Online Radicalisation: Pathways from Grooming to Violence

Dr. Anjali Yadav
Assistant Director, Forensic Psychology Division
Central Forensic Science Laboratory, Delhi, India

***Abstract*—Online radicalisation represents one of the most pressing security and psychological challenges of the digital era. This manuscript examines the multistage pathways through which individuals are groomed and subsequently drawn toward violent extremism via online platforms. Drawing on empirical research from behavioural sciences, terrorism studies, and clinical psychology, the paper analyzes key theoretical frameworks—including the Pyramid Model of Radicalisation, the Three-N Model, and the Significance Quest Theory—to illuminate how digital environments accelerate cognitive, emotional, and social transformation in vulnerable individuals. Specific attention is given to grooming mechanisms such as identity exploitation, incremental commitment escalation, in-group/out-group polarisation, and algorithmic amplification. The manuscript also examines individual-level vulnerability factors (e.g., trauma history, identity uncertainty, social isolation) and structural enablers (e.g., echo chambers, encrypted messaging, gamification of ideology) that facilitate the transition from passive radicalization to active violence. Implications for early intervention, counter-narrative strategies, and platform regulation are discussed. This review underscores the urgent need for transdisciplinary collaboration between psychologists, policymakers, and technology companies to disrupt radicalization pipelines before violent outcomes occur.**

Index Terms*—online radicalisation, grooming, violent extremism, digital terrorism, radicalisation pathways, behavioral sciences, counter-terrorism

I. INTRODUCTION

The proliferation of digital communication platforms has fundamentally restructured the landscape of extremist recruitment and political violence. What once required physical proximity, covert meetings, and geographic coordination can now be accomplished across continents through a smartphone screen. Since the early 2010s, jihadist networks, white nationalist movements, incel communities, and eco-extremist cells have exploited online environments to recruit, indoctrinate,

and mobilise adherents—often with devastating consequences (Berger, 2018; Moonshot CVE, 2020; Neumann, 2013).

Online radicalisation is not a monolithic phenomenon. It involves a complex, iterative process through which ordinary individuals—often psychologically vulnerable—are exposed to extremist content, drawn into ideological communities, and incrementally committed to beliefs that may eventually sanction violence (McCauley & Moskalenko, 2017). The role of digital grooming in this process has received increasing empirical attention (Conway, 2017; Gill et al., 2017), yet a comprehensive behavioral-scientific framework linking grooming mechanisms to violent outcomes remains underdeveloped in the literature.

This manuscript addresses that gap by synthesising existing theoretical models with empirical evidence on online grooming, radicalisation trajectories, and violence onset. The paper is structured as follows: first, key theoretical frameworks are reviewed; second, the mechanisms of online grooming are examined in depth; third, individual and structural vulnerability factors are analysed; fourth, the transition from radicalisation to violence is explored; and finally, implications for intervention and policy are discussed.

II. THEORETICAL FRAMEWORKS OF RADICALISATION

The Pyramid Model

One of the earliest and most widely cited frameworks in radicalisation research is McCauley and Moskalenko's (2008) Pyramid Model, which conceptualises radicalisation as a process of progressive movement from sympathiser at the base to terrorist actor at the apex. The model posits that while many individuals may hold radical opinions, far fewer translate these into radical action—suggesting that opinion radicalisation and action radicalisation are distinct psychological processes. Online environments complicate this framework by collapsing the traditional gatekeeping functions that once slowed progression up the pyramid (McCauley & Moskalenko, 2017).

The Three-N Model

Kruglanski et al.'s (2014) Three-N Model offers a motivational account of radicalisation, positing that extremist violence emerges from the interaction of Need (a quest for personal significance), Narrative (an ideology that frames violence as a legitimate path to significance), and Network (a social environment that validates and reinforces this ideology). This triadic model has particular salience for understanding online radicalisation, as digital platforms serve as powerful network-amplifiers—enabling individuals experiencing significance loss to access narratives of heroic violence and communities that celebrate such frames (Kruglanski et al., 2019).

Significance Quest Theory

Related to the Three-N Model, Significance Quest Theory (SQT) proposes that the fundamental motivation underlying radicalisation is the desire to matter—to achieve a sense of personal

importance and dignity (Kruglanski et al., 2022). Online environments uniquely exploit this motivation by offering outsider individuals the possibility of achieving celebrity status within extremist communities. The anonymous yet hyper-social nature of platforms such as Telegram, Discord, and 4chan enables a kind of 'dark celebrity' through viral content sharing and community valorisation of violent acts (Moonshot CVE, 2020; Neumann, 2013).

