CTED Trends Report

Beyond messaging: terrorist propaganda as operational infrastructure

Photo Credit: © iStockphoto.com/Diana Latypova



United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

September 2026

Table of contents

I. Overview 1
II. Introduction 2
III. Emerging trends in terrorist propaganda 6
- Use of artificial intelligence in propaganda 6
- Exploitation of gaming platforms and alternate online spaces 8
- Gore and nihilistic content as pathways to radicalization to terrorism 10
- Ideological convergence and fluidity 12
- Increased targeting of children and youth 14

IV. Cross-cutting propaganda patterns across regions 16
- Governance activity as propaganda 16
- Ethnic and grievance-based targeting 18
- Resilient propaganda infrastructure 18
- Competition as a propaganda accelerant 20
- Integration of propaganda into operational planning and intent 21

V. Challenges Member States face 22

I. Overview

This Trends Report was prepared by the Counter-Terrorism Committee Executive Directorate (CTED) in accordance with Security Council resolutions 2617 (2021) and 2810 (2025). In those resolutions, the Council reaffirms the essential role of CTED within the United Nations to identify and assess issues, trends and developments relating to the implementation of resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017) and other relevant resolutions.

CTED Trends Reports are designed to provide policy-relevant insights into emerging or evolving terrorism trends, within the mandate of the Security Council Counter-Terrorism Committee and of United Nations agencies and policymakers, identified through CTED's engagement with United Nations Member States on their implementation of the relevant Council resolutions. The Reports also include research conducted by members of the CTED Global Research Network (GRN) and other researchers.

For the purposes of this Report, "terrorist propaganda" refers to the production and dissemination of terrorist narratives, messaging, and related content intended to recruit, radicalize to terrorism, incite or facilitate terrorist acts, legitimize terrorist groups and their activities, and mobilize support, including financial support. As reflected in relevant Security Council resolutions, including resolutions 1624 (2005), 2178 (2014), 2354 (2017) and 2396 (2017), such content may be used to facilitate recruitment and radicalization to terrorism and encourage individuals to support, facilitate, or participate in terrorism. The term "terrorist propaganda" is used consistent with its application in the comprehensive international framework to counter terrorist narratives,[1] the applicable statement by the President of the Security Council,[2] and the reports of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida and the Taliban and associated individuals and entities. It encompasses the full spectrum of terrorist communicative output, including the underlying narratives and messaging through which terrorist groups seek to advance their objectives, recognizing that propaganda is the primary vehicle through which such narratives are produced and disseminated at scale.

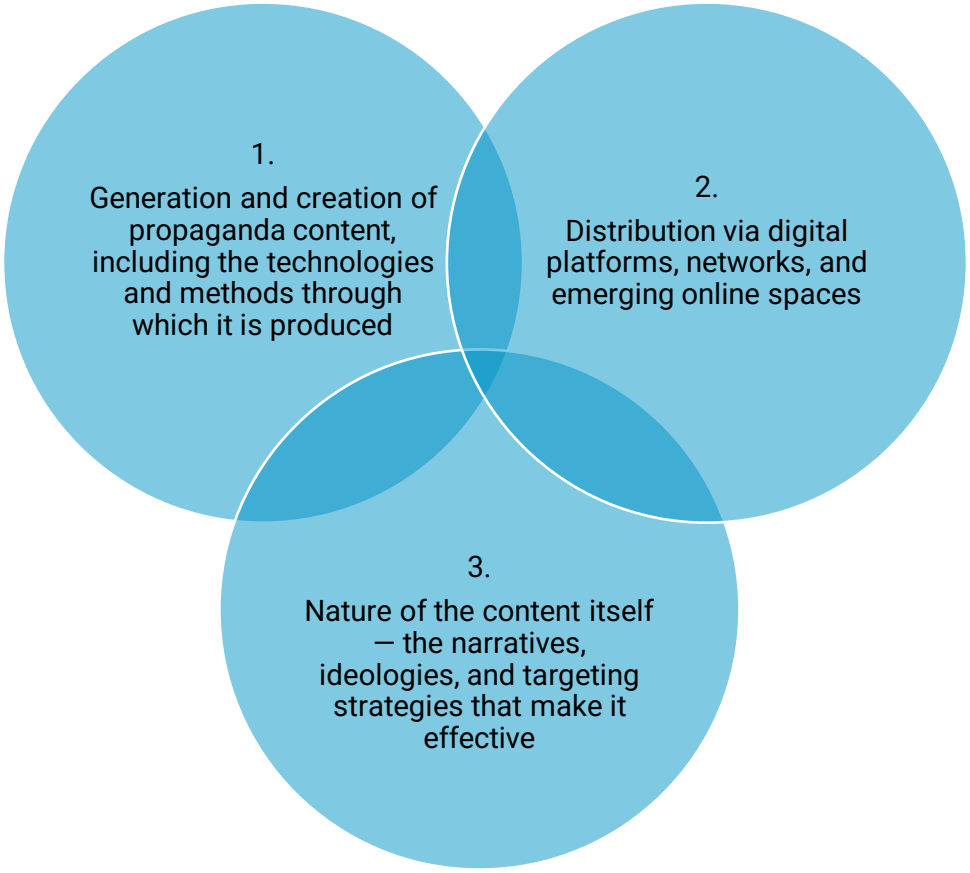
[1] United Nations (S/2017/375, annex).
[2] Ibid. (S/PRST/2016/6).

II. Introduction

Terrorist groups use propaganda as a core operational tool to recruit, radicalize to violence, raise funds, and provide guidance to followers. This Report examines terrorist propaganda across three interrelated dimensions. Each section addresses one or more of these dimensions regarding emerging trends, regional patterns, and Member State responses.

Figure 1

Three interrelated dimensions of terrorist propaganda



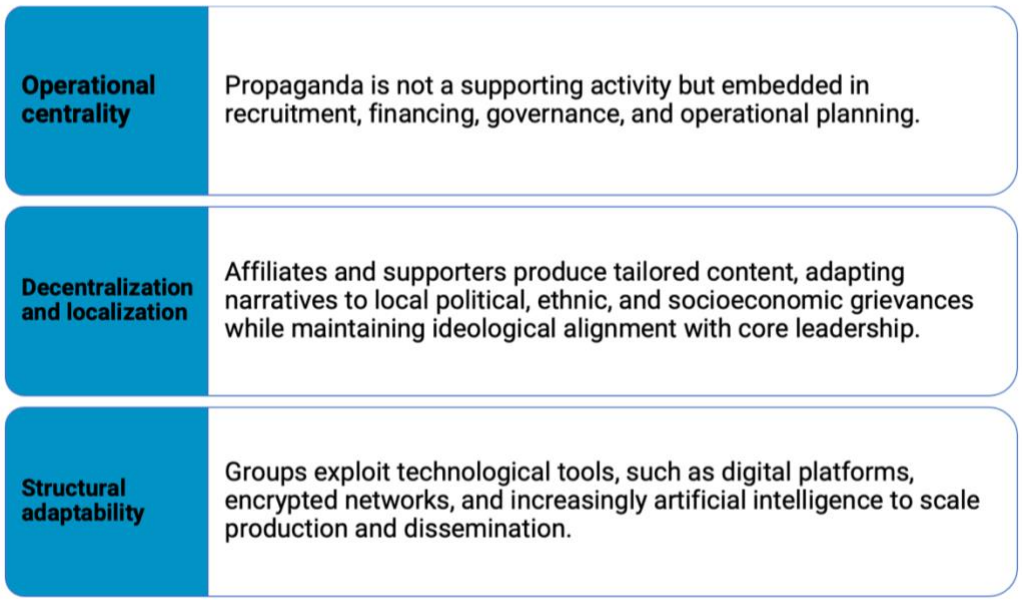
While terrorists have long made propaganda integral to their strategies, the deployment and scale of propaganda have evolved significantly, and its function is now more central, integrated, and adaptive than in earlier phases. Historically, terrorist groups such as Al-Qaida relied on centralized messaging distributed through physical media and limited online platforms. This shifted with the emergence of ISIL (Da'esh) in the mid-2010s, which used high-volume,

multilingual, digitally distributed propaganda ecosystems.[3,4,5] Subsequent countermeasures by Member States and technology companies did not diminish Da'esh's reliance on propaganda but instead drove adaptation, fragmentation, and diversification across platforms.[6] Rather than retreating from the online space, terrorist actors increasingly adopted multiplatform dissemination strategies, exploiting a diverse ecosystem of mainstream platforms, smaller online services, file-sharing and archiving platforms, and, in some cases, terrorist-operated websites to maintain reach and resilience despite platform content moderation and takedown efforts.[7,8,9]

Today, terrorist propaganda is characterized by three defining features, which shape not only how propaganda is produced, but how it operates in practice with regard to recruitment, influence, and strategic communication.

