Evolving Trends in Terrorism and Counterterrorism

Naureen Chowdhury Fink

Since the adoption of the UN Global Counterterrorism Strategy (Global Strategy) in 2006 and the focus on prevention throughout the subsequent reviews by Member States, a key trend shaping the terrorism and counterterrorism landscape has been its shift to online spaces. Although terrorist groups have long thrived on media attention, the adoption of emerging technologies and digital platforms for recruitment, propaganda, and operational planning has been an increasingly key feature of contemporary terrorists and violent extremists. Groups like ISIS recognized the integral role of social media in contemporary life, optimizing these tools to reach and mobilize an unprecedented number of potential recruits and supporters. From livestreaming brutal murders to developing slick outreach material targeted at young global audiences, they heavily invested in proliferating their message through emerging social media platforms to reach their target audience.

This trend has continued with individuals and groups espousing a wide range of ideologies and motivations. During two consecutive attacks on March 19, 2019, during Friday prayers, a perpetrator wearing a GoPro camera killed 51 worshippers at two mosques in Christchurch, New Zealand. The livestreamed attack, which quickly went viral, saw Facebook remove about 1.5 million videos of the attack globally within the first 24 hours. Since that time, perpetrator-produced content has taken the form of videos, images, and related content such as manifestos, as highlighted by the range of activations of the Incident Response Framework of the Global Internet Forum to Counter Terrorism (GIFCT), the mechanism that helps member companies respond to online dimensions of offline violence. These incidents reflect different types of perpetrator-produced online content and activity associated with offline attacks.

The evolution of technology extends well beyond social media, however. The emergence of Generative Artificial Intelligence means that content can be created and disseminated at unprecedented volumes and speed. GIFCT's multistakeholder Working Groups have highlighted a number of associated risks

associated with AI and terrorist content, including the proliferation of deepfakes, the manipulation of legitimate content for malicious purposes, and fostering distrust in media given the presence of questionable AI content. A report from the Konrad Adenauer Foundation (KAS) and GIFCT outlined the uses of AI by violent nonstate actors and noted the importance of these developments for the creation of images, videos, and audio for propaganda and instruction, if not yet for attack perpetration. Moreover, as GenAI is better trained and updated, it offers opportunities for communications and outreach that can emulate the critical social connections that mobilize and incentivize terrorists and violent extremists.

This trend raises three important questions for the design and development of preventive interventions. First, the windows of mobilization have shortened. In earlier decades, individuals were targeted and groomed for years by violent nonstate actors, necessitating travel and training in distant lands. Yet discussions with law enforcement and experts indicate that individuals may be radicalized and mobilized in months, even weeks, leaving little opportunity for threat identification and monitoring. The speed of radicalization or mobilization has been a key concern expressed by several governments.

Second, there are increasing concerns about youth; this is particularly the case for "nihilistic violent extremist" groups or hybrid online subcultures aiming to incentivise gore and violence without an obvious political or ideological goal. These groups have adopted imagery and aesthetics associated with violent far-right groups but have created a gamified ecosystem that celebrates violence and targets young victims, oftentimes with youth as the perpetrators. There are overtones and overlaps with criminal and terrorist groups, warranting a reassessment of traditional counterterrorism and PVE approaches to ensure they respect the rights and needs of minors, while ensuring these hybrid harms are effectively addressed.

Third, terrorist and violent extremist content is not found on a single platform. This necessitates cross-sector and cross-platform collaboration and information sharing and highlights the critical importance of public-private partnerships that include engagement with the tech sector, and avenues for dialogue and collaboration amongst government, industry, academia, and civil society to better understand the threat and develop collaborative solutions. GIFCT's hash-sharing database allows member companies to identify and share known terrorist or violent extremist content in a secure, efficient and privacy-protecting manner. This is one tool in fostering greater cross-platform collaboration.

Challenges for PVE in Policy and Practice

The evolution of PVE approaches has demonstrated the importance of whole-of-government and whole-of-sector collaboration, difficult as that may be in some contexts. Through UN, regional and national counterterrorism strategies and measures to prevent and counter violent extremism, governments, practitioners, and civil society organizations have sought to develop programs focused on community resilience, financial inclusion, strategic communications, youth engagement, education, and supporting women's participation. These have aimed in large part to address what the Global Strategy calls "conditions conducive to the spread of terrorism," and help address the grievances and dynamics that can be exploited by terrorists and violent extremists. There have also been initiatives focused on rehabilitation and reintegration and aimed at preventing recidivism and fostering reentry into communities where feasible.

The development of social media has allowed for rapid shifts in the modes of communication and engagement across global and generational groups. Photos, short-form videos, text and images with text have gained currency, lowering barriers to entry and opening audiences up to content creators and algorithms that can tailor content closely to individual user preferences. Memes, slogans, and hashtags could be used to glorify terrorist acts and disseminate propaganda without being easily identified or recognized as violative content; modifications in games could signal violent ideologies and goals; songs and films could be repurposed by terrorist and violent extremist groups. In this environment, PVE efforts aiming to tackle propaganda or counter speech could be complicated by the utilization of "lawful but awful" content - i.e., content that does not actually violate any laws or platform policies - and be difficult to identify or interpret.

Each year, GIFCT convenes multistakeholder Working Groups to tackle some of the pressing issues raised among the members and the global stakeholder community. In 2025, one of these groups addressed the issue of Addressing Youth Radicalization and Mobilization. Bringing together members of the tech industry, civil society, and practitioners, the discussions highlighted a number of key considerations:

Violent online networks are increasingly targeting children and youth; the convergence of child harms with violent extremist and terrorist groups is taking a wide range of forms, including grooming, radicalization, child sexual abuse, self-harm, and violence against animals. In many of these cases, the violence itself is purportedly the goal, with perpetrators vying with peers to gain status through the commission of violence.