The Staircase to Terrorism Model

Moghaddam's (2005) Staircase to Terrorism model uses a physical metaphor to represent radicalisation as sequential ascent through psychological floors, each characterised by distinct cognitive and motivational states: perceived injustice, displacement of aggression, moral engagement and disengagement, categorical thinking, and finally, sidestep inhibitory mechanisms toward violence. This model has been critiqued for its linearity (Horgan, 2008), but it retains utility as a heuristic for understanding how online grooming systematically targets individuals at each level, providing justifications and social support that enable upward movement.

III. ONLINE GROOMING: MECHANISMS AND PROCESSES

In the terrorism literature, online grooming refers to a strategic process by which extremist actors identify, target, cultivate, and psychologically prepare vulnerable individuals for radicalization and potential violent action (Conway, 2017; Saltman & Russell, 2014). Unlike child sexual exploitation contexts where grooming is typically dyadic, terrorist grooming frequently operates at scale—through mass exposure to propaganda, algorithmically curated content, and community-level socialization—though individualized one-to-one grooming by recruiters also occurs (Gill et al., 2017).

Identity Exploitation

A primary mechanism of online grooming involves the exploitation of identity uncertainty, particularly among adolescents and young adults navigating developmental transitions (Awan, 2017; Wiktorowicz, 2004). Extremist content strategically addresses questions of purpose, belonging, and identity, offering what Wiktorowicz (2004) terms a 'cognitive opening'—a moment of existential vulnerability in which radical narratives appear uniquely satisfying. Online platforms enable extremist actors to precisely target such individuals through search engine optimization, social media profiling, and community infiltration of mainstream spaces (Berger, 2018).

Research on former extremists consistently identifies identity crises—related to migration, discrimination, failed relationships, or career disruption—as precipitating vulnerabilities exploited by online groomers (Horgan, 2008; Bjørgo, 2009). Digital platforms enable groomers to identify these moments of vulnerability through behavioral cues such as search history, comment sentiment, and community activity, and to intervene with precisely calibrated messaging (Neumann, 2013).

Incremental Commitment Escalation

Online grooming characteristically proceeds through incremental steps that gradually escalate commitment to extremist beliefs without triggering premature rejection (Saltman & Russell, 2014). This process mirrors the 'foot-in-the-door' technique documented in social psychology (Freedman & Fraser, 1966): initial exposure to moderate critiques of society is followed by progressively more radical content, until individuals find themselves consuming materials advocating violence without having experienced a clear break from their prior values. The algorithmic architecture of platforms such as YouTube and TikTok has been documented to facilitate this escalation by serving increasingly extreme content to users who engage with ideologically adjacent material (Moonshot CVE, 2020; Ribeiro et al., 2020).

Social Bonds and In-Group Formation

A third mechanism involves the deliberate cultivation of social bonds within extremist communities. Online radicalisation is rarely a purely cognitive process; it is fundamentally social. Extremist online communities offer belonging, camaraderie, humour, and collective identity—affective rewards that are particularly powerful for socially isolated individuals (Berger, 2018; Sageman, 2004). Grooming processes leverage these bonds through community rituals, shared language and memes, collective grievance narratives, and the establishment of in-group/out-group boundaries that deepen commitment and reduce the salience of external social ties (Conway, 2017; Kruglanski et al., 2019).

Research by Sageman (2004) on global Salafi jihad networks demonstrated that friendship and kinship bonds within cells were more predictive of recruitment than ideological attraction per se—a finding extended to online contexts by subsequent scholars (Gill et al., 2017). Online platforms enable the formation of intense pseudo-familial bonds among geographically dispersed individuals who may never meet in person, yet exhibit strong commitment to collective violent action (McCauley & Moskalenko, 2017).

Moral Disengagement and Dehumanisation

Bandura's (1990, 1999) theory of moral disengagement provides a critical explanatory lens for how individuals who are generally opposed to harming others become capable of perpetrating or endorsing mass violence. Online grooming systematically deploys moral disengagement mechanisms including: euphemistic labeling of violence ('operations,' 'defensive jihad'), advantageous comparison with ostensibly worse historical violence, displacement of responsibility onto authority figures or ideological necessity, and dehumanisation of target populations through repeated exposure to derogatory representation (Moonshot CVE, 2020; Saltman & Russell, 2014). Digital propaganda is particularly efficient at fostering dehumanisation due to its capacity for visual saturation: repeated exposure to dehumanising imagery, memes, and narrative frames targeting specific ethnic, religious, or political groups progressively desensitises individuals and normalises violent attitudes (Berger, 2018; Awan, 2017).