Figure 2

Defining features of contemporary terrorist propaganda



[3] Asaad Almohammad and Charlie Winter (Combating Terrorism Centre at West Point), "From battlefront to cyberspace: demystifying the Islamic State's propaganda machine", June 2019.
[4] Ahmad Saiful Rijal Hassan and Nur Aziemah Azman, "Islamic State's visual propaganda: amplifying narratives and affecting radicalization", *Counter Terrorist Trends and Analyses*, vol. 12 No. 5 (September 2020).
[5] Lucas Webber and Daniele Garofalo (Global Network on Extremism and Technology (GNET)), "Fursan al-Tarjuma carries the torch of Islamic State's media jihad", 5 June 2023.
[6] Scott N. Romaniuk, Amparo Pamela H. Fabe and Debasish Nandy (GNET), "Terrorist platform migration: the move to smaller, less regulated online spaces", 23 June 2023.
[7] Arthur Bradley and Deeba Shadnia (Tech Against Terrorism and George Washington University Programme on Extremism), "Examining online migration to terrorist and violent extremist-owned domains", July 2022.
[8] Tech Against Terrorism, "Patterns of online terrorist exploitation: TCAP insights", 28 April 2023.
[9] Ibid., "Beyond content moderation: the urgent need to stop terrorist-operated websites", 2 January 2025.

These features shape how propaganda engages individuals, embedding ideological narratives within everyday experiences and perceptions of grievance. The COVID-19 pandemic intensified these dynamics by weakening protective factors and creating a larger, more captive audience for terrorist messaging.[10,11] Together, these developments further entrenched an ongoing shift towards technology-driven propaganda ecosystems.

Terrorist propaganda derives its effectiveness less from sophistication than from persistence, proximity, and volume. Its influence stems not only from repeated exposure but also from the sheer volume of content amplified through decentralized supporter networks, creating an environment in which certain narratives are reinforced and attain disproportionate visibility. It consistently appears in spaces where individuals feel marginalized or unheard and speaks directly to perceived injustices where credible alternative voices are absent.[12] By repeatedly validating personal and collective grievances in accessible language and familiar formats, terrorist actors normalize ideologically driven interpretations of lived experiences, foster a sense of belonging, and position violence as a meaningful or inevitable response. These narratives are frequently tailored to gendered identities, experiences and expectations, drawing on perceptions of masculinity and femininity, discriminatory gender norms, and grievances relating to status, belonging and social roles in order to increase their resonance with specific audiences.[13,14] At the structural level, terrorist groups deliberately exploit local grievances and communication vacuums – particularly where State presence is weak – shaping how grievances are interpreted and positioning themselves as credible alternatives to the State.[15] They also exploit underlying socioeconomic and political conditions and perform quasi-governance functions that reinforce the groups' influence and sustain support.[16,17] In such contexts, the most effective propaganda is not the most sophisticated but the most pervasive – filling spaces where no competing narrative exists.

United Nations reporting has consistently highlighted the adaptiveness of terrorists' propaganda in recruitment and fundraising efforts, as well as for communicating strategic priorities and reinforcing group cohesion, which are amplified through growing networks of

---

[10] United Nations, CTED, "The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism: update", December 2020.
[11] Ibid., "The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism: update December 2021", December 2021.
[12] European Commission and EU Knowledge Hub on Prevention of Radicalization, *Strategic Communication and Artificial Intelligence, Digital Media and Radicalization. The Hub. Insights* (Brussels 2026).
[13] Aleksandra Dier and Gretchen Baldwin (CTED and International Peace Institute), "Masculinities and violent extremism", 9 June 2022.
[14] United Nations Development Programme (UNDP) and United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women), *Conflicting Identities: The Nexus Between Masculinities, Femininities and Violent Extremism in Asia* (New York, 2020).
[15] United Nations, CTED, "Civil society perspectives: terrorism and counter-terrorism in West Africa", April 2026.
[16] United Nations, Report of the Secretary-General on the Plan of Action to Prevent Violent Extremism (A/70/674).
[17] Ibid., CTED, "Trends Alert – Counter-terrorism and border management in Africa: fundamental and cross-cutting challenges", April 2024.

supporters across platforms. Recent evidence points to a deeper structural shift in how propaganda intersects with other core functions of terrorist activity, increasingly converging with terrorist financing and emerging technologies.[18,19] Propaganda is used to recruit donors, raise funds and disseminate financing instructions, and connect otherwise dispersed actors, functioning as the trust infrastructure through which terrorist financing can scale.[20]

For example, in its thirty-seventh report on ISIL (Da'esh), Al-Qaida and associated individuals and entities, the Analytical Support and Sanctions Monitoring Team notes that Islamic State in Iraq and the Levant-Khorasan Province (ISIL-K) has incorporated cryptocurrency donation mechanisms directly into its Voice of Khorasan publication, embedding Monero and bitcoin wallet addresses and QR codes within propaganda content to facilitate fundraising.[21] In the Analytical Support and Sanctions Monitoring Team's 33rd report, it has identified in some contexts, particularly in parts of Africa, a tactical evolution – the deliberate uncoupling of propaganda from public attribution of attacks – with groups claiming fewer attacks than they perpetrate, likely an effort to maintain local support and legitimacy.[22]

The use of artificial intelligence (AI) represents the current frontier of this convergence between terrorist propaganda and technological innovation. In recent reporting, the United Nations has noted a discernible increase in the effective use of new technologies, with terrorist groups demonstrating growing sophistication in integrating AI tools and visual effects into radicalization to terrorism and recruitment efforts.[23,24] This is further reflected in AI-enhanced translation, which enables rapid outreach in multiple languages, and the amplification of terrorist messages by supporters across platforms.[25]

These developments underscore the defining characteristic of contemporary terrorist propaganda: structural adaptability. Terrorist groups have consistently outpaced countermeasures by continuously layering new technologies onto enduring ideological

---

[18] Ibid., Analytical Support and Sanctions Monitoring Team, Thirty-sixth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2025/482).
[19] United Nations, Twenty-first report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat (S/2025/496).
[20] Ibid., CTED, "CTED hosts Insight Briefing on how propaganda ecosystems enable terrorist financing", April 2026.
[21] Ibid., Analytical Support and Sanctions Monitoring Team, Thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44).
[22] Ibid., Thirty-third report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2024/92).
[23] Ibid., Thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44).
[24] United Nations, Twenty-third report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat (S/2026/638).
[25] Ibid., Analytical Support and Sanctions Monitoring Team, Thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44).

narratives. Successive technological shifts have expanded reach, accelerated pathways to radicalization to terrorism, and integrated propaganda more deeply into recruitment, financing, and operations.[26] As a result, propaganda is no longer merely communicative – it is increasingly central to how terrorist groups organize, sustain, and project their activities, particularly in environments shaped by governance gaps and unmet grievances. This has direct implications for Member State responses, which must increasingly address propaganda not only as content but as a core operational enabler of terrorism.

III. Emerging trends in terrorist propaganda

- Use of artificial intelligence in propaganda

Successive United Nations reports and CTED's GRN partners have documented an escalating pattern of AI use: terrorists are experimenting with AI, particularly generative AI, to enhance propaganda efforts, primarily for radicalization to terrorism and recruitment, including issuing guidance to supporters on evading detection while using generative AI tools.[27,28,29] AI has the potential to reduce the capabilities gap between terrorist organizations and State-led security mechanisms, with terror groups increasingly using AI to enhance the sophistication and intensity of attacks and incite violence.[30,31] It can be used to generate and distribute propaganda content faster and more efficiently than ever before – from interactive recruitment and influencing behaviour via social media channels, to spreading disinformation and ideologies conducive to terrorism. AI-powered bots can amplify violent extremist content at scale, making it harder to detect and respond to, while enabling targeted interaction with potential recruits through personalized messaging that appeals to their interests, beliefs, and grievances.[32] AI applications can unintentionally accelerate the radicalization of vulnerable individuals as users increasingly rely on them for companionship, guidance, and advice. Personalized AI interactions can reinforce existing beliefs and vulnerabilities, which may be exploited to increase

[26] The Soufan Centre, "TikTok jihad: terrorists leverage modern tools to recruit and radicalize", 9 August 2024.
[27] United Nations, Twenty-second report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat (S/2026/57).
[28] Ibid., Twenty-first report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat (S/2025/496).
[29] United Nations Interregional Crime and Justice Research Institute (UNICRI), United Nations Office of Counter-Terrorism (UNOCT) and United Nations Counter-Terrorism Centre, *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes* (New York 2021).
[30] Rahul Rawat and Neha Kaushal (Observer Research Foundation), "AI in terrorism: emerging threats for State security", January 2026.
[31] Alessandro Bolpagni and Eleonora Ristuccia (GNET), "AI-powered translation: how AI tools could shape a new frontier of IS propaganda dissemination", 9 July 2025.
[32] Gabriel Weimann and others (Combating Terrorism Centre at West Point), "Generating terror: the risks of generative AI exploitation", *CTC Sentinel* (January 2024).

susceptibility to terrorist influence and recruitment.[33] Recent research also suggests that AI may function as a radicalization environment rather than merely a tool, potentially reinforcing grievances, identities and existing beliefs through sustained personalized interactions that remain largely invisible to traditional counter-terrorism monitoring approaches.[34]

AI may further amplify the role of gender in terrorist propaganda. Experts have noted that generative AI enables the rapid production and localization of gendered propaganda tailored to men and women, girls and boys, allowing terrorist and violent extremist actors to adapt narratives to specific audiences at greater scale and to disseminate them at an accelerated pace.[35]

At the operational level, specific documented uses have emerged across groups and regions. Da'esh supporters launched an AI-generated programme called News Harvest to disseminate propaganda videos.[36] In its thirty-seventh report, the Analytical Support and Sanctions Monitoring Team documents terrorist actors demonstrating greater sophistication in integrating AI tools and visual effects into propaganda content, with AI-enhanced translation enabling rapid outreach across multiple languages simultaneously.[37] Reports suggest Da'esh has sought to recruit cyberexperts to bolster capacities and tailor propaganda to local contexts.[38] At the platform level, Tech Against Terrorism identified 10,000 URLs hosting verified terrorist content in a single 30-day period, underscoring a growing gap between the scale of content production and the capability of platforms to detect and remove it.[39] Recent Tech Against Terrorism research highlights the limitations of existing AI safeguards. Of 27 leading AI models, in approximately one-third of test cases, AI models provided information beyond what is readily available through a standard web search, including assistance relevant to attack planning or explosive-device construction. It further found that relatively simple prompt modifications could circumvent safety mechanisms, suggesting that existing guardrails remain inconsistent and vulnerable to misuse.[40]

Groups motivated by xenophobia, racism and other forms of intolerance, or in the name of religion or belief (XRIRB), have similarly operationalized AI for propaganda production.