Online subcultures, such as gaming communities, can bring together legitimate players and participants, but also those seeking to disseminate hate-based extremist narratives. They can foster conditions that lead perpetrators to undertake "clout-based" criminal acts and use "edgy" humor to normalize violence or evade content moderation.

These trends and dynamics highlight another key shift in terrorism and counterterrorism over the past two decades: the threats are increasingly diffused and decentralized. A recognizable group "brand" has been less important in attacks perpetrated by individuals rather than those organized and publicly acknowledged by groups. This raises questions for governments and practitioners about the design and development of PVE programs that target specific ideologies, groups, or geographies.

GIFCT's initial taxonomy for the hash-sharing database, designed to reduce the possibility for perpetrator content to go viral online and prevent the recirculation of content that might incite or motivate violence, was centered on the UN Counterterrorism Sanctions list established by Security Council Resolution 1267, and subsequently, Resolution 1989, focused on ISIL and Al-Qaida. However, the need to address attacks perpetrated by individuals unaffiliated with these groups and espousing a wide range of ideologies led to the addition of behavioral indicators for determining inclusion in the hash-sharing database

For PVE practitioners centered on tackling ideological motivations and goals, this diffusion and diversification bring with them a challenge of developing ideologically agnostic programs and approaches. In the UK, the *Prevent* program was created to offer individuals tailored interventions and support, and a referral system to offer those at risk access to services, including counseling, employment, education, or other resources as needed. In 2023/2024, the Home Office reported that 36% of the referrals were related to individuals with a vulnerability, but "no ideology or CT risk." For ideological referrals, 19% were related to extreme right-wing; 13% related to Islamist radicalization. Of all the Prevent referrals in 2023/2024: the remaining 3% were related to concerns regarding school massacres or incel-related issues.

Considerations for Future Approaches to Preventing Violent Extremism

The trends and challenges highlighted above raise a number of issues for policymakers and practitioners looking ahead to the review of the Global Strategy in summer 2026 and the field more widely. Although the previous reviews have yielded lengthy outcome documents with over 100 operative paragraphs, they do

not always reflect contemporary aspects of the threat, such as the online dynamics. Below is a set of considerations for states and experts in the coming months:

- **Invite the private sector to join deliberations on preventing and responding to violent extremist threats.**

The private sector includes entities of diverse sizes, goals, and capabilities, and may have many of the key resources needed for PVE, including social media platforms, commercial media and messaging outlets, arts and culture institutions, for example. Bringing in their perspectives and knowledge to develop solutions, while also deepening their understanding of various contexts and dynamics, can help actors leverage collective capabilities to develop and deploy tailored PVE solutions.

- **Foster approaches to prevention programming that are ideologically agnostic but can be applied to a range of motivations.**

Developing programs and tools that can adapt to diverse motivators or ideologies will help prepare for a range of needs. These approaches may be focused on terrorist acts as defined in international and domestic laws, and aligned with international human rights obligations, and therefore be more reflective of current trends and evolutions.

- **Recognize interrelationships between online and offline dynamics, and continue to invest in offline prevention strategies.**

“Push factors,” including grievances relating to governance, human rights violations, personal trauma, social isolation, marginalization, perceived or experienced injustices, for example, continue to be reflected in the stated motivations of many perpetrators of violent acts, including those with online components. Discussions with frontline practitioners continue to highlight many of the risks and vulnerabilities that may create an enabling environment for terrorists and violent extremists to exploit or incentivize individuals. Continued investments in empowering community organizations, local governments, and frontline practitioners, remain key to supporting efforts to support vulnerable individuals or groups.

- **Establish a grant-making body to support local and community actors to implement the Global Strategy through emerging technologies**

The UN could establish a grant-making body, or work via existing mechanisms like the Global Community Engagement and Resilience Fund, for example, to support local and community actors to develop PVE programs and projects in line with the Global Strategy and to ensure these are reflective of current threats and trends. These grants may support working with governments and/or the private sector, and allow for the development of capacities and resources to work with emerging technologies, including Generative Artificial Intelligence, to develop effective and timely projects to prevent violent extremism.

The views expressed in this article, and all errors or omissions, are those of the author alone and do not represent the views of GIFCT.

About the Author

Naureen Chowdhury Fink is the Executive Director at the Global Internet Forum to Counter Terrorism (GIFCT). Prior to this, she was the Executive Director at The Soufan Center, and before that, a senior policy adviser on counterterrorism and sanctions at the U.K. Mission to the United Nations, leading related negotiations in the UN Security Council and the General Assembly. She has previously worked at the UN Counter-Terrorism Committee Executive Directorate (CTED) and UN Women.

Before joining the United Nations, she was head of research and analysis for the Global Center on Cooperative Security, leading the multilateral security portfolio on the international response to terrorism and violent extremism, armed conflict, and political instability, and the role of international and regional actors. This built on her earlier work at the International Peace Institute, where she developed the portfolio on counterterrorism and transnational security threats and was an active contributor to the IPI Global Observatory.

She has developed and implemented multi-stakeholder CT and PCVE projects across the globe, in regions as diverse as West Africa, Europe, and South Asia, and published widely on counterterrorism, gender, sanctions, international security, and the UN. She is a regular speaker at international high-level events, in the media, and at conferences bringing together policymakers, civil society, academia, and the private sector.