IV. INDIVIDUAL VULNERABILITY FACTORS

Psychosocial Risk Factors

Empirical research has identified a constellation of individual-level vulnerabilities that heighten susceptibility to online radicalization. These include but are not limited to: social isolation and loneliness, experiences of discrimination or perceived injustice, trauma history, mental health difficulties (particularly personality disorders and mood disorders), low self-esteem, identity confusion, and a history of seeking belonging in group contexts (Horgan, 2008; Neumann, 2013; Awan, 2017).

It is critical to note, however, that no single psychological profile reliably predicts radicalisation, and most individuals with these vulnerabilities do not radicalise (Gill et al., 2017; Horgan, 2008). The relationship between psychosocial vulnerability and radicalisation is probabilistic and contingent on environmental triggers—including online exposure—rather than deterministic. Overreliance on psychological profiling risks stigmatising vulnerable groups and has been criticised for poor predictive validity in counterterrorism contexts (Horgan, 2008; Sageman, 2014).

Cognitive and Motivational Factors

At the cognitive level, susceptibility to radicalisation has been associated with need for cognitive closure (Kruglanski et al., 2014)—a motivational orientation toward clear, unambiguous answers—as well as black-and-white thinking, susceptibility to conspiracy belief, and a tendency toward grievance-based worldviews. Extremist online content is strategically designed to satisfy these cognitive needs by offering simple, morally absolute narratives that explain complex social suffering through the identification of clear enemies and heroic remedies (McCauley & Moskalenko, 2017; Kruglanski et al., 2022).

V. STRUCTURAL AND ENVIRONMENTAL FACILITATORS

Algorithmic Amplification and Echo Chambers

The architecture of contemporary social media platforms plays a significant structural role in facilitating radicalisation by promoting content that maximises engagement—which algorithmic research consistently demonstrates correlates with emotional arousal, outrage, and divisiveness (Moonshot CVE, 2020; Ribeiro et al., 2020). Recommendation algorithms on platforms including YouTube, Facebook, and Twitter have been documented to create 'rabbit holes'—escalating sequences of increasingly extreme content—that progressively expose users to radicalising material without active seeking behaviour (Ribeiro et al., 2020).

Closely related is the phenomenon of the echo chamber: algorithmically and socially curated information environments in which users are predominantly exposed to viewpoints consonant with their existing beliefs (Sunstein, 2017). Within such environments, extremist positions are normalized through repeated exposure and social validation, counterarguments are minimised, and identity-based commitment to radical communities is reinforced (Conway, 2017; Berger, 2018). Research by Moonshot CVE (2020) found that individuals who engaged with extremist content

online showed rapid escalation in consumption of more extreme material, suggesting a compounding effect of algorithmic recommendation.

Encrypted Platforms and Dark Web Forums

A significant structural challenge for counter-radicalisation efforts is the migration of extremist communities to encrypted and decentralised platforms including Telegram, Signal, and various dark web forums, where content moderation is minimal or absent (Conway, 2017; Gill et al., 2017). These environments provide operational security for extremist networks, enable uninhibited dissemination of violent propaganda, and facilitate direct operational planning. Research has documented extensive use of Telegram channels by the Islamic State and white nationalist networks for both propaganda distribution and direct member recruitment (Moonshot CVE, 2020; Neumann, 2013).

Gamification of Ideology

An emerging mechanism in online radicalisation is the gamification of extremist ideology—the use of gaming aesthetics, challenges, ranking systems, and competitive violence framing to engage, particularly, young male audiences (Berger, 2018; Moonshot CVE, 2020). Manifestos associated with mass shooters including the Christchurch attacker have explicitly adopted gaming vocabulary ('high score,' 'achievements'), and subsequent attacks have been framed as part of a competitive challenge. Research suggests this gamified framing may lower psychological resistance to violence by embedding it within familiar ludic frameworks (Moonshot CVE, 2020).

VI. FROM RADICALISATION TO VIOLENCE: THE FINAL TRANSITION

Understanding the transition from radical belief to violent action remains one of the most theoretically challenging problems in terrorism research. The vast majority of individuals who hold extreme views never commit acts of violence, and the factors that distinguish those who do remain incompletely understood (Horgan, 2008; Sageman, 2014). However, several precipitating dynamics have been identified in the online context.

First, the presence of a direct mobilising trigger—such as a real or perceived attack on in-group members, a personal humiliation, or a call to action by an admired figure—appears to catalyse the shift from ideation to action in individuals already embedded in online extremist communities (McCauley & Moskalenko, 2017; Kruglanski et al., 2022). Online environments accelerate the transmission of such triggers globally and in real-time.

Second, social facilitation within online communities plays a critical role. Research on lone-actor terrorists—who by definition act without direct accomplices—nonetheless consistently reveals extensive prior online engagement with extremist communities that provided ideological justification, tactical information, and social validation for planned attacks (Gill et al., 2017). The

community thus serves as a surrogate network that enables violence even in the absence of physical co-conspirators.

Third, access to operational knowledge through online channels—instructions for weapons construction, attack planning guidance, target selection criteria—represents a significant practical facilitator. The Islamic State's multilingual online magazine Dabiq, and its successor Rumiyah, provided precisely calibrated operational guidance for online-inspired lone-actor attacks across Western nations (Neumann, 2013; Moonshot CVE, 2020).

VII. INTERVENTION STRATEGIES AND POLICY IMPLICATIONS

Early Intervention and Prevention

Behavioral-scientific research underscores the importance of early intervention—ideally before radicalisation progresses beyond its initial stages. Programs targeting at-risk youth through school-based resilience education, mentorship, and critical media literacy have demonstrated some efficacy in reducing susceptibility to extremist messaging (Awan, 2017; Moonshot CVE, 2020). The United Kingdom's Channel program, the United States' Countering Violent Extremism (CVE) initiative, and Germany's Beratungsstelle Radikalisierung represent institutional frameworks for early intervention that involve multi-agency coordination between social services, educators, law enforcement, and mental health professionals.

Counter-Narratives and Alternative Narratives

Counter-narrative strategies—direct refutation of extremist claims through competing messaging—have received extensive policy attention, though empirical evidence for their effectiveness remains mixed (Berger, 2018; Saltman & Russell, 2014). Alternative narrative strategies, which shift focus from rebutting extremist claims to affirming positive identities and belonging, have shown greater promise, particularly when delivered by credible former-extremist voices (Moonshot CVE, 2020). Online platforms including Google's Redirect Method, which serves counter-narrative content to individuals searching for extremist material, represent promising technologically-mediated interventions requiring rigorous evaluation.

Platform Regulation and Algorithmic Accountability

Given the structural role of platform architecture in facilitating radicalisation, regulatory frameworks that impose accountability obligations on technology companies represent a critical layer of systemic intervention. The European Union's Digital Services Act (2022) and the United Kingdom's Online Safety Act (2023) represent significant legislative steps, requiring platforms to assess and mitigate risks associated with illegal and harmful content, including terrorist material (Moonshot CVE, 2020). However, tensions between content moderation and freedom of expression, the transnational jurisdiction of online platforms, and the technical sophistication of extremist actors in circumventing moderation remain persistent challenges.

VIII. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

Several important limitations characterise existing research on online radicalisation. First, much empirical work relies on post-hoc case study methodology—examining the online histories of known attackers—which introduces selection bias and limits causal inference (Horgan, 2008; Gill et al., 2017). Prospective longitudinal research, though methodologically challenging given ethical and legal constraints, is urgently needed to map radicalisation trajectories in real time.

Second, the heterogeneity of online radicalisation pathways across different ideological contexts—jihadist, white nationalist, incel, eco-extremist—limits the generalisability of findings across domains. Context-specific research that attends to the distinct dynamics of each movement is needed alongside comparative synthesis (McCauley & Moskalenko, 2017; Berger, 2018).

Third, the rapid evolution of digital platforms—including the emergence of generative artificial intelligence as a potential tool for scalable, personalised extremist content production—requires continuous updating of empirical frameworks and policy responses (Moonshot CVE, 2020). Future research should specifically investigate the radicalisation potential of AI-generated content and synthetic media in online environments.

IX. CONCLUSION

Online radicalisation represents a multidimensional behavioral phenomenon with profound consequences for individuals, communities, and global security. The pathways from initial grooming to violent action are shaped by the interaction of individual vulnerabilities, digital platform architectures, community dynamics, and macrosocial grievances—none of which is sufficient in isolation to produce violent extremism, but which together create trajectories that behavioral science is increasingly equipped to map and interrupt.

NOTE- This manuscript has reviewed core theoretical frameworks, delineated the mechanisms of online grooming, analysed structural facilitators, and examined the dynamics of the radicalisation-to-violence transition. The evidence underscores that effective responses require transdisciplinary collaboration—between psychologists, political scientists, technology researchers, platform designers, and policymakers—alongside sustained investment in rigorous empirical research that keeps pace with the evolving digital landscape.