---

[33] Priyank Mathur, Clara Broekaert and Colin P. Clarke (International Centre for Counter-Terrorism), "The radicalization (and counter-radicalization) potential of artificial intelligence", 1 May 2024.
[34] Michael Varga (GNET), "The counterterrorism blind spot: AI as a radicalisation environment", 9 July 2026.
[35] Organization for Security and Cooperation in Europe, "Artificial intelligence in the context of preventing and countering violent extremism and terrorism: challenges, risks and opportunities", summary document of expert-level event, September 2024.
[36] The Soufan Centre, "TikTok jihad: terrorists leverage modern tools to recruit and radicalize", 9 August 2024.
[37] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44).
[38] Ibid., Thirty-sixth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2025/482).
[39] Tech Against Terrorism, "Beyond 10,000 URLs: a TCAP milestone that demands immediate action", 5 December 2026.
[40] Ibid., "Counter-terrorism AI (CT-AI) benchmark", July 2026.

Accelerationist networks on Telegram have dedicated channels to creating and disseminating AI-generated memes and other visual propaganda, while also exploiting large language models to support attack planning or interpret accelerationist manifestos – with AI generating disinformation campaigns, feeding radicalizing content to unsuspecting users, and providing instructions for creating explosive devices.[41] A review of online boards and publications commonly used by XRIRB groups – including Gab, 4chan, and The Daily Stormer – revealed how these communities actively discuss, debate, and devise strategies around AI technologies, using generative AI for ideological outreach, propaganda dissemination, and recruitment.[42]

AI-enabled propaganda is also increasingly intersecting with terrorist financing. As noted above, ISIL-K has integrated cryptocurrency fundraising directly into its propaganda – while AI-enhanced translation amplifies such content across multiple languages and audiences.[43] More broadly, large language models have the potential to lower barriers to fundraising by enabling the rapid generation of tailored, multilingual narratives and coordinated outreach campaigns, allowing terrorist actors to expand donor engagement and enhance perceived legitimacy at relatively low cost.[44]

- Exploitation of gaming platforms and alternate online spaces

Gaming platforms and related online spaces platforms – most notably Discord, Twitch, and Steam – have emerged as a significant and underregulated channel for the dissemination of terrorist and violent extremist propaganda, providing infrastructure for recruitment and community building. Terrorist recruitment has targeted young people through gaming, with many groups designing violent extremist-themed first-person shooter games and modifying existing games to embed violent extremist narratives within familiar entertainment formats.[45] In some cases, terrorist groups across the ideological spectrum have developed simple custom games incorporating ideological narratives designed to support propaganda and fundraising efforts, reinforcing messaging through interactive and visual engagement.[46,47]

Several United Nations and GRN reports highlight the growing use of gamified propaganda – content designed to encourage user engagement through game-like features such as rewards,

[41] Federico Borgonovo, Silvano Rizieri Lucini and Giulia Porrino (GNET), "Weapons of mass hate dissemination: the use of artificial intelligence by right-wing extremists", 23 February 2024.
[42] Liram Koblentz-Stenzler and Uri Klempner (GNET), "Navigating far-right extremism in the era of artificial intelligence", 25 January 2024.
[43] Daria Alexe (GNET), "'Agentic Smurfing': how AI-Autonomous micro-laundering is outpacing traditional terrorist financing detection", 28 January 2026.
[44] Jason Blazakis (Royal United Services Institute for Defence and Security Studies), "Terrorist financing in the age of large language models", 2026.
[45] United Nations, CTED, "Trends Alert: Growing alarm as terrorist exploitation of children rapidly evolves, outpacing Member State responses", October 2025.
[46] Ibid.
[47] Gonzalo Saiz (Royal United Services Institute for Defence and Security Studies), "Virtual threats: terrorist financing via online gaming", 2025.

competition, progression, and interactive participation.[48,49] Terrorist and violent extremist actors increasingly operate through private and semi-private online groups and servers, making the prevalence of such content difficult to monitor. XRIRB actors have exploited these platforms to disseminate propaganda, build closed communities, and facilitate recruitment, often through immersive and participatory formats embedded within gaming culture, leveraging features such as real-time chat, donations, and audience participation.[50]

These trusted online communities may also facilitate fundraising by directing supporters to virtual asset wallets and other payment mechanisms, including microtransactions and in-game purchases that can obscure the source and movement of funds. Multiplayer environments, voice-chat functions, and linked messaging groups further support relationship-building, creating ecosystems that can simultaneously facilitate propaganda dissemination, recruitment, and fundraising.

Weaknesses and limitations in existing moderation frameworks make these platforms particularly conducive to propaganda dissemination and recruitment and terrorist-financing activity. A significant proportion of gaming-related violent extremist content may be characterized as "awful but lawful" – extreme in nature but falling below the threshold that triggers removal under existing platform policies or national legislation.[51] The normalization of hateful rhetoric, even when it falls short of explicit terrorist messaging, may contribute to environments more conducive to the dissemination of violent extremist narratives and recruitment efforts, although the relationship between exposure and radicalization to terrorism remains complex and contested. Girls and young women face particular risks in these spaces, where gender-based harassment and sexualized abuse and threats are well documented.[52] Such dynamics can undermine their participation in online communities and may increase their vulnerability to manipulation and exploitation by malicious actors, including violent extremists.[53] Technical solutions alone are insufficient to address this challenge. Sustainable responses require integrated approaches that combine online safety measures, digital literacy, psychosocial support, and gender-responsive prevention efforts. Multi-stakeholder cooperation among governments, educators, civil society, technology companies and youth-focused organizations remains essential to mitigating these risks.

[48] UNICRI and UNOCT, *Level Up – Gaming and Violent Extremism in Africa* (New York, 2025).
[49] Linda Schlegal (GNET), "Competing, connecting, having fun: how gamification could make extremist content more appealing", 12 July 2021.
[50] Liram Stenzler-Koblentz, Eitan Azani and Carlotta Rinaudo (International Institute for Counter-Terrorism), "From gaming to grooming: how far-right extremists exploit video game-adjacent platforms for radicalization and recruitment", 22 December 2025.
[51] William Allchorn and Elisa Orofino, "Policing extremism on gaming-adjacent platforms: awful but lawful?", *Frontiers in Psychology*, vol. 16 (30 July 2025).
[52] Galen Lamphere-Englund (United Nations Children's Fund (UNICEF) Innocenti), "Protecting children in online gaming: mitigating risks from organized violence", working paper, October 2025.
[53] Galen Lamphere-Englund and others, "Building resilience against violent extremism digitally: trialing a new gender-based approach among gamers", *Frontiers in Psychology*, vol. 16 (July 2025).

The challenges facing Member States as they respond to the spread of propaganda through the nexus of gaming and violent extremism conducive to terrorism are distinct from those of conventional social media platforms. This presents States with a regulatory gap that existing counter-terrorism frameworks were not designed to address.

As digital access expands rapidly across Africa – now home to approximately 350 million gamers – the continent represents a significant and largely unaddressed frontier for terrorist propaganda through gaming spaces. In their Level Up report, UNICRI and UNOCT warn that terrorist groups are likely to attempt to leverage gaming platforms for propaganda, recruitment, and radicalization as Africa's rapidly expanding and increasingly connected gaming ecosystem grows, creating new opportunities for exploitation. They also identify the potential for terrorist and affiliated criminal networks to exploit in-game microtransactions and mobile gaming economies to move and conceal funds, including through a scenario examining possible future use by actors operating in Somalia. Boko Haram has used offline games to train child soldiers, while Al-Shabaab's capacity for rapid technological adoption signals that migration to gaming platforms for propaganda is a near-term risk. These challenges are compounded by gaps in regulation and enforcement: law enforcement agencies often lack investigative tools for monitoring voice, video, and in-game communications, while moderation in many African languages remains limited or absent.[54]

- ## Gore and nihilistic content as pathways to radicalization to terrorism

Graphic violent ("gore") content and nihilistic online subcultures are increasingly important spheres for the dissemination of terrorist propaganda. Unmoderated or lightly regulated "gore" platforms host large volumes of extreme violent imagery – including terrorist-produced execution footage, mass-casualty attacks and other forms of spectacle violence – which are often recirculated and repurposed in ways that attract attention, normalize extreme violence, and reinforce terrorist narratives.[55] The deliberate production of gore content by terrorist organizations – including execution footage and mass-casualty imagery released through official media channels – reflects an understanding that shock and spectacle function as effective propaganda tools, driving engagement and increasing the visibility of terrorist messaging.[56,57]

[54] UNICRI and UNOCT, *Level Up – Gaming and Violent Extremism in Africa* (New York, 2025).
[55] Ali Fisher and Arthur Bradley (Human Digital), *Gore and Violent Extremism: An Explorative Analysis of the Use of Gore Websites for Hosting and Sharing Extremist and Terrorist Content*, (VOX-Pol, n.p., 2025).
[56] Yuanbo Qi, "Propaganda in focus: decoding the media strategy of ISIS", *Humanities and Social Sciences Communications*, vol. 11 (2 September 2024).
[57] Miron Lakomy, "*Danse macabre*: gore images in the Islamic State's 'Dabiq' Magazine as a propaganda device", *The International Journal of Intelligence, Security, and Public Affairs*, vol. 21, No. 2 (2019).

Such content is not designed to be consumed in isolation but is embedded within hybrid online ecosystems where violent imagery is combined with ideological messaging, memes, and subcultural cues, allowing propaganda to be reframed through shock value or subcultural identity, rather than relying solely on overt messaging.[58] This creates an environment in which propaganda operates less through persuasion alone and more through affective mechanisms – desensitization and psychological conditioning – potentially lowering psychological barriers to violence and contributing to conditions conducive to radicalization to terrorism among some users.[59]

Reactions to graphic violent content are not uniform. Studies indicate gender differences in responses to violent content, with some evidence suggesting that repeated exposure may contribute to desensitization among some users, although the extent of this effect remains uncertain.[60,61] Recent research suggests overlap between gore-related online communities and violent extremist ecosystems, with users able to move between violent imagery, hate content, and terrorist propaganda on interconnected online spaces.[62,63] Although the causal relationship between gore consumption and radicalization to terrorism remains contested, gore-focused online communities may increase exposure to violent extremist material and reinforce engagement with violent narratives through peer networks, platform architecture, and normalization of violence.

Recent research suggests that "gore websites host thousands of videos created by terrorist organizations or lone attackers … including both graphic and non-graphic violent propaganda."[64] At the same time, the authors highlight "a lack of research on the role of gore within terrorist group propaganda and online violent extremist communities", including the factors that shape content volume and viewing figures."[65]

---

[58] Anti-Defamation League, "From gore to hate: how 'WatchPeopleDie' serves as a gateway to extremism", 21 August 2025.
[59] Rachel Jones and Beth Daviess (Centre for Naval Analyses), "Explainer: gore content and violent extremism", 2026.
[60] Sylvie Mrug and others, "Emotional and physiological desensitization to real-life and movie violence", *Journal of Youth and Adolescence*, vol. 44, No. 5 (19 October 2014).
[61] Laura Louise Nicklin, Emma Swain and Joanne Lloyd, "Reactions to unsolicited violent, and sexual, explicit media content shared over social media: gender differences and links with prior exposure", *International Journal of Environmental Research and Public Health*, vol. 17, No. 12 (16 June 2020).
[62] Anti-Defamation League, "From gore to hate: how 'WatchPeopleDie' serves as a gateway to extremism", 21 August 2025.
[63] Ali Fisher and Arthur Bradley (Human Digital), *Gore and Violent Extremism: An Explorative Analysis of the Use of Gore Websites for Hosting and Sharing Extremist and Terrorist Content*, (VOX-Pol, n.p., 2025).
[64] Ibid., p. 5.
[65] Ibid., p. 9.

- Ideological convergence and fluidity

There is a growing convergence and fluidity of ideologies within online violent extremist ecosystems, where propaganda functions as the primary connective mechanism across otherwise disparate movements. Terrorist and violent extremist content is increasingly designed to transcend ideological boundaries, blending narratives, symbols, and grievances from several contexts to maximize resonance and reach a range of audiences.

In these environments, violence itself is increasingly foregrounded as a unifying theme. As documented earlier, the emergence of "nihilistic violence" reflects a subculture in which the glorification of harm becomes central, with graphic content operating simultaneously as a recruitment tool and a mechanism of socialization.[66] Research conducted by GRN partners indicates that for some younger recruits, violence functions less as the product of ideological commitment than as its starting point – with attraction to the spectacle, aesthetics, and identity of mass violence preceding, or substituting for, coherent ideological belief.[67,68] CTED analysis suggests that a significant proportion of deadly attacks have stemmed from nihilistic subcultures, outpacing defined ideologies in a shifting threat landscape.[69]

These dynamics are reinforced by processes of cross-group learning, whereby violent extremist movements emulate one another's propaganda techniques, narratives, and modes of mobilization across ideological divides.[70] Similar patterns are evident across online XRIRB ecosystems, where violent misogyny, accelerationist narratives, and mass-casualty imagery intersect, with propaganda reinforcing perceived grievances and the normalization of violence across loosely networked communities.[71] Two recent cases illustrate how far this cross-pollination has progressed. In South-East Asia, perpetrators of nihilistic attacks have drawn on neo-Nazi imagery, pro-Da'esh content, antisemitic conspiracy theories, and mass-shooter glorification simultaneously – appropriating whichever propaganda resonates most effectively rather than adhering to any coherent ideological tradition.[72] The May 2026 attack on the Islamic Centre of San Diego in the United States reinforces this pattern: two teenage perpetrators drew

[66] Jared Holt and Katherine Keneally (Institute for Strategic Dialogue), "Online radicalization and the nexus to violence in the US: 2024 year in review", 18 July 2025.
[67] Steven Rai (Institute for Strategic Dialogue), "San Diego mosque shooting highlights new generation of neo-Nazi accelerationism", 18 June 2026.
[68] Julie Charnov Hwang (The Soufan Centre), "Nihilistic violent extremism in Southeast Asia", 3 December 2025.
[69] United Nations, CTED, "Trends Alert: Growing alarm as terrorist exploitation of children rapidly evolves, outpacing Member State responses", October 2025.
[70] Friederike Wegener (GNET), "Striking similarities between Islamist terrorism and violent right-wing extremism", 18 September 2020.
[71] Ali Fisher and Arthur Bradley (Human Digital), *Gore and Violent Extremism: An Explorative Analysis of the Use of Gore Websites for Hosting and Sharing Extremist and Terrorist Content*, (VOX-Pol, n.p., 2025).
[72] Julie Charnov Hwang (The Soufan Centre), "Nihilistic violent extremism in Southeast Asia", 3 December 2025.

simultaneously on neo-Nazi accelerationism, violent misogyny, and mass-shooter glorification – assembled from overlapping online subcultures rather than any single movement or doctrine.[73]

Gender stereotypes, discriminatory social norms, and misogyny play a particular role within these converging online ecosystems, functioning not merely as an associated form of harmful content but increasingly intersecting with pathways to violent extremism.[74,75] Online communities centred on grievances related to gender roles and identity, including incel and manosphere networks, increasingly intersect with conspiratorial and other violent extremist online ecosystems, enabling the circulation and amplification of narratives that reinforce hostility, exclusion and, in some cases, support for violence.[76,77,78] The Secretary-General of the United Nations has noted that such communities are united by opposition to gender equality and are amplified by digital environments that reward provocative and polarizing content.[79,80] The growing normalization of online misogyny and opposition to gender equality is increasingly recognized as a factor that can facilitate exposure to broader violent extremist ecosystems, particularly among young people exposed to overlapping networks centred on grievance, identity and social exclusion.[81,82] These dynamics illustrate how contemporary radicalization pathways increasingly transcend traditional ideological categories, exposing individuals to interconnected forms of violent extremist and harmful content. Importantly, these harms are not confined to online environments and may contribute to broader patterns of gender-based violence and abuse offline.[83]

Antisemitism has emerged as another potent cross-ideological connective narrative within these converging ecosystems. XRIRB actors exploit discussions of current events to disguise their ideology within mainstream discourse, disseminating antisemitic propaganda through short-form video platforms, artificially manufactured engagement, and demographic-targeted memes – with the aim of normalizing XRIRB ideology and facilitating pathways to radicalization

---

[73] Steven Rai (Institute for Strategic Dialogue), "San Diego mosque shooting highlights new generation of neo-Nazi accelerationism", 18 June 2026.
[74] Aleksandra Dier and Gretchen Baldwin (CTED and International Peace Institute), "Masculinities and violent extremism", 9 June 2022.
[75] United Nations, Report of the Secretary-General on intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls (A/79/500).
[76] UNDP and UN-Women, *Conflicting Identities: The Nexus Between Masculinities, Femininities and Violent Extremism in Asia* (New York, 2020).
[77] Georgia Lala (GNET), "Into the Manosphere: Louis Theroux's documentary and how platforms enable the business of misogyny", 2 June 2026.
[78] Fabio Daniele and others (GNET), "Monetising misogyny: engagement farming and the tactics behind incendiary online content", 17 December 2025.
[79] United Nations, Report of the Secretary-General on intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls (A/79/500).
[80] Ibid., Conor Lennon (UN News), "Online 'manosphere' is moving misogyny to the mainstream", 7 March 2025.
[81] UNDP and UN-Women, *Conflicting Identities: The Nexus Between Masculinities, Femininities and Violent Extremism in Asia* (New York, 2020).
[82] United Nations, Report of the Secretary-General on intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls (A/79/500).
[83] Ibid.

among broader audiences.[84] Da'esh and its affiliates have similarly incorporated antisemitic narratives into their propaganda, embedding them within broader grievance-based and geopolitical messaging.[85,86] Antisemitic online rhetoric has inspired offline violent extremism across otherwise divergent ideologies, as terrorist actors exploit geopolitical crises to disseminate overlapping grievance narratives, recruit non-aligned audiences, and set in motion radicalization trends that can contribute to wider distrust in democratic institutions.[87,88] AI is now enhancing these mechanisms – making propaganda faster to produce, harder to detect, and more adaptable across narrative contexts – including through information laundering, whereby falsehoods circulate through fringe platforms until they acquire the appearance of verified information.[89]

As a result, propaganda is no longer tied to a single coherent doctrine but circulates through shared digital cultures – embedded in humour, language, and social interaction – lowering barriers to engagement and facilitating cross-ideological mobilization.[90] This convergence across hybrid ecosystems means that individuals may move from casually encountering terrorist and violent extremist content to actively engaging with it, even where ideological beliefs remain fragmented, fluid, or poorly defined.[91,92]

- Increased targeting of children and youth

Children and young people are increasingly among those exposed to and targeted by terrorist and violent extremist propaganda and recruitment efforts. While the drivers of this trend are varied and context-specific, the convergence of digital environments, algorithmic amplification, tailored outreach strategies, and the social and developmental vulnerabilities of younger users have created conditions in which violent extremist content reaches children and young people at scale.[93] This is reflected in the widespread exposure of children to such content globally, as

[84] Uri Klempner and Liram Koblentz-Stenzler (GNET), "Methodologies in manipulation: the far-right's antisemitic discourse online amid the Israel-Hamas war", 11 July 2024.
[85] Daniel Rickenbacher, "The centrality of anti-semitism in the Islamic State's ideology and its connection to anti-Shiism", *Religions*, vol. 10, No. 8 (16 August 2019).
[86] Michaela Rana and Josh Lindsay (GNET), "Antisemitism and terrorist manifestos: 'Where did you get your current beliefs? Mostly from the internet", 15 August 2025.
[87] Ibid.
[88] William Allchorn, Elisa Orofino and Lakshmi Babu Saheer (GNET), "Critical world events: extremist disinformation networks and narratives in times of crisis", 3 June 2025.
[89] D. Santus and C. Bettin, "Antisemitism in the algorithmic age: propaganda, disinformation, and generative AI", *Journal for Religion, Society and Politics* (2025).
[90] Cecilia Polizzi (GNET), "The feed that shapes us: extremism and adolescence in the age of algorithms", 12 December 2025.
[91] Ibid.
[92] United Nations, CTED, "Trends Alert: Growing alarm as terrorist exploitation of children rapidly evolves, outpacing Member State responses", October 2025.
[93] Ibid., Analytical Support and Sanctions Monitoring Team, Thirty-eighth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/651).

well as in developments throughout the European Union, where the number of children and young people involved in terrorist and violent extremist activities continued to grow in 2024.[94]

Terrorist actors leverage social media, gaming platforms, and online communities frequented by children and young people to disseminate propaganda and progressively guide them from mainstream platforms into more closed and immersive environments, where exposure to increasingly violent propaganda content, including graphic imagery, may facilitate socialization into violent extremist ecosystems.[95] These strategies are designed to appeal directly to the emotional and psychological needs of youth – such as identity formation, belonging, and grievance – making propaganda more relatable, interactive and increasingly embedded within youth culture itself.[96] In a recent Trends Alert, CTED highlights how groups motivated by XRIRB – particularly those which are active in gaming spaces – have pioneered a "youth-on-youth" recruitment model where teenage conscripts actively recruit their peers, making detection more difficult for authorities and parents.[97] This is reinforced by a common pattern in which terrorist and violent extremist groups increasingly deploy culturally fluent recruiters, who communicate in the language, aesthetics, and platforms of their target audiences, making violent extremist messaging harder to distinguish from mainstream youth content.[98,99]

The gendered dimensions of terrorist propaganda and recruitment targeting children and youth are distinct and require specific attention. Girls and young women are often targeted through narratives that exploit vulnerabilities related to belonging, protection, identity, and relationships, while boys and young men may be exposed to hypermasculine messaging that frames violence as a source of status, purpose, and power.[100] United Nations reporting has documented the use of gendered messaging by terrorist groups, including Da'esh, to recruit and exploit children in a range of roles, highlighting the need for prevention and intervention efforts that take into account the distinct ways in which girls and boys are targeted online.[101,102,103]

---

[94] European Union Agency for Law Enforcement Cooperation, *TE-SAT: European Union Terrorism Situation and Trend Report 2025* (The Hague, 2025), p. 10.
[95] Galen Lamphere-Englund (UNICEF Innocenti), "Protecting children in online gaming: mitigating risks from organized violence", working paper, October 2025.
[96] Cecilia Polizzi (GNET), "The feed that shapes us: extremism and adolescence in the age of algorithms", 12 December 2025.
[97] United Nations, CTED, "Trends Alert: Growing alarm as terrorist exploitation of children rapidly evolves, outpacing Member State responses", October 2025.
[98] Nicolas Stockhammer and Colin P. Clarke (Combating Terrorism Centre at West Point), "The August 2024 Taylor Swift Vienna concert plot", *CTC Sentinel*, vol. 18, No. 1 (January 2025).
[99] Federico Borgonovo, Silvano Rizieri Lucini and Giulia Porrino (GNET), "Weapons of mass hate dissemination: the use of artificial intelligence by right-wing extremists", 23 February 2024.
[100] Aleksandra Dier and Gretchen Baldwin (CTED and International Peace Institute), "Masculinities and violent extremism", 9 June 2022.
[101] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44).
[102] United Nations, Report of the Secretary-General on children and armed conflict (A/78/842-S/2024/384).
[103] Aleksandra Dier and Gretchen Baldwin (CTED and International Peace Institute), "Masculinities and violent extremism", 9 June 2022.

Terrorist and violent extremist networks increasingly exploit the convergence of online and offline spaces, using propaganda and recruitment strategies that target youth across both domains, with digital environments reinforcing and extending their reach.[104] These trends indicate that children and youth are no longer peripheral targets but central audiences in terrorist propaganda strategies, requiring integrated prevention responses that address both digital and social dimensions of radicalization to terrorism.

IV. Cross-cutting propaganda patterns across regions

Analysis of the propaganda apparatus of terrorist and violent extremist groups in Africa and Central and South Asia reveals several recurring patterns. These patterns appear in varying combinations among Jama'a Nusrat ul-Islam wa-Muslimin (JNIM) in the Sahel, Al-Shabaab in Somalia, ISIL-K in Central and South Asia, and Tehrik-e Taliban Pakistan (TTP). Collectively, they illustrate what propaganda looks like and what it does operationally in each context. This is also consistently documented in United Nations reporting, including reports of the Analytical Support and Sanctions Monitoring Team and of the Secretary-General and Security Council briefings, as referenced throughout this report.

- Governance activity as propaganda

The most visible and consistently documented pattern is the use of governance activity as a means of projecting legitimacy. While the provision of services by terrorist groups and their affiliates is not a new phenomenon, terrorist organizations increasingly document, package, and disseminate information about these activities as part of deliberate propaganda campaigns designed to reinforce authority and cultivate support. Where State authority is absent, contested or perceived as predatory, terrorist groups often invest in visible service provision, including courts, clinics, taxation systems, and security guarantees.[105]

Governance-focused propaganda may also draw on narratives concerning family life, social conduct and gender roles, leveraging existing gender norms and power structures to reinforce claims of legitimacy, authority and moral order.[106] In such contexts, propaganda is not ancillary but integral, promoting and disseminating governance functions as evidence of authority.

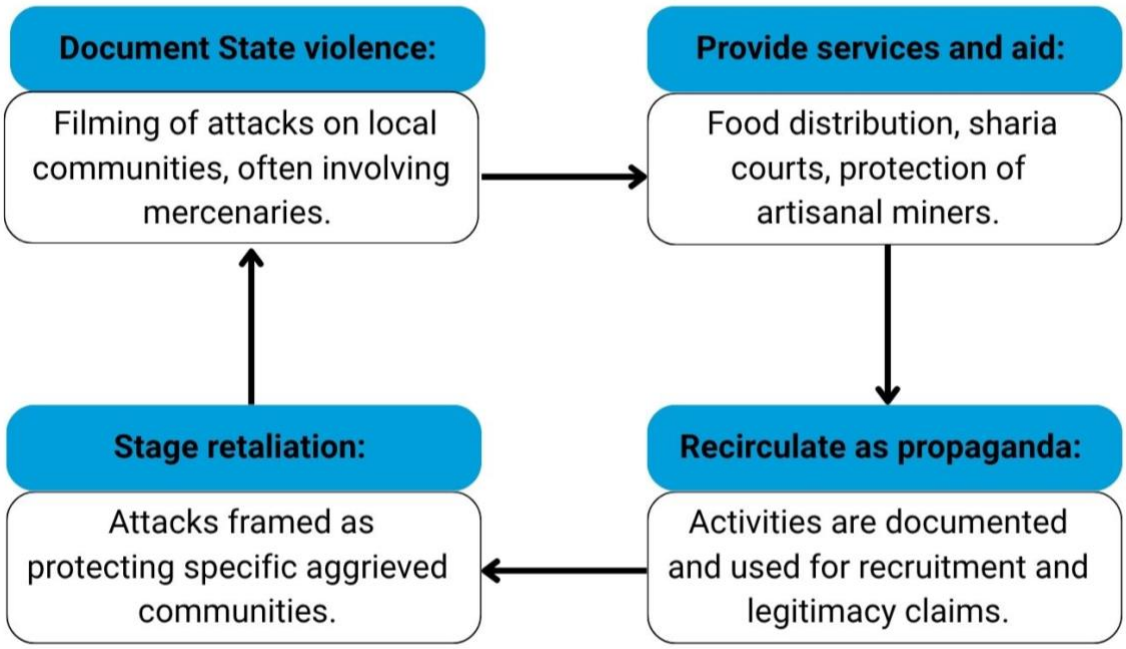
JNIM in the Sahel illustrates this dynamic: the group documents State violence or absence, provides services in response, and circulates information about both as part of its propaganda strategy to position itself as a credible authority.

---

[104] Global Internet Forum to Counter Terrorism, "Online subcultures, child exploitation, and the shifting landscape of terrorism", September 2025.
[105] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-second (S/2023/549), Thirty-third (S/2024/92) and Thirty-fourth reports submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2024/556).
[106] UNDP and UN-Women, *Conflicting Identities: The Nexus Between Masculinities, Femininities and Violent Extremism in Asia* (New York, 2020).

Figure 3

JNIM's propaganda–governance cycle in the Sahel[107]



Variations of this model are observed in various contexts. Al-Shabaab maintains structured governance systems, which are reflected in its media output as indicators of State-like capacity.[108,109] ISIL-K, by contrast, emphasizes the failures of de facto Taliban governance, particularly regarding the protection of minority communities, and uses these narratives in its propaganda to position itself as an alternative authority.[110,111] TTP propaganda similarly frames

[107] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-second (S/2023/549) and Thirty-fourth reports submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2024/556); Institute for Security Studies, "Illicit activities fuel extremism in the Sahel's conflict zones", July 2025; Africa Defence Forum, "By taking on government roles, terrorists tighten grip on Sahel's rural areas", 29 July 2025; and The Soufan Centre, "JNIM expanding geographic reach and staging coordinated attacks in the Sahel", 5 June 2025.
[108] Georgia Gilroy (Combating Terrorism Centre at West Point), "The online frontline: decoding Al-Shabaab's social media strategy", *CTC Sentinel* (January 2024).
[109] Frederick Appiah Afriyie (Cogent Social Sciences), "What fuels terrorism in Somalia? Perspectives from the jihadist group Al-Shabaab", 2025.
[110] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-first report submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2023/95).
[111] Ibid., Thirty-fourth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2024/556).

the group as a centre of power, but, unlike the others, it does not demonstrate comparable, systematic governance activity.[112,113]

- Ethnic and grievance-based targeting

A second consistent pattern is the targeting of propaganda and recruitment to specific ethnic groups or communities experiencing State violence, neglect, or marginalization. In these cases, propaganda explicitly frames the terrorist or violent extremist group as the protector of these communities.

JNIM's systematic radicalization efforts among Fulani communities in the Sahel, exploiting grievances linked to State violence and inter-communal tensions, is well documented.[114,115] Through Fulani and Tuareg representation, leadership composition itself can function as propaganda, projecting pan-Sahelian inclusion. ISIL-K adopts a segmented approach, producing multilingual propaganda tailored to Tajik-, Uzbek-, and Russian-speaking audiences, including diaspora communities in Central Asia and beyond.[116] TTP propaganda has shifted from purely religious framing to explicitly invoking Pashtun ethnic identity and localized grievances, while expanding its messaging beyond Khyber Pakhtunkhwa to diaspora communities and wider audiences, reflecting the group's ambition.[117,118] Al-Shabaab's propaganda is less explicitly ethnic, reflecting the different structure of Somali clan politics, while exploiting localized community grievances in its messaging.[119]

- Resilient propaganda infrastructure

The third pattern concerns the sophistication and resilience of propaganda dissemination infrastructure. While scale and sophistication vary, all cases demonstrate adaptive systems designed to survive countermeasures and reach dispersed audiences rapidly.[120] Terrorist groups increasingly rely on multilayered dissemination models in which their official media

---

[112] Pearl Pandya (Armed Conflict Location & Event Data (ACLED)), "The battle for the borderlands: the Tehreek-i-Taliban Pakistan challenges the state's control", 6 October 2025.
[113] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-fifth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2025/71/Rev.1).
[114] Ibid., Thirty-first report submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2023/95).
[115] The Soufan Centre, "JNIM expanding geographic reach and staging coordinated attacks in the Sahel", 5 June 2025.
[116] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-first report submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2023/95).
[117] Amira Jadoon, Saif Tahir, and Joey Moran (The Diplomat), "From jihad to jirga: how the TTP is rebranding itself as defender of the Pashtun nation", 20 August 2025.
[118] Sameer Patil and Soumya Awathi (Observer Research Foundation), "Pakistan Taliban's evolving social media propaganda", 28 January 2025.
[119] Georgia Gilroy (Combating Terrorism Centre at West Point), "The online frontline: decoding Al-Shabaab's social media strategy", *CTC Sentinel* (January 2024).
[120] For detailed findings on the scale of terrorist content online and platform resilience challenges, see Tech Against Terrorism sources cited in this Report, as well as the thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44, annex).

output is amplified through affiliates, supporters, local intermediaries, and decentralized online networks. This redundancy reduces dependence on any single platform, communications channel, or media outlet, allowing propaganda ecosystems to continue functioning despite content removals, platform moderation efforts, leadership losses, or operational setbacks.

Figure 4

Digital dissemination models across Al-Qaida and ISIL networks, including core media structures and key affiliate propaganda hubs[121]

Group	Propaganda infrastructure
Al-Qaida core	***Centralized ideological direction through As-Sahab*** • Through As-Sahab, Al-Qaida sets strategic messaging and disseminates leadership communications across affiliates • Provides ideological guidance and broad narrative direction across the Al-Qaida network
Al-Qaida in the Arabian Peninsula (AQAP)	***Secondary media and dissemination hub through Al-Malahem*** • Al-Malahem contains recruitment, radicalization and outreach content, including *Inspire* magazine • AQAP operates with significant propaganda autonomy, while receiving media support from other affiliates
JNIM: Sahel	***Decentralized, community-embedded dissemination*** • Local religious figures and intermediaries carry messaging • Effective in rural areas with weak State presence and low connectivity
Al-Shabab: Somalia	***Centralized, high-speed dissemination*** • Multiple Telegram channels share content within minutes of release • Thousands of subscribers reached instantaneously despite government restrictions on platforms

[121] Georgia Gilroy (Combating Terrorism Centre at West Point), "The online frontline: decoding Al-Shabaab's social media strategy", *CTC Sentinel* (January 2024); United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-fourth (S/2024/556), thirty-fifth (S/2025/71/Rev.1) and thirty-seventh reports submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44); The Soufan Centre, "Islamic State Khorasan Province and terrorist networks throughout Central Asia", 29 March 2024; Amira Jadoon, Saif Tahir, and Joey Moran (The Diplomat), "From jihad to jirga: how the TTP is rebranding itself as defender of the Pashtun nation", 20 August 2025; and Sameer Patil and Soumya Awathi (Observer Research Foundation), "Pakistan Taliban's evolving social media propaganda", 28 January 2025.

ISIL/Da'esh core	***Centralized narrative coordination through Al-Naba and Al-Amaq*** • Al-Naba signals propaganda priorities and operational focus across affiliates. • Al-Amaq publicizes attacks and amplifies affiliate operations globally.
Islamic State West Africa Province (ISWAP)	***Regional propaganda and coordination hub within ISIL's African network*** • ISWAP's influence within the wider ISIL (Da'esh)'s Africa network has increased as pressure on other branches has intensified • ISIL (Da'esh)'s Al-Naba publication regularly covers ISWAP operations as part of its Africa-focused propaganda output, reinforcing the group's prominence
ISIL-K: Central and South Asia	***Multilingual, diaspora-targeted ecosystem*** • Parallel outlets in Tajik, Uzbek, Russian, Pashto, and Arabic • Geographically dispersed facilitators sustain reach across borders
Associated Group	
TTP: Pakistan/Afghanistan	***Operationally focused digital messaging*** • Propaganda increasingly invokes ethnic identity, anti-State narratives and localized grievances • Online outreach supports recruitment, mobilization and cooperation among aligned actors

- Competition as a propaganda accelerant

Inter-group competition can function as a multiplier of propaganda output rather than a constraint. In situations where multiple groups compete for the same recruitment base or territorial legitimacy, attacks and outreach activity may become mechanisms through which groups seek to differentiate themselves, mobilize support, and assert dominance.[122]

In the Sahel, rivalry between JNIM and Islamic State in the Greater Sahara – also known as Islamic State Sahel Province – has led to competing claims of attacks and assertions of dominance, driving sustained escalation in operations, recruitment, and geographical

[122] Sara M.T. Polo and Blair Welsh, "Violent competition and terrorist restraint", *International Organization* vol. 78, issue 3 (29 August 2024).

expansion.[123,124,125] In Afghanistan and Central Asia, competition between ISIL-K, the Taliban, and associated groups contribute to a complex information environment in which groups seek to undermine one another's legitimacy. ISIL-K, for example, combines attacks targeting Taliban officials and aligned communities with propaganda efforts in multiple languages and regions aimed at expanding recruitment by portraying the Taliban as illegitimate.[126] This dynamic is less evident in the TTP case, where cooperation rather than competition characterizes relationships with aligned actors. For example, in its reports, the Analytical Support and Sanctions Monitoring Team has highlighted the Afghan Taliban's sustained logistical, financial, and operational support to TTP, including access to some recruitment and training infrastructure.[127,128]

- Integration of propaganda into operational planning and intent

Terrorist groups increasingly design certain operational activities around their anticipated propaganda value. Rather than merely documenting outcomes after the fact, many groups now integrate propaganda considerations into operational planning, incorporating symbolic target selection, staged weapons display, and near-immediate footage releases.[129,130]

In its reports, the United Nations has shown that propaganda does not only follow operations but can precede and signal them. An analysis of keyword frequency in Da'esh's flagship weekly publication, Al-Naba, reveals a clear shift in propaganda emphasis on parts of Africa, with increased references to Mozambique and to the targeting of Christian communities – a shift that does not necessarily reflect the reality of operations on the ground, but the propaganda priorities that Da'esh seeks to promote.[131] In recent reports, the Analytical Support and Sanctions Monitoring Team further noted a marked increase in references to the Syrian Arab Republic, Iraq and the Islamic Republic of Iran, alongside renewed emphasis on Africa and increasingly explicit sectarian messaging and highlighted how propaganda can reveal evolving

[123] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-second report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2023/549).
[124] Héni Nsaibia (ACLED), "New frontlines: jihadist expansion is reshaping the Benin, Niger, and Nigeria borderlands", 27 March 2025.
[125] Counter Extremism Project and Konrad-Adenauer-Stiftung, "Sahel monitoring – February 2024", February 2024.
[126] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-fourth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2024/556).
[127] Ibid., Thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44).
[128] Ibid., Thirty-fifth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2025/71/Rev.1).
[129] Héni Nsaibia (ACLED), "New frontlines: jihadist expansion is reshaping the Benin, Niger, and Nigeria borderlands", 27 March 2025; and Counter Extremism Project, "Sahel monitoring – July 2025", July 2025.
[130] Asaad Almohammad and Charlie Winter (Combating Terrorism Centre at West Point), "From battlefront to cyberspace: demystifying the Islamic State's propaganda machine", June 2019.
[131] United Nations, Analytical Support and Sanctions Monitoring Team, Thirty-seventh report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44).

strategic priorities beyond current operational trends.[132] Propaganda thus functions both as an instrument of influence and as an indicator of future operational priorities.

V. Challenges Member States face

The speed at which terrorist groups adapt their propaganda strategies has created an "acceleration gap" between their strategies and the legislation and policies of Member States.

The rapid evolution of terrorist recruitment and propaganda strategies has created an "acceleration gap", reflecting a widening divergence between the pace of non-State innovation and Member State response capabilities.[133] Terrorist actors adjust tactics quickly, while policy responses and their implementation have longer legislative and operational timelines. The effect is particularly evident in digital environments, where groups engage in ongoing platform migration from one online space to another as authorities struggle to develop countermeasures.[134]

CTED's findings from the assessment visits conducted on behalf of the Security Council Counter-Terrorism Committee have highlighted the challenges Member States face in responding to rapidly evolving online ecosystems. Member States frequently report difficulties identifying, monitoring, and countering terrorist content produced outside their jurisdictions, often in foreign languages and disseminated through unfamiliar or rapidly changing platforms. These dynamics can leave vulnerable communities exposed to large volumes of propaganda while limiting the ability of States to detect, disrupt, or offer credible alternatives to such messaging. At the same time, some major platforms are increasingly relying on AI-enabled moderation systems to identify and review harmful content at scale. While such systems may improve speed and coverage, concerns remain regarding contextual understanding, linguistic and cultural accuracy, transparency, and accountability in decisions affecting borderline content.[135,136] The acceleration gap extends beyond State responses. Delays between the identification of terrorist content and its removal by online platforms can allow propaganda to continue circulating, migrating, and reaching new audiences even after it has been detected.

The growing use of AI by terrorist groups, as covered elsewhere in this Report, exacerbates this gap. Recent field research suggests that terrorist adoption of AI may be advancing more rapidly than previously understood. Both Boko Haram factions have reportedly used AI tools for

---

[132] Ibid., Thirty-eighth report submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/651).
[133] United Nations, CTED, "Trends Alert: Growing alarm as terrorist exploitation of children rapidly evolves, outpacing Member State responses", October 2025.
[134] Arthur Bradley and Deeba Shadnia (Tech Against Terrorism and George Washington University Programme on Extremism), "Examining online migration to terrorist and violent extremist-owned domains", July 2022.
[135] Soorya Balendra, "Meta's AI moderation and free speech: ongoing challenges in the Global South", *Cambridge Forum on AI: Law and Governance*, vol. 1 (16 May 2025).
[136] Oversight Board, "Content moderation in a new era for AI and automation",17 September 2024.

operational planning, weapons troubleshooting, and other operational tasks, with some former members describing structured training and dedicated AI functions within the organization.[137] This suggests that terrorist experimentation with emerging technologies, in some contexts, may be progressing faster and in a more systematic manner than many existing counter-terrorism frameworks were designed to address.

The increasing ideological fragmentation and fluidity of terrorist and violent extremist propaganda require Member States to develop more adaptive and comprehensive legal and analytical frameworks.

While traditional terrorist ideologies continue to pose a threat, the terrorism landscape is no longer defined by discrete, clearly defined ideological movements. Young people are increasingly influenced by a mix of ideologies, conspiracy theories, and hybrid violent extremist movements that do not fit within conventional classifications or demonstrate sustained adherence to a single ideological framework. As propaganda increasingly operates at the intersection of conspiracy theories, misogyny, and violent extremist content, it challenges analytical, prevention, and response frameworks that were developed around more clearly defined ideological categories. This requires Member States, together with digital platforms and other stakeholders, to adapt existing approaches to emerging threat environments and develop more comprehensive legal, analytical, and policy frameworks, alongside adjustments to platform policies and moderation practices.

The intersection of online misogyny and other gendered harms with terrorist and violent extremist propaganda poses challenges for Member States, highlighting the need for more gender-sensitive approaches

The gendered dimensions of terrorist and violent extremist propaganda are increasingly recognized by Member States as a distinct and underaddressed threat, one that existing counter-terrorism frameworks – designed primarily around discrete ideological categories – are poorly equipped to detect or disrupt. Member States and practitioners have expressed concern that violent extremist, conspiratorial, and misogynistic narratives increasingly circulate within overlapping online ecosystems, particularly on social media, gaming and other youth-focused platforms. Yet, counter-terrorism, online safety, and gender-based violence prevention frameworks often operate under distinct legal, policy and institutional frameworks, despite addressing increasingly interconnected harms.

As a result, gaps in detection, attribution and response can emerge, creating opportunities for terrorist and violent extremist actors to exploit these weaknesses. Developing integrated, gender-responsive approaches that bridge these frameworks is therefore both an operational and policy imperative for Member States. It is also essential for ensuring survivor-centred responses and accountability.

[137] Antonia Juelich, *"God Has Helped Us, and So Will AI": How the Terrorist Group Boko Haram Uses Frontier AI* (Cambridge University, 2026).

Counter-terrorism frameworks designed around clearly defined ideological groups are increasingly ill-suited to a threat landscape defined by hybrid identities, decentralized networks, individualized radicalization pathways, and the growing convergence of online misogyny and other harmful online narratives – underscoring the need for more integrated and adaptive policy responses.

Terrorist propaganda operates across digital platforms that fall outside national jurisdictions.

Terrorist groups across the ideological spectrum have developed sophisticated "funnel strategies" –moving individuals from mainstream platforms into progressively more violently extreme and encrypted spaces that fall outside the reach of any single national jurisdiction. Da'esh and Al-Qaida have decentralized and diversified to evade threat detection and disseminate propaganda across borders.[138] These strategies exploit the transnational nature of digital platforms, creating regulatory and enforcement gaps that no single Member State can address unilaterally.

The limitations of unilateral national responses are well documented. When the Government of Somalia banned Telegram and TikTok in August 2023 citing Al-Shabaab's use of the platforms for its recruitment and operations, the ban appeared to have little impact on the group's online networks and was exploited by the group to bolster its narratives around government censorship.[139] This pattern is consistent across groups and regions: crackdowns and suspensions have forced Da'esh and Al-Qaida to find alternatives, but government efforts have only had a marginal impact on overall output and transmission methods. Da'esh temporarily migrated to multiple applications before consolidating on Telegram, and Al-Qaida built a more durable architecture through Rocket Chat's Geo News platform.[140] Addressing this challenge requires coordinated multilateral responses – by governments, platforms, and international institutions – that match the transnational and adaptive nature of the propaganda infrastructure itself.

Platform bans and national takedown orders address symptoms rather than root causes – and in doing so, they can inadvertently validate terrorist and violent extremist narratives about State censorship, which is further exploited by these groups.

[138] Ahmad Helmi bin Mohamad Hasbi, Nurrisha Ismail and Saddiq Basha, "Key trends in digital extremism 2024: the resilience and expansion of jihadist and far-right movements", *Counter Terrorist Trends and Analyses*, vol. 17, No. 1 (January 2025).
[139] Georgia Gilroy (Combating Terrorism Centre at West Point), "The online frontline: decoding Al-Shabaab's social media strategy", *CTC Sentinel* (January 2024).
[140] Héni Nsaibia and Rida Lyammouri (Policy Centre for the New South), "The digital transformations of Al-Qaeda and Islamic State in the battle against online propaganda", 20 May 2021.

Member States must ensure that their efforts to counter terrorist propaganda comply with their obligations under international human rights law.

The Security Council has consistently recognized the role of terrorist content and incitement in facilitating recruitment, radicalization to terrorism, mobilization, and support for terrorist acts. In its resolutions 1624 (2005), 2178 (2014), 2354 (2017) and 2396 (2017), the Council emphasizes that effective responses should promote credible alternative narratives, engage communities, strengthen the rule of law, and address the underlying conditions conducive to terrorism, complementing but extending beyond law enforcement responses. Through the comprehensive international framework to counter terrorist narratives,[141] endorsed by the Security Council in its resolution 2354 (2017), the Council further highlighted the importance of whole-of-society approaches involving governments, civil society organizations, religious and community leaders, women, youth, and the private sector, while ensuring compliance with international human rights law. Additionally, in his 2022 report on countering disinformation,[142] the Secretary-General reaffirmed that while international law requires the prohibition of incitement to violence, any restrictions must meet strict human rights safeguards. The United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has consistently reinforced this position, warning that overly broad counter-terrorism measures risk criminalizing legitimate expression and disproportionately affecting civil society actors, journalists, and minority communities, particularly in the context of online content regulation.[143,144]

In practice, this tension manifests in the full range of measures that Member States employ against terrorist propaganda. Platform takedowns, encryption backdoors, and mass surveillance programmes carry risks of overreach that can suppress legitimate dissent, human rights advocacy, and free speech alongside violent extremist content.[145] As highlighted above, counter-terrorism measures affecting freedom of expression, privacy, and due process must comply with the principle of legality, and rights' limitations must be premised upon assessments of necessity and proportionality, as failures to do so can be counterproductive and reinforce grievance narratives exploited by terrorist groups. Blanket age restrictions, when implemented without robust verification systems, risk leaving the most vulnerable young people with fewer protections rather than more – as platform developers lose incentives to build meaningful safety features for users who simply circumvent the barriers.

Recent developments illustrate these challenges. A growing number of Member States have adopted or are considering legislative and regulatory measures to restrict young people's access to certain online services and social media platforms in an effort to reduce exposure to

[141] United Nations (S/2017/375, annex).
[142] Ibid., Report of the Secretary-General on countering disinformation for the promotion and protection of human rights and fundamental freedoms (A/77/287).
[143] Ibid., Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/HRC/55/48).
[144] Ibid., Human Rights Council, Statement by Ben Saul, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,12 March 2024.
[145] United Nations, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/HRC/52/39).

harmful content and online risks. However, such approaches have also raised complex questions regarding effectiveness, children's rights, privacy, access to information, and the implications of age-assurance mechanisms for broader populations.[146] Human rights advocates have warned that blanket approaches may disproportionately affect children, particularly those who are isolated or marginalized, while age assurance processes present privacy risks for the broader population. They have called for platforms to be made inherently safer and for young people to be meaningfully consulted, rather than excluded.[147,148]

This tension underscores that the protection of human rights and effective counter-terrorism measures need to be mutually reinforcing rather than competing priorities. As consistently emphasized across the United Nations system, the protection of freedom of expression and the right to privacy and due process are not constraints on effective counter-terrorism but foundational to it. Measures that undermine these rights risk fuelling the grievances and mistrust that terrorist narratives seek to exploit. The most effective frameworks are narrowly tailored, evidence-based, subject to robust oversight, developed in consultation with affected communities, and reflect the complementary nature of human rights protection and counter-terrorism measures.

The convergence of terrorist propaganda with financing and governance functions has outpaced Member States' analytical and legal frameworks.

Finance-oriented propaganda campaigns are carried out through a variety of channels, including social media platforms, messaging applications, streaming platforms, traditional media, and in-person outreach, which existing financial frameworks are not equipped to disrupt. The integration of propaganda into terrorist financing architectures presents a specific and underaddressed challenge for Member States, whose counter-terrorist-financing frameworks were designed primarily to identify, trace and disrupt financial flows and terrorist-financing activity rather than address the broader online ecosystems, narratives and networks that enable terrorist financing. At its April 2025 Insight Briefing to Member States, CTED identified a structural development that reframes how propaganda should be understood: for terrorist organizations, propaganda serves to expand their support base, legitimize their actions, intimidate adversaries, and facilitate fundraising activities, including by recruiting donors, soliciting financial contributions and disseminating instructions on how to provide financial support, thereby functioning as the trust infrastructure that enables terrorist financing to scale.[149]

This convergence is increasingly evident across digital platforms. The Financial Action Task Force (FATF) has noted that social media, messaging applications, and streaming platforms

[146] UNICEF, "Drawing a line in digital spaces: age-based restriction of social media", policy note, April 2025.
[147] Australian Human Rights Commission, "Explainer: proposed social media ban for under-16s", 21 November 2024.
[148] UNICEF Australia, "Social media ban" (accessed on 31 July 2026).
[149] United Nations, CTED, "CTED hosts Insight Briefing on how propaganda ecosystems enable terrorist financing", April 2026.

increasingly blur the boundaries between propaganda, recruitment, operational communications, and terrorist-financing activities, complicating detection and disruption efforts.[150] Some terrorist groups continue to operate active crowdfunding campaigns through dedicated digital propaganda channels, using ideological narratives to gain financial support. With regard to XRIRB exploitation of gaming platforms, researchers found that violent extremist actors embed cryptocurrency wallet addresses within streaming content, transforming ideological affinity into economic support, creating potential pathways for the transfer of virtual assets to such actors or supporters and blurring the line between propaganda consumption and financial patronage.[151] Similar dynamics have been documented in Da'esh-linked fundraising networks, where online propaganda and narrative framing are used to mobilize diaspora communities through encrypted platforms and digital payment tools, including cryptocurrency wallets discussed earlier in this report, sustaining decentralized financial flows under the guise of humanitarian support.[152]

These developments have outpaced Member State frameworks, which continue to treat propaganda primarily as a communications issue rather than recognizing its financial, operational and enabling dimensions. FATF notes that while enforcement and compliance mechanisms implemented by social media, instant messaging applications and streaming platforms are primarily focused on the removal of terrorist content, mechanisms and capabilities to identify and disrupt terrorist-financing activity are still being developed. Closing this gap requires enhanced and evidence-based risk understanding, strengthened legal frameworks, inter-agency coordination, enhanced public-private information-sharing mechanisms and deeper engagement between financial intelligence units, counter-terrorism practitioners, technology platforms, and other private sector actors, particularly in addressing the growing use of emerging technologies, virtual assets, and digital financial services for terrorist purposes.

While significant challenges remain, in its engagement with Member States, CTED has identified a number of efforts made by States to adapt responses to address evolving propaganda and recruitment ecosystems. Emerging good practices include the expansion of multidisciplinary intervention programmes for individuals influenced by mixed, hybrid, or ideologically fluid forms of violent extremism; the development of off-ramping mechanisms that connect at-risk online users with offline support services; and the prioritization by some law enforcement and intelligence services of cases involving mixed or hybrid violent extremist narratives as part of threat-assessment efforts. Member States are also strengthening international information-sharing arrangements and practitioner networks to exchange lessons learned on online radicalization to violence pathways, emerging recruitment trends, and the management of increasingly fragmented threat profiles. Together, these efforts reflect a shift from ideology-

[150] FATF, "Detecting and disrupting terrorist financing activity through social media and streaming platforms", June 2025.
[151] Liram Stenzler-Koblentz, Eitan Azani and Carlotta Rinaudo (International Institute for Counter-Terrorism), "From gaming to grooming: how far-right extremists exploit video game-adjacent platforms for radicalization and recruitment", 22 December 2025.
[152] Mona Thakkar (GNET), "Free the captives: Islamic State Central Asian fundraising networks in support of IS families in Syria and Iraq", 13 March 2025.

specific approaches towards more flexible frameworks capable of addressing rapidly evolving and hybrid threat environments.