes can create visually appealing images, but their cartoon-like feature is that repetition of the same stimulating event, cortical response grows and, beyond a certain point, becomes negatively valenced, leading to avoidance [6]. User-produced and follower-engaged social signals guide group-aggregated attention regulation in a cumulative logic emphasizing novelty-seeking behaviors, such that the popular news feed principle steers attention to hitherto unencountered information [7].

**Role of Content Moderation and Platform Design**

Content moderation and platform design play a crucial role in addressing radicalization online. Social media has been used to facilitate radical political engagement and has contributed to movements like the Arab Spring [4]. While social networks mediate information, they can also filter and shape perceptions, impacting political and violent radicalization [3]. Although extremist content like videos and images can act as catalysts for radicalization, evidence suggests it is not the sole cause of violent radical actions. The threat posed by the Internet is often framed by whether radical content leads to violence, with policy focus on its potential to radicalize individuals into terror attacks [2].

**Empirical Evidence and Methodologies**

The empirical literature on online radicalization is broad and diverse. It includes a variety of approaches, qualitative and quantitative, theoretically driven or exploratory, cross-sectional or longitudinal, observational or experimental, and directed toward the analysis of contents (e.g., messages, videos) as well as social network dynamics [4]. Consequently, the empirical evidence presented here does not exhaust the richness of the state of play. Instead, the goal is to highlight a few selected studies that measure radicalization pathways in line with the framework outlined in previous sections. Data sources and measurement strategies are described to facilitate exploration of additional evidence [5]. Frameworks for describing empirical evidence and testing expectations fall within and outside the online radicalization pathway perspective. Although the notions of exposure and shaping are admittedly helpful for describing and interpreting results, the discussion of empirical studies is organized around study designs, ranging from cross-sectional to quasi-experimental [6].

**Cross-Sectional Analyses of Online Communities**

Empirical assessments have examined the interrelations between self-reported exposure to radical views on social media and reported attitudes, actions, and intentions in both offline and online communities [7]. These analyses often examine communities in cross-sectional proximity to a real-world violent terrorist incident, assessing whether exposure to violent extremist content propagandistic or glorifying in nature is associated with extreme attitudes, intention to engage in extreme actions, or willingness to support extreme actions [5]. Evidence suggests that stronger exposure to radical material from one's own group is associated with more extreme predispositions or attitudes. Exposure to actual hateful content cross-sectionally predicted intentions to engage in hateful actions [2]. A similar pattern holds for intention to join a terrorist group, being positively predicted by the amount of exposure to the actual group's content and negatively predicted by the amount of exposure to the opposing group's hateful content. In the context of planned mass shootings, exposure to content denying the Holocaust is associated with self-reported support and/or engagement in actual group activities [3]. A further study assessing self-reported exposure to radical material during the 2019 Christchurch shooting found correlations with willingness to undertake supportive actions, including visitation of the attackers' memorial page and joining the attackers' channel on a messaging application[3]. Exposure to such kinds of content is thus linked with reported real-world behaviors, with cross-sectional evidence suggesting that exposure to such hateful content may support engagement in actual actions. However, the patterns of exposure to radical content as a moderator or predictor of attitude towards different actors during a polarized event have not reached a consensus[4]. Research employing Twitter data around the Black Lives Matter protest and counter-protests in 2020 suggested that the

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770
pattern of attitude towards the two opposing groups had a negligible association with the personal echo chamber's content [6].

**Longitudinal Studies and Causal Inference**

Longitudinal studies are essential for understanding the processes of radicalization and causal relationships. Future research should define the similarities and differences between extremists and make comparisons within and outside ideological groups, as well as with other criminal groups [5]. Studying online extremist activities can shed light on mechanisms of online radicalization, and creative methods are needed to access radical populations, such as engaging through social media [6]. Because populations are inaccessible, reliance on multiple imputation techniques is necessary for handling missing data, though these depend on assumptions that may not always hold [5].