Ultimately, while no intervention can guarantee the prevention of all online-inspired violence, the behavioral sciences offer indispensable tools for identifying vulnerable individuals, disrupting grooming processes, and building the social and cognitive resilience that constitutes the most durable form of counter-extremism.

REFERENCES

[1] Wan, I. (2017). Cyber-extremism: Isis and the power of social media. Society, 54(2), 138–149. https://doi.org/10.1007/s12115-017-0114-0

[2] Bandura, A. (1990). Mechanisms of moral disengagement in terrorism. In W. Reich (Ed.), Origins of terrorism: Psychologies, ideologies, theologies, states of mind (pp. 161–191). Cambridge University Press.

[3] Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. Personality and Social Psychology Review, 3(3), 193–209. https://doi.org/10.1207/s15327957pspr0303_3

[4] Berger, J. M. (2018). Extremism. MIT Press.

[5] Bjørgo, T. (2009). Leaving terrorism behind: Individual and collective disengagement. Routledge.

[6] Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. Studies in Conflict & Terrorism, 40(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

[7] Freedman, J. L., & Fraser, S. C. (1966). Compliance without pressure: The foot-in-the-door technique. Journal of Personality and Social Psychology, 4(2), 195–202. https://doi.org/10.1037/h0023552

[8] Gill, P., Horgan, J., & Deckert, P. (2017). Bombing alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists. Journal of Forensic Sciences, 59(2), 425–435. https://doi.org/10.1111/1556-4029.12312

[9] Horgan, J. (2008). From profiles to pathways and roots to routes: Perspectives from psychology on radicalisation into terrorism. The ANNALS of the American Academy of Political and Social Science, 618(1), 80–94. https://doi.org/10.1177/0002716208317539

[10] Kruglanski, A. W., Bélanger, J. J., Gelfand, M., Gunaratna, R., Hettiarachchi, M., Reinares, F., Orehek, E., Sasota, J., & Sharvit, K. (2013). Terrorism—A (self) love story: Redirecting the significance quest can end violence. American Psychologist, 68(7), 559–575. https://doi.org/10.1037/a0032615

[11] Kruglanski, A. W., Gelfand, M. J., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., & Gunaratna, R. (2014). The psychology of radicalisation and deradicalisation: How significance quest impacts violent extremism. Political Psychology, 35(Suppl. 1), 69–93. https://doi.org/10.1111/pops.12163

[12] Kruglanski, A. W., Molinario, E., Jasko, K., Webber, D., Leander, N. P., & Pierro, A. (2022). Significance-quest theory. Perspectives on Psychological Science, 17(4), 1050–1071. https://doi.org/10.1177/17456916211034825

[13] Kruglanski, A. W., Webber, D., & Koehler, D. (2019). The radical's journey: How German neo-Nazis voyaged to the edge and back. Oxford University Press.

[14] McCauley, C., & Moskalenko, S. (2008). Mechanisms of political radicalisation: Pathways toward terrorism. Terrorism and Political Violence, 20(3), 415–433. https://doi.org/10.1080/09546550802073367

[15] McCauley, C., & Moskalenko, S. (2017). Friction: How radicalisation happens to them and us (2nd ed.). Oxford University Press.

[16] Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. American Psychologist, 60(2), 161–169. https://doi.org/10.1037/0003-066X.60.2.161

[17] Moonshot CVE. (2020). Online radicalisation: From hate speech to terrorism. Moonshot CVE. https://moonshotcve.com/online-radicalisation

[18] Neumann, P. R. (2013). The trouble with radicalisation. International Affairs, 89(4), 873–893. https://doi.org/10.1111/1468-2346.12049

[19] Ribeiro, M. H., Ottoni, R., West, R., Almeida, V. A. F., & Meira, W. (2020). Auditing radicalisation pathways on YouTube. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (pp. 131–141). ACM. https://doi.org/10.1145/3351095.3372879

[20] Sageman, M. (2004). Understanding terror networks. University of Pennsylvania Press.

[21] Sageman, M. (2014). The stagnation in terrorism research. Terrorism and Political Violence, 26(4), 565–580. https://doi.org/10.1080/09546553.2014.895649

[22] Saltman, E. M., & Russell, J. (2014). The role of prevent in countering online extremism. Quilliam Foundation.

[23] Sunstein, C. R. (2017). #Republic: Divided democracy in the age of social media. Princeton University Press.

[24] Wiktorowicz, Q. (2004). Joining the cause: Al-Muhajiroun and radical Islam. In The roots of Islamic radicalism conference. Yale University.