MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Gen-Z and Reconfiguration of the Violent Extremist Landscape

Saman Ayesha Kidwai

December 30, 2025

Summary

Gaming platforms, AI-enabled propaganda, socio-psychological factors, social media, and emotionally resonant narratives have overwhelmingly shaped the contours of radicalisation in the contemporary era. Governments confront multifaceted challenges in dealing with new manifestations of violent extremism that involve a lower demographic threshold, are technologically savvy, and consistently tap into social and identity-based vulnerabilities.

Introduction

The violent extremist landscape that has emerged today is due to the decentralisation and democratisation of the digital domain, and its access to Gen-Z (born between 1997 and 2012) teenagers. While many Gen-Z extremists have displayed tendencies of ideological fluidity, some, after prolonged radicalisation, have also displayed Islamist, neo-Nazi, or hybrid ideological worldviews. This demographic has dramatically altered the violent extremism landscape by tapping into expansive digital platforms, including social media, gaming ecosystems and encrypted chat forums.

As highlighted by Deputy Superintendent Andy Meeks, Head of Investigations for Counter-Terrorism Policing North West in the UK,

> There has been a significant increase in online investigations of individuals who have been committing acts of terrorism online. A lot, I think, coincided with the pandemic … It's certainly an increased focus of our work in counter-terrorism policing.'[1]

Digital Grooming and the Search for Identity & Belonging

In several cases, Gen-Z teenagers have been mobilised by extremist recruiters, who exploit insecurities, identity crises, and a desire for belonging or rebellion within a borderless digital space. Extremist recruiters, or lone actors who present themselves as self-proclaimed digital leaders, offer impressionable teenagers a sense of community, belonging, and purpose that they otherwise lack. This process, in some cases, may also lay down the foundation of ideological indoctrination linked to values propagated by Islamist jihadism, white nationalism, or neo-Nazism as the culmination of this radicalisation pathway.

In other cases, the digital domain may also lead to the transnationalisation of extremist beliefs. For example, teenagers as young as 16 have been arrested in connection with an attempted attack on two mosques in Singapore in January 2021. This Singaporean youth was inspired by an online manifesto and live streaming of the massacre carried out in Christchurch, New Zealand, in March 2019.[2] Furthermore, after watching ISIS videos online, he was radicalised and developed hostility towards Muslims.

---

[1] Josh Halliday, **"More Young People Being Radicalised Online, Says UK Counter-terror Officer"**, *The Guardian*, 18 March 2024.

[2] **"Detention of Singaporean Youth Who Intended to Attack Muslims on the Anniversary of Christchurch Attacks in New Zealand"**, Ministry of Home Affairs, Singapore, 27 January 2021.

Limits of the State's Conventional Counter-Terror Approaches

To counter the broader threat of radicalisation, states tend to overwhelmingly rely on factual narrative building, raids, detention, or post-extremism de-radicalisation programmes. These fail to account for how identity-based and emotionally anchored narratives, disseminated through fast-paced technological advancements, continue to shape the worldview of the younger generation. Instead, what is required is the creation of visually appealing, authentic and emotionally resonant counter-narratives, including by leveraging the power of generative Artificial Intelligence (AI).

Additionally, states have yet to develop concrete frameworks and initiatives to counter the threat posed by the convergence of extremism and 3D technology. Recently, some arrested individuals have been placed under detention due to the potential danger they pose to their respective communities, including their role in attempting to create 3D weapons. For instance, in July 2025, an 18-year-old school student, inspired by a Nazi worldview, was arrested.[3] In Edinburgh, Scotland, he plotted a mass shooting at his school using a 3D-printed gun. These weapons are low-cost and require no checks or background verification, thus increasing their appeal and potency.

Overlooked Drivers: Mental Health Challenges and Social Isolation

The process of radicalisation can become exacerbated if an individual is experiencing mental health concerns. This could accelerate the timeline of their radicalisation if the signs remain ignored or unnoticed for an extended period. EUROPOL's Terrorism Situation and Trends Report (2025) lists 'mental health problems, social isolation, and digital dependency' as some of the main drivers of teenage radicalisation.[4] These factors have played a fundamental role in cultivating communities among like-minded youth, both in physical and digital domains.