**Experimental and Quasi-Experimental Approaches**

Experiments and quasi-experiments provide insight into counter-radicalization strategies. They allow concepts or frameworks from other fields to be operationalized and tested for generalizability to online radicalization contexts [5]. The extreme multiplicity of online pathways to radicalization and the associated potential for any given dataset to provide only partial insights suggests that experiments, which often mathematically model and then test specific facets of broader processes, have greater explanatory power than areal or longitudinal studies. Experimental interventions can also help test whether centrality, homophily, or echo chambers materially influence engagement with extremist content [4]. Existing evidence supported a similar hypothesis that greater exposure to misinformation heightens further engagement, underlining the need to understand platform dynamics, content moderation, and influence agent support in radical pathways [3]. Designs tackling ethical and practical constraints, e.g., time-honoured two-sided concealed training-wave schemes, lower non-internal validity while preserving direct applicability and trackable consequences. Moreover, enhanced incentives, formal recognition, and adaptability increase intrinsic motivation and, thereby, project sustainability [5].

**Interventions and Countermeasures**

One promising avenue for curbing online radicalization involves countering the underlying motivation to seek antisystem narratives [6]. Narrative-based counter-messaging highlights the implications, pitfalls, and lack of fulfillment associated with violent extremism while presenting alternative narratives that satisfy the same grievances and desires. Such exploitation of the motivation to connect with antisystem narratives requires knowledge of the psychographic and behavioral tendencies that illustrate an ongoing need for such narratives. Grievance-based radicalization pathways are evident across the spectrum of extreme ideologies and social movements [7]. Therefore, counter-narratives that address the narrative grievances in many destructive pathways remain applicable even while specific concerns change [5]. Yet many systems designed to reduce recruitment fail to address ongoing radicalization through group messages that exploit narratives properly boxed into recruitment. Intervention against these ongoing narrative-fed pathways constitutes an important issue for governments, social organizations, and academic researchers alike [4].

**Platform-Level Interventions and Policy Implications**

Direct Action Intervention is defined as "interventions in a social system designed to stimulate immediate activity toward predetermined goals"[3]. Advocacy includes "direct action to insert issues into the agenda of public, social, organisational, or political decision makers", policy thereby representing "initiatives of governmental authorities". Radicals, extremists, and terrorists share common grievances with elements of the social system who see themselves as disadvantaged or deprived [4]. The radicalisation process itself can thus be seen as a form of collective action where grievances or discontents are brought into the open and discussed [3]. Platform-level interventions consider structural characteristics of platforms, such as group involvement or breaking connectivity between new arrivals and other users. Interventions can prevent exploitation of structural properties that favour radicalisation while preserving democratic availability of the underlying communication channels. Applying delays to messages sent by a user who just joined a group lessens the potential for engagement with radical content early in the user–platform relationship [4]. Zero tolerance on pre-existing channels or groups would need to transfer to a less radical new group before a recommended group was shut down. Configuration proposing a reduced recommendation for groups, channels, or follows suggestions as a User Just Joined Interventions. New follow recommendations for those with high potential to influence or shape user preferences are avoided. Scope emphasis on recommended groups would assist in identifying the presence of a wider ecosystem. Aesthetics, constituting freedom of expression, human rights, or protection from discrimination, can further assist in listening to grievances and contextualising extremist content [5]. Policy measures catering to counter-violent extremism interventions financed through legally constituted channels could be envisaged. These allow access to legitimate parliamentary debate or steps on grievances without pre- or post-conditions by the state [6]. Flexible, adaptable policy measures designable through legally constituted AVEC channels would be needed for issues that require

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770


continued presence within the public space. Grievances might be heard without added socio-economic conditions being imposed. Such platform-level pre-interventions address existing platform subgroups before any transition may be considered [6].

**Community-Based and Educational Interventions**

Community-based and educational interventions are crucial to countering radicalization. The internet supports radicalization, but offline influences, especially peer groups and families, remain decisive [2]. Numerous studies confirm that online terrorist trajectories parallel offline pathways, reinforcing the need to address both environments. The relationship between online and offline influences, rather than merely the digital component, remains central in understanding the process [4]. Engagement strategies focus on underserved audiences and marginalized groups not targeted by major online communities [2]. Content creation or outreach targets offline grievances. Narrative-driven approaches promote counter-speech and substitute dominant narratives with widely shared cultural templates, values, beliefs, or strategies on grievances ignored by mainstream actors. Participants in such interventions report increased visits to radical spaces, legitimizing outreach efforts [3].

**Digital Literacy and Critical Evaluation**

Digital Literacy, Critical Evaluation of Digital Resources, and Engaging Action Competencies reduce exposure to extremist content, nurture digital competence, and encourage tolerance, creativity, and participative culture while promoting structure for information decoding and critical evaluation of values embedded in the material [7]. Youngsters are also encouraged to analyse how extremism manipulates public discussions, to scrutinize the rise of hate speech, and to develop specific counter-messages [2].

**Evaluation of Intervention Effectiveness**

A variety of metrics have been proposed to assess the effectiveness of interventions, including prescriptive and descriptive evaluations, behavioral and attitudinal indicators, process-versus outcome-oriented analyses, long-versus short-term time frames, and computational versus survey-based approaches[6]. Interventions have been examined at different levels and with varying comparisons, including broad assessments where measures are not necessarily tied to the specifics of targeted processes or counter-strategies, comparisons not suited for general conclusion drawing, and analyses that do not convey programs- or policies-specific insights on the breadth or nature of target behavior [5]. The types of interventions and comparison frameworks analyzed in the literature, alongside the most commonly adopted methods, measurement instruments, and reported outcomes, can therefore help identify salient features of online radicalization, inform the design of future efforts, and facilitate knowledge transfer across disparate discourses [3].

**Ethical, Legal, and Social Considerations**

Online radicalization raises prominent ethical, legal, and social concerns. The ecosystem of public online discourse embraces diverse views on politically sensitive topics, often entangled with explicit or subtle calls to action or group identity formation [7]. Although unfettered expression is heralded as a marker of healthy democracy, it produces harm, notably through the hateful targeting of minorities, including migrants and other groups; political violence, threats, and intimidation; the denial of historical injustices; the promotion of the acceptance of unjustified privileges; and other concrete safety concerns [4]. These harms shape debates on the boundaries of free expression and incitement, making safety and security considerations central concerns of governing bodies. As a result, social media companies face pressure to moderate online discourse and reshape underlying processes that elevate harmful communication and behavior. Defining whose speech is regulated, in what manner, and how these decisions are executed is not easy [7]. Difficult ethical questions often arise for experimenting and evaluating potential interventions in online spaces, as established procedures for laboratory or field experiments on human subjects are hard to apply when these subjects are immersed in online environments equipped with highly personalized and attention-seeking recommendation systems that filter, prioritize, and de-prioritize information according to past actions and declared preferences, often without explicit recall or reprisal from users subject to these manipulations[6]. Distinctions between the provision of information and possible subsequent influence or behaviour of users cannot always be drawn: a mere smiley button to indicate approval may signal whether a sender is a member of an accepted group or a stranger. With the absence of the physical domain, participants' exposure to such layouts and asymmetric interactions cannot be explicitly controlled. Ultimately, these elements also introduce novel issues, such as privacy and confidentiality that remain unresolved [7].

**Free Speech, Safety, and Human Rights**

To sensibly manage free expression at a time of rising discontent, it is crucial to uphold the fundamentals of a democratic society; advocate for a free, open, and secure exchange of ideas; and resist coercive approaches to VR. Such perspectives and actions may constitute a robust foundation for human rights-based and free-speech-centred efforts to mitigate radicalization effectively [5]. The first priority is to place existing violence in a historical context. Any forms of violence that rise must always be carefully compared to previous generations [2]. Such

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770


comparisons may help to offer relevant perspectives regarding any number of comparative dimensions of violence, their potential triggers, and their development [3]. Consideration might encompass the factual volume of violent acts before and after the rise of new media platforms globally. In many instances, existing ground conditions favour the emergence of violent ideas or acts, irrespective of the medium or platform through which they surface; stabilizing those existing ground conditions might be more broadly leveraged in preventing radicalization. Trends and patterns of violence evident globally during past decades provide yet another benchmark for making fuller assessments about the relative severity of contemporary processes [2]. Efforts to broaden the scope of free expression by allowing consideration of non-violent, less extreme views in conjunction with consideration of violent, extreme views open the present debate to comparisons with the much longer historical trajectory of such views, dating back centuries to at least the French Revolution or earlier[1].

**Privacy, Surveillance, and Data Ethics**

The literature illustrates various awkward aspects of privacy, surveillance, and data ethics in social media open to automatic collection of data and its dissemination [3]. Consent is a key principle informing ethical engagement with social media data, and exercising control over its use often relies on the actions of platforms or other intermediaries [4]. Furthermore, social media platforms remain opaque on their data policies. While personal information is removed from such data sets, authors are normally not informed how exactly the collected data is being managed, nor made aware of the enduring nature of social media footprints even after deletion. Some researchers, however, rely on this previously collected data despite attribution implications [6]. Current data-sharing practices tend to extend detrimental socio-economic inequality by privileging developed over emerging nations. The Philippines, for example, has emerged as both a relative leader in social media engagement and the major supplier of verbal content moderation for providers currently removing collation of data labelled as human rights violations from broad commercial offerings[5]. Academic engagement with these data-sharing practices thus appears necessary and urgent [2].

**Responsible Innovation and Accountability**

To rein in radicalization online, it is critical to take a whole-of-society approach that attends to situational characteristics and needs. Governance structures and oversight mechanisms should bear this in mind. In this regard, the paradox of regulated freedom comes into play [3]. When properly regulated, freedom of expression can help combat radicalization by reducing grievances and social exclusion. The problem grows when voices calling for moderation reach an overwhelming volume, to the point where others feel pressured to conform and self-censor. Even substantial freedom for violent extremists can serve broad social objectives when safeguards are built into governance systems [2]. Wherever the boundaries of freedom are drawn, however, it is essential to foster experimentation with a view to discovering the best governance structures and oversight mechanisms, and to enable rather than suppress designers to assist society in this endeavor [6]. Some industry leaders have a vested interest in such experimentation, but there are also widespread calls from civil society to develop tools for safety while preserving freedoms both online and offline [3]. Domain-range factors and the problem of escalation exacerbate the urgency of the situation. Restrictions placed on internet use are frequently counterproductive, but in an online world where time appears less significant, people can nevertheless be drawn into violent extremism over exceedingly short periods, prompting the need for precautions [1].

**Case Studies and Comparative Perspectives**

Online platforms are not replacing offline radicalization processes but are facilitating them. The Internet is a complementary tool that provides access to potentially radicalizing content and connections with like-minded individuals [5]. As a consequence, empirical analyses of radicalization phenomena observed in physical environments may have validity in virtual environments. Radicalization has been characterized as a process that exhibits different stages. In the context of violent extremism, scholars propose a typology consisting of five interdependent stages, namely: (a) pre-radicalization, (b) self-identification, (c) indoctrination, (d) action initiation, and (e) conversion. These stages have been used to explain the pathways leading to the involvement of individuals in violent groups and terrorist activities. A similar typology can be found in the radicalization model developed by the study of violent extremism [4]. The principles that underlie the gradual escalation towards violent extremism reflect a universal trend that remains inflexibly valid across geographies. The individual psychological characteristics of radicalized persons and the contingent socio-historical context from which they emerge may vary widely. Yet, the foundational dynamics that support the emergence and perpetuation of radical groups are template-like and may broadly be termed radicalizable sources [6]. Because radicalization continues to occur in offline environments, many scholars predict the emergence of different online radicalization trajectories. Trends of global radicalization, followed by the COVID-19 pandemic, have diffused attention and specialized study of the online component of radicalization. Such analyses have nevertheless been regularly undertaken around the world since before the pandemic in many different geographic and institutional contexts [6]. Research shows that online

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770
participation in social media services is consistent with the radicalization of individuals without prior historical records of violent behavior who subsequently initiate and attempt to mobilize fellow citizens toward achieving violent objectives [6]. Based on the material made available and the interaction patterns observed, a preliminary account of some of the interdependent processes believed to be significant in the radicalization of individuals in the online domain has been assembled. Social networks, nevertheless, remain key facilitators in radicalization because online and offline participation typically coalesce. Individuals regularly interact in both venues, and violence is often physically planned in public places of congregation, such as parks, before being executed [5].



**Gaps in Knowledge and Directions for Future Research**

Online radicalization pathways: social network dynamics and interventions, despite an active scholarly discourse on online radicalization, several topics warrant further exploration. Future inquiries may consider the following priority questions [5]. Investigating the similarities and differences between extremist groups, defining the distinctions among extremists remains critical; future investigations should explore commonalities and contrasts both within and beyond the radical ideology and examine other criminal counterparts. Particularly pertinent, radicalization parallels with joining legal movements constitute a potentially fruitful line of inquiry [5]. Examining behavioural patterns and experiences in extremist settings, to gain deeper knowledge of the mechanisms underpinning online radicalization, it is essential to understand individuals' actions and experiences in extremist digital environments [5]. Direct contacts with extremists through social media and analogous creative approaches may be employed to access populations otherwise unavailable to researchers. Improving data accessibility and facilitating causal attribution, the collection of primary data is severely impeded by security threats in numerous war-afflicted countries [7]. Relaxed political tensions could enable fieldwork in non-threatening territories, while publicly available datasets, such as the Global Terrorism Database or the Open Source Centre, provide valuable information without exposing researchers to substantial jeopardy. Many investigations still depend on secondary sources, including news articles and gray literature. These limitations preclude causal attribution and call for methods such as multiple imputations to manage incomplete datasets, despite the inherent constraints [5]. Acknowledge the interaction of online networks and physical bonds; the reciprocal interplay between online affiliations and offline ties is insufficiently recognized. Treating virtual realms as distinct from real-world interactions oversimplifies the online radicalization issue; existing approaches neglect to investigate the persistent integration of the digital and physical domains and remain agnostic toward the individuals' location, whether in a war zone or a politically tranquil area. Future research should therefore bridge this pertinent gap [7].

**CONCLUSION**

Online radicalization represents a distinct and evolving challenge that integrates technological, social, and psychological dimensions. Social network structures, algorithmic personalization, and exposure to extremist content collectively shape radicalization pathways, while the interplay between online and offline interactions reinforces ideological commitment. Effective interventions must adopt a multi-level approach, encompassing digital literacy, community engagement, narrative counter-messaging, and platform-level policies that mitigate exposure without infringing on human rights or free expression. Empirical research demonstrates the critical role of network dynamics and content dissemination in shaping attitudes and behaviors, but significant knowledge gaps persist, particularly regarding causal mechanisms and the integration of digital and physical social networks. Addressing these gaps through innovative methodologies and cross-disciplinary studies will enhance understanding of radicalization processes and inform evidence-based strategies to prevent and counter violent extremism in the digital age.

**REFERENCES**

1. Binder JF, Kenyon J. Terrorism and the internet: How dangerous is online radicalization?. Frontiers in psychology. 2022 Oct 13;13:997390.
2. Aly A. Brothers, believers, brave mujahideen: Focusing attention on the audience of violent jihadist preachers. InViolent Extremism Online 2016 May 5 (pp. 106-122). Routledge.
3. Baumann F, Lorenz-Spreen P, Sokolov IM, Starnini M. Modeling echo chambers and polarization dynamics in social networks. Physical review letters. 2020 Jan 31;124(4):048301.
4. Nasim M, Weber D, South T, Tuke J, Bean N, Falzon L, Mitchell L. Are we always in strife? a longitudinal study of the echo chamber effect in the Australian Twittersphere. arXiv preprint arXiv:2201.09161. 2022 Jan 23.
5. Bastug MF, Douai A, Akca D. Exploring the "demand side" of online radicalization: Evidence from the Canadian context. Studies in Conflict & Terrorism. 2020 Jul 2;43(7):616-37.
6. Valentini D, Lorusso AM, Stephan A. Onlife extremism: Dynamic integration of digital and physical spaces in radicalization. Frontiers in psychology. 2020 Mar 24;11:524.

Open Access
Print ISSN: 2992-6114
ISSN: 2992-5770

7. McNicol S. Responding to concerns about online radicalization in UK schools through a radicalization critical digital literacy approach. Computers in the Schools. 2016 Oct 1;33(4):227-38.

**CITE AS: Asuman Banywana (2026). Online Radicalization Pathways: Social Network Dynamics and Interventions. NEWPORT INTERNATIONAL JOURNAL OF CURRENT ISSUES IN ARTS AND MANAGEMENT, 7(1): 1-9.** https://doi.org/10.59298/NIJCIAM/2025/71.1900