Meanwhile, it is seen that these social and psychological factors impacting radicalisation frequently do not find mention or focus within counter-terrorism frameworks or national security strategies, formulated by states worldwide. They are often viewed in isolation, as community-based issues and under the purview of families, guardians, or school-level educational programmes. Policymakers, law enforcement officials and domestic intelligence agencies must take these socio-psychological problems into account when planning counter-radicalisation programmes.

---

[3] Reuben Dass, **"Gen-Zs and Ghost Guns: Trends, Threats, and Implications"**, Insights, Global Network on Extremism & Technology, 24 September 2025.

[4] **"European Union Terrorism Situation and Trend Report (EU TE-SAT)"**, Report, European Union Agency for Law Enforcement Cooperation (Europol), 2025.

The Incubators of Digital Extremist Communities

The initial drivers of recruitment, as mentioned above, provide a pathway for extremist groups or individual leaders to reinforce their ideology amid sustained state pressures to root out extremist beliefs that challenge the state's monopoly of violence and its paramountcy as the legitimate governing authority. This has been achieved by forging digital communities on platforms such as Discord, Tam Tam, TikTok, YouTube, Reddit, WhatsApp, Roblox, Fortnite, Instagram, Telegram and 4Chan, among others. These platforms have transcended geographical boundaries to bind teenagers—particularly those active on video gaming and encrypted chat platforms—into a wider community. As rightly pointed out by Bruce Hoffman and Jacob Ware, extremists have successfully exploited 'cutting-edge' technologies for nefarious purposes.[5]

This has been enabled by a state's unwillingness or inability to address these social challenges at the grassroots level. Notably, the drivers of recruitment among Gen-Z youth, at least during the initial phase, have less to do with any specific ideology. It is only later that radicalisation may assume a defined ideological identity. This has been one of the major gaping loopholes in states' counter-violent extremism (CVE) strategies, regardless of their socio-economic status or military and intelligence superiority, and a fact extensively exploited by extremist recruiters.

Often, the gamification, memification, or glorification of violence in the online sphere also plays a central role in facilitating the normalisation and desensitisation of violent acts among youth in physical communities. It also contributes to the reinforcement of xenophobia and support for violent extremism, based on the theme of a specific game and its characters, among a demographic particularly susceptible to indoctrination through gamified avenues. Roblox is an example of one such gaming platform. It has been found that *Remove Kebab*, one of the games available on this platform for users based in the United States and the UK, has played a key role in normalising Islamophobia and radicalising young gamers, as young as 13 years old.[6]

This matter becomes more complex because Gen-Z teens have been particularly vulnerable to falling into the rabbit hole of watching trending or recommended reels, for example, on Instagram. Such content may be fused with extremist opinions, ideology, memes, and graphic videos or images in a never-ending loop. Over time, the normalisation of violence through passive support or active participation becomes the norm in societies.

---

[5] Bruce Hoffman and Jacob Ware, **"Are We Entering a New Era of Far-Right Terrorism?"**, *War on the Rocks*, 27 November 2019.

[6] George Hancorn, **"Mosque Shootings and Far-right Skins: Teens Playing Roblox Exposed to Extremist Content"**, *itvX*, 17 November 2025.

Evolving Extremist Demographics

Analysts have raised concerns about the lack of sound judgement and impulse control among young adolescents. This is profoundly affected by the changing demographic of violent extremism, with arrest profiles of violent extremists averaging at the age of 15 years. It has been broadly estimated that between 18 and 20 per cent of arrested individuals in Europe and Australia reflect the growing trend of youth radicalisation on a transnational scale. This shifting demographic landscape has also been recognised by international organisations like the United Nations, which, in October 2025, launched a report detailing how extremist recruitment, while targeting teenagers, has expanded its focus to an even lower age demographic. One of the key revelations of the report indicates that children as young as 8 to 9 years old in Europe and North America are also being groomed by extremist recruiters.[7] As a result, between 2021 and 2025, a 42 per cent surge was observed in investigations into terror-related offences in these regions.

Moreover, according to the Pew Research Center, in the US in 2025, one in five teenagers is constantly active on platforms such as TikTok and YouTube, while three out of ten teenagers are active members of AI platforms such as Character.ai and ChatGPT daily. It is evident from such surveys that First World democratic countries have been more affected by this crisis than authoritarian states. Arguably, one reason is that digital ecosystems in liberal democracies are more open and decentralised, with access available even in remote areas and a broad, often ambiguous scope for freedom of speech and expression, unlike those in authoritarian one-party systems.

Ideological Fluidity, AI, and Misinformation

Interestingly, the challenge of detecting such threats, particularly among teenagers today, has increased.[8] This is because online spaces and forums have opened a new dimension of violent extremism by forging ties with overlapping extremist strands that encourage violence against individuals and the state establishment.[9] This mutation within the global violent extremist fold has made the task of intelligence

[7] **"Growing Alarm as Terrorist Exploitation of Children Rapidly Evolves, Outpacing Member States Responses"**, Report, United Nations Counter-Terrorism Committee Executive Directorate (CTED), October 2025.

[8] Milo Comerford, Moustafa Ayad and Jakob Guhl, **"Gen-Z & The Digital Salafi Ecosystem"**, Report, Institute for Strategic Dialogue, 16 November 2021.

[9] Daveed Gartenstein-Ross, **"The Digital Battlefield: How Terrorists Use the Internet and Online Networks for Recruitment and Radicalization"**, Foundation for Defense of Democracies, 4 March 2025.

and law enforcement agencies far more complex in detecting and neutralising potential radicalised security threats.

The challenge related to threat detection primarily arises from the overlapping of extremist ideologies or trends, which gives rise to a new hybrid threat with no clearly defined attributes, scope, ideology, enemies, or intent. Consequently, the prospect of neutralising such unprecedented threats becomes even more difficult. Simply put, the era of hybridisation of threats has turned the extremist landscape on its head, challenging conventional narratives around radicalisation and extremism.

Meanwhile, the rising popularity of the decentralised web—a network of interconnected computer systems in which independent users control data usage and storage rather than major corporate entities—enables direct data sharing, sovereignty over digital footprints and profiles, and evasion of censorship or speech moderation.[10] This has significantly restricted state control over information disseminated on the internet and over its removal. This has enabled the unrestricted dissemination of extremist propaganda in an unprecedented manner.

While white supremacist or Islamist narratives may lead to eventual recruitment or radicalisation of youngsters, policymakers and law enforcement agencies must incorporate how segments of Gen-Z could be influenced by conspiratorial narratives, misinformation, disinformation, and influence operations in the CVE plans. These dynamics can create echo chambers that enable simultaneous bottom-up and top-down reinforcement of extremist narratives, eventually leading to their mainstreaming. This situation may become exceptionally volatile in regions experiencing widespread political polarisation, as seen in the United States and Europe.

In this context, it is essential to recall a key finding from a report released by the Institute for Strategic Dialogue in 2023, which is relevant even today:

> A hybridised blend of extremisms is giving rise to an era of ideological fluidity. While internal dynamics within extremist groups have shaped these trends, the internet and technology have hyper-charged them and emboldened a tech-savvy, ideologically fluid Generation Z.[11]

[10] Maria Zuppello, **"From TechHaven to Telegram: How Latin American Youth Are Being Drawn into Jihadist Networks"**, Insights, Global Network on Extremism & Technology, 14 November 2025.

[11] Isabel Jones, Jakob Guhl, Jacob Davey and Moustafa Ayad, **"Young Guns: Understanding a New Generation of Extremist Radicalization in the United States"**, Report, Institute for Strategic Dialogue, 2023.

Video Games as the Pathway to Radicalisation

Alex Newhouse, an expert on online radicalisation and extremism, has spotlighted the correlation between youth involvement in video games and subsequent radicalisation that underscores that time spent playing video games has a greater impact on whether a person becomes radicalised and begins expressing an authoritarian or extremist worldview, rather than on the content of the video games themselves.[12]

This is because potential recruits engaged in multiplayer video games may find themselves in an interactive ecosystem, often through chat-enabled features, with an extremist recruiter. Through repeated interactions, they could establish a social, emotional and trustworthy relationship. Once such a connection is established, it could result in the recruiter grooming new joiners to commit, or be involved in the preparatory stages of, a violent extremist act. Over time, it is plausible that these recruits could gradually assume the mantle at the grassroots level, that is, of micro-cells or chapters, and later, in the event of the arrest of a high-profile leader, assume charge instead. Furthermore, as a domino effect, such individuals could radicalise their peers, younger family members, and other community members. This could facilitate the emergence of a new wave of extremism and lead to a rise in a new frontier of radicalisation and its physical manifestations.

Neo-Nazis and Exploitation of AI-Enabled Propaganda

One of the biggest dangers of the democratisation of access to technology, especially amid the normalisation of white supremacist beliefs and neo-Nazism across North America and the European continent, has been the dissemination of AI-generated videos and speeches using services provided by ElevenLabs, cloned from Adolf Hitler's available voice recordings.[13] Neo-Nazi extremist groups adhering to National Socialist ideology have sought to repackage Hitler's persona, actions, and worldview as benign or misunderstood to appeal to a broader and unsuspecting demographic. They have relied on significant platforms such as Instagram, X, YouTube and TikTok to spread their message to Gen-Z, while deftly avoiding Nazi icons or vivid imagery to prevent detection or enforcement under these platforms' safety guidelines.

In an effort to target the younger generation, Hitler's audio has been combined with visual propaganda and appealing background music in short 30-second segments,

[12] **"Video Games and Youth Radicalization"**, Webinar, Institute of Digital Media and Child Development, March 2023.

[13] Daria Alexe, **"Neo-Nazi Exploitation Online: AI Voice-Cloning and the Revival of Hitler Speeches"**, Insights, Global Network on Extremism & Technology, 21 November 2025.

reflecting the limited attention spans of contemporary viewers. Due to advanced services available through commercial, easily accessible platforms such as ElevenLabs, German audio is swiftly translated into English, and the finished product is subsequently disseminated on the aforementioned digital platforms. In November 2025, a 17-year-old in Canberra, Australia, was arrested on grounds of possession of extremist far-right propaganda, bomb-making equipment, and an imitation gun, drawing inspiration from the Ku Klux Klan, Nazi symbols and the Christchurch massacre.[14]

Conclusion

Global state actors must overhaul their national security frameworks and shift the focus from combating conventional terrorism to a more fluid—organisationally, geographically and ideologically—violent extremist threats by adopting more pre-emptive approaches. For this purpose, states must enact legislative reforms establishing streamlined guidelines under which a nodal agency would assume responsibility for dismantling real-time threats, such as the proliferation of extremist propaganda across video content, social media and encrypted chat platforms operating within their respective jurisdictions.

While the absolute neutralisation of digital-centric threats and the de-radicalisation of affected or vulnerable Gen-Z remains improbable, it is still conceivable for states to work towards a defined timeline with digital corporations to modify required algorithms and reduce the availability of extremist—covert or overt—content for unrestricted online consumption. At the same time, rather than responding with a repressive attitude, governments should tap into generative AI to create emotionally and visually resonant, digital literacy-centric content, including via YouTube Shorts, Telegram, TikTok and Instagram Reels and accessible video games, to moderate the material accessed by Gen-Z within their respective geographical domains.

Finally, governments need to broaden their approach to countering violent extremism. They must systematically and simultaneously focus on defeating the ideologies associated with extremist beliefs while pursuing an interventionist role in addressing socio-psychological drivers of radicalisation. This includes mental health initiatives undertaken in coordination with community leaders, educators, digitally influential Gen-Z celebrities and influencers, alternative media platforms, local representatives, and family-centric units to succeed.

[14] Elizabeth Byrne, **"Canberra Teenager Behind Bars Over Detailed Plans for Public Attacks, Possessing Violent Extremist Material"**, *ABC*, 6 November 2025.

About the Author

Ms. Saman Ayesha Kidwai is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses