

Fighting Terror with Tech: The Evolution of the Global Internet Forum to Counter Terrorism

Naureen Chowdhury Fink & Erin Saltman

Abstract

This chapter presents phases of the Global Internet Forum to Counter Terrorism's (GIFCT) evolution, from a multilateral tech initiative to an independent non-profit organization managing tools, incident response frameworks, and knowledge-exchange for an increasingly diverse range of platforms. To be effective, there is an important feedback loop between member companies and the multistakeholder community, which is adapted each year to reflect external dynamics and member priorities. In online safety efforts, there is the need to continue reviewing, refining, and adapting tools and solutions. This is particularly key as emerging technologies and capabilities associated with GenAI combined with amorphous online communities compel a reassessment of the threat environment and counterterrorism responses. In the trust and safety space, the lessons learned, and tools developed to solve for one harm type can often provide a roadmap to inspire approaches in tackling other harm types. We hope that GIFCT's journey can help guide further efforts.

Keywords: counterterrorism, counter-extremism, online harms, GIFCT, multistakeholder, hash-sharing, GenAI, incident response.

Introduction

This chapter serves as an illustrative case study from the trust and safety sector, highlighting the evolution of a unique industry-led structure aimed at preventing and countering terrorists and violent extremists from exploiting digital platforms. The Global Internet Forum to Counter Terrorism (GIFCT), first convened in 2017, was born out of the need to create a space for cross-platform collaboration to counter terrorist threats online posed by ISIS, largely through shared tooling. Efforts had to evolve further in reaction to the terrorist attacks carried out in Christchurch, New Zealand, where the perpetrator livestreamed his attacks at two mosques in 2019, initiating the need for shared incident response protocols and an independent structure.

Now GIFCT faces a third evolutionary turn with the acceleration of emerging technologies and atypical threat actors, requiring nuanced knowledge exchange and signal sharing. These evolutionary phases have

seen efforts grow and change the nature of how GIFCT is governed and functions; from a cross-platform initiative led and managed by four tech companies, to an independent non-profit supporting cross-platform and cross-sector efforts with over 35 tech company members.

As this chapter highlights, knowledge exchange between industry, governments, law enforcement, and civil society is critical. As GIFCT enters a distinct third phase in its organizational journey, there will be a need to adapt to adversarial shifts and industry tools. Still, the case study GIFCT offers may be useful for others developing cross-platform and cross-sector solutions to tackle online harms. Multistakeholderism is not just a “nice-to-have,” but a necessary component of understanding the threat, developing solutions, and deploying best practices at scale. To ensure effectiveness GIFCT weaves multistakeholder approaches throughout its workstreams. Regional workshops bring together industry, international organizations, officials, and civil society experts to exchange knowledge. Webinars and virtual events allow for broad-based awareness, and the Global Network on Extremism and Technology (GNET), GIFCT’s academic arm, connects industry to global experts and perspectives and offers global insights for the research and practitioner communities.

In the mid 2010s the nature of terrorist content online began to reflect broader cross-platform internet usage and saw an unprecedented volume and scale in content developed to recruit, support, glorify, finance, and perpetrate terrorist acts. Thus, the need to bring together not only big, but diverse tech industry members has been reflected in the expansion of GIFCT. This chapter examines the context in which this took place and the key issues driving these developments, providing a retrospective on the emergence and evolution of GIFCT.

The Why Now and What For: GIFCT Foundations

Between 2014 and 2017 it became apparent to the world that there was a new form of Islamist extremist terrorism on the rise in the so-called Islamist State, or ISIS. Members and sympathizers of ISIS were

unabashedly open about embracing social media and wider online technologies to radicalize, recruit, and distribute propaganda (Saltman & Winter, 2014). Previous international terrorist organizations, such as Al-Qaeda, were shrouded in an ethos of secrecy and limited distribution of propaganda through trusted networks online and offline. ISIS, in comparison, widely used Twitter, Facebook, Tumblr, Reddit, and other public forums openly, successfully recruiting men and women of different socioeconomic backgrounds estimated at 30,000 fighters from more than 85 countries as of December 2015 and developing targeted strategic communications to persuade recruits and incite violence (Benmelech, E. & Klor, E.F., 2016).

As international concerns about terrorism heightened against the backdrop of a brutal civil war in Syria and lone actor attacks across Europe, the European Commission launched the EU Internet Forum (EUIF) in December 2015 to address the misuse of the internet for terrorist purposes. The EUIF's goals were to reduce accessibility to terrorist content online and increase the volume of effective alternative narratives online (European Union Internet Forum, 2025). Social media companies were brought to the table by the EUIF, the United Nations Security Council's Counter Terrorism Executive Directorate (UN CTED), and individual countries asking companies to discuss their policies and practices for effectively identifying and removing terrorist content. In the hallways and coffee breaks of these meetings, company representatives would talk to each other and compare notes on major online terrorist trends.

For tech platforms, it was very apparent early on that no single platform alone could track the online lifecycle of terrorist recruitment, propaganda dissemination, and operationalization. For example, early outreach from an ISIS recruiter might start on one larger, open social media platform, and migrate their target quickly to a smaller, less regulated platform where the conversation became more specific. This became even more apparent as larger, better-resourced platforms began to crack down on terrorist content at scale, leading to a jihadist information ecosystem that was (and is) a large and complex network, connecting a vast array of platforms (Fisher, A. et. al., 2019). Adversarial shifts, coded language, and the exploitation of newer, smaller platforms were apparent. It was clear that companies needed a more structured approach to working with one another on countering terrorism and violent extremism.

Pressure on leading social media platforms was mounting in 2016 through the EUIF, UN CTED, G7, and Five Eyes governments to better scale efforts to counter terrorist content online as ISIS waves of violent propaganda became commonplace. Since the attacks of September 11, 2001, there had been widespread efforts through forums like the United Nations to foster international legal and policy frameworks to address terrorist threats in partnership with civil society and practitioners. However, the private sector had been underrepresented in these efforts. In parallel, there was no existing peer space where tech companies could meet to discuss trends, share knowledge, and explore cross-platform tooling and solutions. Thus, in December 2016, Facebook (now Meta), Microsoft, YouTube, and Twitter (now X) launched the infrastructure for a hash-sharing database (see: HSDB reference) to focus on known terrorist content (Verney, 2016), and, by June 2017, the Global Internet Forum to Counter Terrorism was established.¹ As such, GIFCT was formed as a voluntary consortium, a tech-led initiative to foster collaboration among tech companies, advance relevant research, and share knowledge (see: Meta Blog, 2019).

Within its first six months of being established, GIFCT had hosted multistakeholder convenings in San Francisco, New York, Brussels, and Jakarta. These created important opportunities for policymakers, practitioners and civil society organizations to better understand the approaches and solutions offered by tech platforms, and vice versa, for the tech sector to deepen understanding of terrorism and counterterrorism dynamics. By the end of 2017, GIFCT announced it had added its first 40,000 hashes and added seven companies to the hash-sharing database and an academic wing was established to connect industry to global experts who could publish on terrorist and violent extremist trends online (see: Meta Blog, 2019b). An increasing number of tech platforms were being drawn to the GIFCT initiative, diversifying the tech stack involved and speaking to industry needs on this topic. GIFCT was rapidly expanding beyond the capacity of what a multilateral initiative managed between four companies could fully handle—when a new form of terrorist threat hit platforms.

¹ The original inclusion parameters for the hash-sharing database transparently stated that the content hashed must be associated with a terrorist entity on the United Nations Security Council’s Consolidated Sanctions List. This was the main point of common ground that tech companies could agree constituted “terrorist content”. This included all ISIS and Al-Qaeda affiliated groups and their published content. See: HSDB Taxonomy.

From Voluntary Consortium to Independent Non-Profit Organization

On March 15, 2019, a white supremacy inspired lone terrorist killed 51 worshippers at the Al Noor and Linwood mosques in Christchurch, New Zealand. The attacker livestreamed the murders on Facebook and imbued the video with a gamified sense (Macklin, 2019). He also released a 74-page manifesto online to ideologically justify his targeting of the Muslim community. The virality of the attacker video and manifesto went above and beyond what most terrorist specialists had ever seen before. Facebook reported it removed an estimated 1.5 million uploads of the attack video globally within the first 24 hours after the attack, blocking 1.2 million shares at the point of upload (Sonderby, 2019). YouTube reported its systems saw videos of the attack being uploaded at a rate of one per second directly after the shooting (Dwaskin & Timberg, 2019). The Christchurch attacks represented a new form of viral online terrorist content, inspiring a new generation of white supremacy and accelerationist attackers.

This attack led GIFCT to enable its first “incident response” protocol, allowing for the labelling and hashing of perpetrator content associated with the attack. Previously, content within the hash-sharing database had to correlate with groups and individuals on the United Nations Security Council Consolidated List associated with sanctions under Resolution 1267 on groups and individuals associated with Al-Qaeda and ISIS, reflecting international consensus through the Security Council for over two decades (see: UN Security Council Consolidated List). The inclusion of hashed material from the Christchurch attacks represented a new development for GIFCT’s database in expanding to content meeting certain behavioral, rather than list-based, criteria. The scale of the online spread of the attack material lent itself to this rapid shift in approach. Within 48 hours after the attack, the hash-sharing database housed over 800 visually distinct hash variations of the attacker video and was able to share URLs and context on enforcement to GIFCT members (see: GIFCT Industry Cooperation).

The decision to transform GIFCT into an independent non-profit organization was closely shaped by the need to expand the scope of GIFCT to include global, cross-platform incident response work while welcoming a growing number of industry members. GIFCT also enhanced and solidified its membership criteria, ensuring companies met certain transparency, human rights, and policy frameworks before joining. As a diverse set of tech platforms looked to join GIFCT, an independent organization was best placed to work consistently with incoming companies, rather than having assessments carried out by peer tech companies (GIFCT Membership, 2024). As new technologies and tactics emerged, adversaries adapted to counterterrorism and online moderation efforts targeting terrorist and violent extremist content. This shift highlighted the increasing need to ensure a space for intra-industry and multistakeholder collaboration, and GIFCT continued to grow beyond the initial four members.

At the 2019 opening of the United Nations General Assembly session, then-serving Prime Minister Jacinda Ardern of New Zealand and President Emmanuel Macron of France held an event discussing GIFCT's progress with the founding company leads, announcing that GIFCT would transform into an independent non-governmental organization (NGO), underscoring its complementarity with the government-led Christchurch Call to Action. The Christchurch Call was therefore established as a government-led initiative in 2019 with the goal of eliminating terrorist and violent extremist content online and worked directly with GIFCT member companies to develop a 9-Point Action Plan. This included both individual platform actions and collaborative actions (Microsoft Blog, 2019). All this took place against the background of an international push for collaboration to address a diversified terrorist threat that went beyond the Islamist extremist groups that had mobilized much of the counterterrorism effort globally until then. The emphasis on the need to address extreme white supremacist and accelerationist violent online content therefore shaped the follow up actions after the attack.

Furthermore, they announced that GIFCT would officially lead an industry focused Incident Response Framework (IRF) to guide a collaborative response amongst GIFCT members to terrorist attacks, commence publishing an annual transparency report, publish a cross-platform Campaign Toolkit to help civil society organizations build online campaigns to challenge hate based extremist ideologies online,

and release algorithms for hashing image and video content to aid smaller companies joining the database (see: Next Steps for GIFCT). In this transition, the four founding member companies became the NGO's Operating Board, and the Board representatives set up an Independent Advisory Committee (IAC) made up of government and non-governmental representatives to guide GIFCT and the Board on key issues. Thus, "GIFCT 2.0" emerged in 2020 as an independent 501(c)(3) non-profit organization.

From Infancy to Maturation: Evolving as an Independent Non-profit

Organization

Since its establishment as an independent non-profit organization, GIFCT has evolved its mission to reflect changes in the adversarial threat landscape and the needs of industry members and partners. The initial years forged a unique tech-led space for industry members to engage with a multistakeholder community of government, practitioners, academia, and civil society organizations. Global attention at that time was focused on transnational terrorist groups like ISIS and Al-Qaeda. ISIS produced branded propaganda, publications, and exploited new platforms to scale up the reach and volume of their materials, including through clearly associated social media accounts purporting support for the group (Fink, 2025). Videos and photographs of murder, violence, and torture were widely associated with the group's modus operandi. As Sara Zeiger and Joseph Gyte noted, "the information revolution has also helped terrorist groups to move away from that of a traditional war model and move towards a new mode of conflict at societal levels. "While terrorist organizations have always put effort into conducting psychological operations, they now have the capacity to conduct information operations on a much grander scale" (Zeiger & Gyte, 2021).

GIFCT's expanded membership—growing from an initial four to over thirty member platforms by early 2025—highlights the diversity of tactics adopted by terrorists and violent extremists across various ideological spectrums and represents an important cross section of the tech stack (see: GIFCT Membership). While member platforms continue to skew towards those hosting user-generated content,

there are also a range of companies that have strengthened efforts to prevent exploitation by terrorists or violent extremists, including platforms representing gaming, marketplace and e-commerce, fintech, E2EE, and travel booking sites.

GIFCT's mission has continued to gain momentum; the workstreams and activities developed each year are designed to reflect the needs, feedback, and priorities of member companies. Beyond industry, GIFCT's unique governance structure allows for inputs from governments and civil society through an IAC, which includes government and civil society representatives, and whose contributions help inform GIFCT's priorities and activities (see: GIFCT Governance). Additionally, each year, GIFCT convenes cross-sector Working Groups to deliberate on topics critical to GIFCT's activities and tools. The Working Groups also allow for a cross-pollination of ideas and experiences through multistakeholder engagement; they allow for civil society members to share concerns and priorities and engage with industry actors directly and for industry to better acquaint practitioners and policymakers with the solutions they've developed and the challenges they've addressed.²

The overarching trajectory for GIFCT's evolution has been to become increasingly member-centric while connecting key stakeholders to share lessons learned, resources, and good practices. Such a multistakeholder approach has been especially important in GIFCT's regional events and workshops, developed with a regional or national partner. In addition to supporting outreach to industry in other regions, these workshops allow for the development of a deeper understanding of threats, trends, and contexts in a region and an expansion of a global network of experts to inform and support GIFCT members and stakeholders. Recent regional engagements have focused on West Africa, Nordic countries, Asia, and Latin America (see referenced GIFCT Blog Posts on each regional workshop).

² GIFCT Working Groups have evolved into more targeted convenings focusing on key themes or tools that directly shape GIFCT's work and activities. In 2025, for example, these focus on investigating online harms through a dedicated community of practice; identifying threats and opportunities within artificial intelligence (AI); and addressing youth radicalization and mobilization (see: Year 5 Working Groups). Previously, such Working Groups have produced reports on GIFCT's Incident Response Framework (see: IRWG, 2025); Red Teaming (Thorley, 2023) and Blue Teaming new technologies (Saltman & Johnson, 2023); creating best practices for risk mitigation on gaming threat surfaces (Kowert & Chittick, 2025); and reviewing inclusion parameters for the hash-sharing database (Doody, S. & Jensen, M., 2024).

In 2024, GIFCT adopted a new three-year Strategic Plan, which provides a roadmap to build on the strong foundations created while also reflecting member and stakeholder feedback. It also represents a maturation of the organization and reflects the increasingly diverse and expanded industry membership, and the updated tools and supports GIFCT can provide them against the background of an evolving threat landscape. Between 2025 through 2027, GIFCT aims to support and strengthen a collaborative tech-led, multistakeholder community to develop and share cross-platform solutions and support. This includes facilitating information sharing and knowledge exchange to increase collective capacities of the tech sector, and delivering on incident response to inform industry efforts to prevent the exploitation of digital platforms and respond to terrorist and violent extremist events with significant online aspects. It also has a key focus on ensuring global perspectives and analysis is brought to the tech sector to fully understand threats and solution potentials.³

Although the wider contours of GIFCT's work have remained steadily focused on delivering on its original mission, the updates and changes reflect organizational maturation and greater recognition within and outside industry of the importance of cross-platform collaboration. At the beginning of 2025, GIFCT integrated the full suite of membership support services in-house and fostered partnerships to offer targeted support. Integrating new member outreach and engagement, providing support to current members, and fostering ongoing dialogue and engagement with this key stakeholder community are key. These workstreams will enhance GIFCT's ability to direct engagement with companies and provide

³ GIFCT's updated 2025 - 2027 Strategic Plan offers some strategic coherence and is centered on three key goals: (1) *Enhance the collective capacities and capability of the tech industry and its partners and support them to adapt to a dynamic threat environment, including by connecting industry to expertise and regional stakeholders; delivering curated and action-oriented analysis, recommendations, and activities; fostering a network of expert partnerships; and ensuring that GIFCT members are well placed to respond to terrorist and violent extremist content online.* (2) *Strengthen and diversify a global approach to delivering on GIFCT's mission and foster a diverse community of GIFCT member companies reflective of the evolving threat landscape and a global perspective drawn from a multistakeholder community that includes industry, government, and civil society representatives.* (3) *To achieve these goals, the Strategic Plan sets out several core objectives and indicators to ensure alignment with GIFCT activities and initiatives, even as events and crises may also require the organization to adapt to emerging trends or crises, and industry needs, to ensure that GIFCT is actually responsive to developments on the ground and evolving member priorities.*

continuous overviews while better understanding the needs and priorities of platforms in addressing terrorist and violent extremist content.

For many companies joining GIFCT, the hash-sharing database remains a critical tool in the event of incidents or the emergence of terrorist and violent extremist materials that meet the database inclusion criteria. At the same time, the diversity of member companies has also compelled GIFCT to consider additional updates to incident response frameworks and to consider a wider range of content related to offline incidents. The updates to the IRF in 2025 reflect the long list of activations since GIFCT's inception, as well as the feedback from members, affected communities, civil society, policymakers and practitioners (see: GIFCT Incident Response Working Group Report). However, updates will also incorporate lessons learned from each activation, which have generated greater awareness and understanding across the GIFCT team of the various needs and expectations around each incident.

GIFCT's commitment to connecting member platforms with global research and analysis, as well as experts from across a range of academic disciplines, remains unchanged. GIFCT's academic wing, GNET, housed in King's College London, remains a key vehicle for ensuring that tech companies can deepen understanding of the various regional and contextual dynamics, cutting-edge research, and emerging trends to better identify and address terrorist and violent extremist content (see: GNET). The GIFCT team has worked closely with GNET to align on member needs and priorities and highlight dynamics in regions where ongoing violence and conflicts may be generating content and conditions resulting in terrorist and violent extremist content online.

Futurecasting “GIFCT 3.0”

Like law enforcement and offline safety fields, as the efforts to challenge and counter a threat evolve, so too do the adversarial shifts. Reflecting on the foundations of organizations like GIFCT, the initial hurdle was to create tools and institutional structures that could address a defined content threat as it spread

across platforms, largely social media platforms. Since its foundation in 2017 a lot has evolved, above and beyond social media platforms and expanding to review new forms of violent extremism and terrorism.

There is an important feedback loop from member companies and the multistakeholder community which is adapted each year to reflect external dynamics and member priorities. Each year, for example, GIFCT updates the themes and focus areas of its Working Groups to work on newly identified threats or safety gaps. It is only through this perspective that a better comprehension of threats and solutions can be developed, so while the new Strategic Plan offers a roadmap for GIFCT activities, it also allows for adaptation as member priorities and needs evolve.

As the terrorism and tech landscapes have continued to shift, new challenges and opportunities have emerged for GIFCT and its related practitioner community:

1. New technologies;
2. A diversified tech stack;
3. Undefined networks and actors.

New Technologies

New technologies posing concerns for tech companies and governments alike include the exploitation of generative artificial intelligence (GenAI), the misappropriation of unmanned aerial devices (or drones), and the abuse of 3D printing technologies to make bespoke weapons (see: 79th UNGA GIFCT Blog Post).

AI is increasingly deployed for everyday use by individuals around the world. This can be seen in the increased use of chatbots, search engines, and graphic design support. In parallel, there has been rising concern about the risks posed by GenAI for terrorist and violent extremist purposes. Researchers have

already identified groups exploiting GenAI tools to scale propaganda and recruitment efforts through enhanced image, audio, and video designs (Saltman & Gilmore, 2025; Borgonovo, Bolgpani, & Rizieri, 2024; Dean, 2025; Engler, 2023) and through chatbots that can deliver more personalized messaging and outreach to vulnerable users (Lakomy, 2023). As GIFCT’s 2023 Working Groups highlighted, AI can facilitate terrorist groups in the production “deepfake” images or audio, including in overlaying music or voices to exploit popular themes and music, both aiding misinformation campaigns as well as creating popular subcultures bringing in a new wave of younger audiences (Saltman & Gilmore, 2025; Engler, 2023).

Beyond propaganda creation and recruitment efforts, there is also increasing concern that GenAI tools can be used to optimize surveillance and weapons capacities by malicious actors when combined with other technologies. Facilitated by the circulation of operational instructions online, practitioners have growing concerns about innovative weapons creation and attack optimization.

Experts have also flagged concerns about the circulation of information regarding bomb making, 3D printed firearms, and future potentials of chemical and biological weapon design. Some cases in the United States, for example, have reported a “3D2A” movement combining 3D printing with accelerationist interpretations of the Second Amendment to develop fully or partially 3D printed guns (see: 3D2A GNET Insight). Terrorist groups have also expanded their use of drone technology in recent years, notably in East and Central Africa, where groups like Al Shabaab and wider Al-Qaeda and ISIS-affiliated groups have used drones for reconnaissance and to record footage to be used for propaganda (Aguilera, 2023; Figueireda, 2024). These new threats also speak to a diversified tech stack in need of trust and safety sector engagement.

A Diversified Tech Stack

Some statistics note that the average smartphone user has 80+ apps on their phone with ± 30 apps used with relative fluency monthly. It follows that we shouldn’t be surprised that the average bad actor is

equally using a diversified range of apps and online tools in a rational choice way to optimize getting things done. Bad actors, in a similar fashion to the average normative user, are using online spaces to get things done more quickly, more cheaply, using apps to reach more global audiences, speaking privately with a defined inner circle, buying goods and services, arranging travel, and raising funds. Subsequently, when thinking through counterterrorism efforts online, the tech stack of concern has grown; a wide range of global violent extremist and terrorist groups have been documented exploiting a wide range of technologies.⁴

This means that no one approach to countering terrorism and violent extremism is foolproof; cross-platform and cross-sector knowledge exchange is therefore ever-more important. Social media, gaming platforms, marketplace and e-commerce, fintech, blockchain, telecommunications, E2EE, online streaming of video and audio, travel booking sites, and even dating sites all have vectors for exploitation. Increasingly, this tech stack is also growing outside of the United States, bringing different languages and regional needs to the table. This diversity is similarly reflected in the expanding membership of GIFCT (see: GIFCT Membership). Some tools will work well across certain types of platforms and other approaches will be needed for others.

Despite some concerns that emerging technologies will render all previous solutions obsolete, the GIFCT experience highlights the need for a process that expands the instruments in the toolkit and not necessarily replaces them. As an example, hash-sharing technology will continue to be a key cross-platform signal-sharing effort for platforms that have high volumes of user-generated content, particularly image or video content being shared. Meanwhile, for gaming platforms or marketplaces, knowing basic coded language, symbols, and key figures being used by bad actor networks will go a long way in proactive threat

⁴ For a diverse range of examples being tracked by researchers around the world we recommend visiting the website of the Global Network on Extremism and Technology (GNET). GNET is the academic research arm of GIFCT, housed within the International Centre for the Study of Radicalisation (ICSR) at King's College London. GNET aims to better understand the ways in which terrorists use technology and publishes new insights from experts each week. See GNET Insights: <https://gnet-research.org/resources/insights/>.

detection. As such, in recent years, GIFCT has set up “communities of practice” to allow specific sides of the tech stack to meet and discuss challenges and best practices.⁵

Undefined Networks and Actors

When GIFCT was first formed, it was in the face of a well-defined threat, which met with global consensus in the post-9/11 era; both Al-Qaeda and ISIS remain the only two groups recognized by the United Nations as threats to international peace and security (Wachtel, 2024). These groups recognized the importance of communication and sought to clearly brand their communications and “own” the narrative. In 2002, Osama bin Laden declared, “It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90 percent of the total preparation for the battles.” (Chowdhury Fink & Barclay, 2013).

At that point in time there were clearer online signals for moderators to action, given the more explicit associations with terrorist content. Ten years later, this easily definable content and online profiles are less readily apparent. While it might exist in some spaces, the obvious terrorist activity remains on smaller, less-regulated platforms less willing to join efforts like GIFCT, the EUIF, or the Christchurch Call. It is also the case that most lone actor attackers do not fit neatly into well-defined organizational boxes, often highlighting a combination of accelerationist, white supremacist, and anti-government sentiments.

Some experts have called this new wave of violent extremism a form of “post-organizational terrorism” (Davey, et. al., 2022). There is a string of groups praising or encouraging violent attacks within online communities that have mixed and varied ideological sympathies. This is combined with online subcultures steeped in increased coded language, meme-based communication, and satirical framing. Networks online linked to various violent extremist and fringe subcultures—including Terrorgram (Kriner & Ihler, 2022), 764 (Argentino, et. al., 2024), and Soyjak Party (Moerking, 2023) —are examples of

⁵ As examples, the 2024 Gaming Community of Practice produced a report on CVE Efforts in Game Spaces (Lamphere-Englund, 2025a), a best practice guide for specific game-play threat surfaces (Kowert & Chittick, 2025), and an annotated bibliography highlighting global open-source research to date about gaming and extremism (Lamphere-Englund, 2025b).

online violent extremist movements making it difficult to build concrete definitions and policies and even more difficult to enforce them at scale. If anything, these trends speak to the critical need for an ongoing dialogue between practitioners, experts, law enforcement, and platforms. GIFCT continues to lean in on its IAC to highlight regional trends and areas of concern and continues to work with its academic wing (GNET) to proactively highlight evolving trends and actionable recommendations for tech companies. The adversary shifts, and so too do the many trust and safety practitioners countering the threat.

Opportunities and Next Steps

In the trust and safety space, the lessons learned, and tools developed to solve for one harm type can often provide a roadmap to inspire approaches in tackling other harm types. GIFCT did not emerge in a silo of counterterrorism expertise, rather, it was able to form because of the trust and safety approaches that had been developing to tackle other online harms. Organizations like the Technology Coalition paved the way to show what an industry-first, cross-sector organization could look like, using hash-sharing technology to counter child sexual abuse material (CSAM).⁶ The Global Network Initiative (GNI) also exemplified what multistakeholder efforts across government, tech, and civil society could look like in efforts to champion human rights in digital spaces (see: Global Network Initiative). Trust and safety efforts can draw on the wealth of experience brought by practitioners, academics, and community organizations in mitigating violence and online harms, and vice versa, as these same stakeholders can also better optimize their utilization of tech through cooperation.

In its evolution, GIFCT will work with member companies and multistakeholder partners to continue reviewing, refining, and adapting tools and solutions through iterative processes that reflect feedback and insights from key stakeholders. This is particularly key as emerging technologies and capabilities

⁶ Hash-sharing technology means that content found by one company can be “hashed” in its raw form, ensuring there is no link to any original platform or user data. Hashes appear as a numerical representation of the original content, and cannot be easily reverse engineered, allowing a singular platform content signal to become a one-to-many signal, amplifying moderation efforts (see: GIFCT: *What is the Hash Sharing Database*).

associated with GenAI, as well as global geopolitical dynamics and developments, compel a reassessment of the threat environment and counterterrorism responses.

However, GenAI also presents tremendous opportunities to boost efforts to prevent and counter terrorism and develop more effective trust and safety solutions. Natural Language Processing can help identify hateful or prohibited content more easily, particularly where linguistic capabilities and cultural understanding may be limited (Nelu, 2025). The scope and volume of content that can be scanned by AI for harms can be increased exponentially, while reducing the potential harms to content moderators who have had to directly review and assess violent and harmful content. AI also presents the potential for more tailored and effective positive interventions with chatbots developed to help engage and redirect or support individuals who may be seeking to disengage from violence, or to find alternative means of addressing grievances without resorting to violent extremism.

What has become clear after several decades of collective efforts to address transnational terrorism and related threats and their online dimensions, is that no single actor can address them effectively alone. The global scope of groups like Al-Qaeda then ISIS underscored the need for collective international action and interagency cooperation. Similarly, adversarial migration to a range of tech platforms underscores the importance of cross-platform, and cross-sectoral collaboration. GIFCT has had deep and longstanding partnerships with the United Nations, the European Union, the Organization for Security and Cooperation in Europe, the Global Counter-Terrorism Forum, The Aqaba Process, and numerous governments and civil society networks around the globe. Their inputs inform GIFCT's awareness and understanding of threats and solutions.

GIFCT is unique in bringing together a range of perspectives on terrorist and violent extremist content to the tech industry and working in partnership to develop the best risk mitigation strategies. Multiple jurisdictions are represented on the IAC; member companies are increasingly based in various regions, which have different regulatory and cultural environments. Building diverse perspectives, geographies and sectors into an organizational strategy does not mean the goal will be full agreement or convergence

in approach. The IAC, Working Groups, and regional workshops often, and proactively, highlight points of disagreement and misalignment between sectors and proposed solutions. However, everyone at the table finds common ground in the aligned overarching mission, to work together in countering terrorism and violent extremism. Understanding where points of disagreement come from, and empathizing with the reasons behind misalignment allows each sector to embrace where there are points of common ground.

Given this diversity, ensuring a commitment to human rights will remain paramount as a foundational principle for ongoing cooperation. Unusually for a small non-profit, GIFCT conducted a Human Rights Impact Assessment in 2020 (see: BSR Human Rights Assessment) and has been working over the years to implement various recommendations. At the same time, member platforms make a commitment to human rights and transparency as part of the joining criteria for GIFCT, aligning with the United Nations Guiding Principles on Business and Human Rights (see: GIFCT Membership). This commitment is enshrined in the membership criteria, informed by longstanding multistakeholder consultations, and continues to be mainstreamed throughout GIFCT's interactions and activities.

Conclusion

Terrorists and violent extremists have already proved themselves to be opportunistic actors, deploying new tactics and approaches as they arise, whether it is through the exploitation of a cassette tape or an app. As such, ensuring that efforts to prevent and counter terrorism can leverage the opportunities presented by industry will continue to be essential as new technologies continue to emerge.

Although counterterrorism has often been the remit of the State and its law enforcement ecosystem, the establishment of GIFCT highlights the critical role of the private sector and multistakeholder partnerships. Collaboration to identify and classify harms, deepen understanding of the relationships between offline and online dynamics, innovate tech solutions and tools, and share lessons learned is essential to ensure a

range of companies can be prepared to respond. While GIFCT's membership is focused on industry, its programs and events incorporate a strong multistakeholder dimension precisely so that sectors can benefit from each other's experiences. In the early post-9/11 years, counterterrorism efforts rarely integrated the private sector. The evolution of GIFCT highlights the importance of cross-sector collaboration.

While this chapter maps some of the current and predicted future threats and opportunities, the trust and safety space remains unpredictable. As new tools and platforms appear, so too will new threats and opportunities. For many online harm types, a safe and voluntary space for tech companies to learn, exchange knowledge, share incident awareness, and benefit from cross-platform tooling does not exist. Entities like GIFCT have grown and evolved in response to tech companies seeking out this support and reiterating through their engagement the need for an industry-led space for cross-platform collaboration and multistakeholder engagement. Ensuring the trust and space needed for cross-platform collaboration and a connection to global expertise will be essential for the development of sustainable, effective, and credible solutions.

Author Bios

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, 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 and brings nearly two decades of experience in nonprofits and international security to her current role.

Dr. Erin Saltman is the Senior Director of Membership and Programs at the Global Internet Forum to Counter Terrorism (GIFCT). She has worked in the technology, NGO, and academic sectors, building out international counterterrorism strategies and programs. Dr. Saltman's background and expertise includes analysis of processes of radicalization within a range of regional and socio-political contexts. Her research and publications have focused on the evolving nature of violent extremism online, youth radicalization, and the evaluation of online intervention approaches. Before joining GIFCT she worked for various global NGOs as a counterterrorism and counter-extremism practitioner and was formerly Meta's Head of Counterterrorism and Dangerous Organizations Policy across Europe, the Middle East, and Africa.

Bibliography

(2019, November 7). "Facebook, Microsoft, Twitter and YouTube announce formation of the Global Internet Forum to counter Terrorism". *Meta Blog*. <https://about.fb.com/news/2017/06/global-internet-forum-to-counter-terrorism/>.

(2025, February). *GIFCT Incident Response Working Group Report: A Review of the Content Incident Protocol and Incident Response Framework*. GIFCT Working Groups. https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-IRWG_Report-1.1.pdf.

(2025, February 6). *3D2A: The Second Amendment, 3D Printed Guns and Meme Accelerationism*. GNET Insights. <https://gnet-research.org/2025/02/06/3d2a-the-second-amendment-3d-printed-guns-and-meme-accelerationism/>.

(2019b, November 7). “Update on the Global Internet Forum to Counter Terrorism”. *Meta Blog*. <https://about.fb.com/news/2017/12/update-on-the-global-internet-forum-to-counter-terrorism/>.

Aguilera, A. (2023, July 5). *Drone Use by Violent Extremist Organisations in Africa: The Case of Al-Shabaab*. GNET Insights. <https://gnet-research.org/2023/07/05/drone-use-by-violent-extremist-organisations-in-africa-a-case-study-of-al-shabaab/>.

Argentino, M., Barrett, G. & Tyler, M.B. (2024, January 19). *764: the intersection of terrorism, violent extremism, and child sexual exploitation*. GNET Insights. <https://gnet-research.org/2024/01/19/764-the-intersection-of-terrorism-violent-extremism-and-child-sexual-exploitation/>.

BBC News. (2015, February 3). *Profile: IS-held Jordanian pilot Moaz al-Kasasbeh*. <https://www.bbc.com/news/world-middle-east-31021927>.

Benmelech, E. & Klor, E.F. (2016). “What Explains the Flow of Foreign Fighters to ISIS?”. *NBER Working Paper Series: Working Paper 22190*. National Bureau of Economic Research. <http://www.nber.org/papers/w22190>.

Borgonovo, F., Bolpagni, A., Rizieri Lucini, S. (2024, May 9). *AI-Powered Jihadist News Broadcasts: A New Trend In Pro-IS Propaganda Production?*. GNET Insights. <https://gnet-research.org/2024/05/09/ai-powered-jihadist-news-broadcasts-a-new-trend-in-pro-is-propaganda-production/>.

BSR. (2021). *Human Rights Assessment: Global Internet Forum to Counter Terrorism*. Business for Social Responsibility. https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf.

Chowdhury Fink, N. & Barclay, J. (2013). *Mastering the Narrative: Counterterrorism Strategic Communication and the United Nations*. Center on Global Counterterrorism Cooperation. https://globalcenter.org/wp-content/uploads/Feb2013_CT_StratComm-1.pdf.

Davey, J., Comerfeld, M., Guhl, J., Baldet, W., Colliver, C. (2022). *A Taxonomy for the Classification of Post-Organisational Violent Extremist & Terrorist Content*. ISD Global. <https://www.isdglobal.org/wp-content/uploads/2022/01/A-taxonomy-for-the-classification-of-post-organisational-terrorist-content.pdf>.

Dean, L. 13 (January 2025). *AI or Aryan Ideals? A Thematic Content Analysis of White Supremacist Engagement with Generative AI*. GNET Insights. <https://gnet-research.org/2025/01/13/ai-or-aryan-ideals-a-thematic-content-analysis-of-white-supremacist-engagement-with-generative-ai/>.

Doody, S. & Jensen, M. (2024). *Hash-Sharing Database Review: Challenges and Opportunities*. GIFCT Year 4 Working Groups. <https://gifct.org/wp-content/uploads/2025/02/GIFCT-24WG-1224-HSDR-Challenges-1.1.pdf>.

Dwoskin, E. and Timberg, C. (2019 March 19). “Christchurch mosque shootings: Inside YouTube’s struggles to shut down video – and the humans who outsmarted its systems,” *Washington Post*. <https://www.washingtonpost.com/technology/2019/03/18/inside-youtubes-struggles-shut-down-video-new-zealand-shooting-humans-who-outsmarted-its-systems/>.

Engler, M. (2023). *Considerations of the Impacts of Generative AI on Online Terrorism and Extremism: GIFCT Red Teaming Working Group*. GIFCT Working Groups. <https://gifct.org/wp-content/uploads/2023/09/GIFCT-23WG-0823-GenerativeAI-1.1.pdf>.

European Union Internet Forum. (2025). Migration and Home Affairs. https://home-affairs.ec.europa.eu/networks/european-union-internet-forum_en.

Figueireda, B. A. (January 2024). *The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa*. UNIDIR. https://unidir.org/wp-content/uploads/2024/01/UNIDIR_Use_of_Uncrewed_Aerial_Systems_by_Non_State_Armed_Groups_Africa.pdf.

Fink, N. (2025, March 18). *Insight: The instrumentalization of gendered narratives in the search for legitimacy of terror groups*. GIFCT. <https://gifct.org/2025/03/18/insight-the-instrumentalization-of-gendered-narratives-in-the-search-for-legitimacy-of-terror-groups/>.

Fisher, A., Prucha, N. & Winterbotham, E. (2019). “Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability”. *Global Research Network on Terrorism and Technology: Paper No. 6*. Royal United Services Institute * Human Cognition. https://static.rusi.org/20190716_grntt_paper_06.pdf.

GIFCT (2022). *HSDB Taxonomy*. GIFCT, <https://gifct.org/wp-content/uploads/2022/12/HSDB-Taxonomy-FOR-PUBLICATION-Dec-2022-1.pdf>.

GIFCT (2024, April 17). *Membership* | GIFCT. GIFCT. <https://gifct.org/membership/>.

GIFCT. (2025, April 8). *Multi-Stakeholder Workshop on Countering Tech-Related Terrorism in West Africa*. GIFCT Blog. <https://gifct.org/2025/04/08/multi-stakeholder-workshop-on-countering-tech-related-terrorism-in-west-africa/>.

GIFCT. (2024, April 29). *News: GIFCT and Firjan host LatAm Tech Workshop in Rio de Janeiro*. GIFCT Blog. <https://gifct.org/2024/04/29/latam-tech-workshop/>.

GIFCT. (2024, November 21). *GIFCT Partnership in the Nordic Democracy Forum in Stockholm*. GIFCT Blog. <https://gifct.org/2024/11/21/gifct-partnership-in-the-nordic-democracy-forum-in-stockholm/>.

GIFCT. (2024, August 15). *GIFCT Strategic Plan 2025-2027 adopted*. GIFCT. <https://gifct.org/2024/08/15/gifct-strategic-plan-2025-2027-adopted/>.

GIFCT. (2024, July 16). *GIFCT Hosts 2024 Multistakeholder Forum in Singapore*. GIFCT Blog. <https://gifct.org/2024/07/16/gifct-hosts-2024-multistakeholder-forum-in-singapore/>.

GIFCT (2023, March 6). *What is the hash-sharing database?* | GIFCT. GIFCT. <https://gifct.org/?faqs=what-is-the-hash-sharing-database>.

GIFCT (2023, April 6). *GIFCT's Hash-Sharing Database* | GIFCT. GIFCT. <https://gifct.org/hsdb/>.

GIFCT, Global Internet Forum to Counter Terrorism. (2025, January 21). *Governance* | GIFCT. GIFCT. <https://gifct.org/governance/>.

GIFCT, Global Internet Forum to Counter Terrorism. (2019, March 18). *Industry Cooperation* | GIFCT. GIFCT. <http://gifct.org/2019/03/18/industry-cooperation/>.

GIFCT, Global Internet Forum to Counter Terrorism. (2025b, February 25). *Year Five Working Groups* | GIFCT. GIFCT. <https://gifct.org/year-five-working-groups/>.

GIFCT. (2021, March 11). *Next steps for GIFCT*. GIFCT. <https://gifct.org/2019/09/23/next-steps-for-gifct/>.

GIFCT. (2024b, October 8). *News: GIFCT side events at the 79th UNGA: Emerging Technologies, Counterterrorism Sanctions, and Youth PVE Initiatives*. GIFCT. <https://gifct.org/2024/10/08/news-gifct-side-events-at-the-79th-unga-emerging-technologies-counterterrorism-sanctions-and-youth-pve-initiatives/>.

Global Network on Extremism and Technology | GNET. <https://gnet-research.org/>.

James Foley Foundation. *Home - Foley Foundation*. Foley Foundation. <https://jamesfoleyfoundation.org/#gsc.tab=0>

Microsoft. (2019, May 5). *Joint Statement in Support of Christchurch Call*. Microsoft Blog. <https://msblogs.thesourcemediaassets.com/sites/5/2019/05/Christchurch-Call-and-Nine-Steps.pdf>.

Kowert, R. & Chittick, S. (2025). *Threat Surfaces in Games: Challenges and Best Practices*. GIFCT Year 4 Working Groups. <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-Threat-Surfaces-1.1.pdf>.

Kriner, M. & Ihler, B. (2022, September 12). *Analysing Terrorgram Publications: a new digital Zine*. GNET Insights. <https://gnet-research.org/2022/09/12/analysing-terrorgram-publications-a-new-digital-zine/>.

Lakomy, M. (2023, December 15). *Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities*. GNET Insights. <https://gnet-research.org/2023/12/15/artificial-intelligence-as-a-terrorism-enabler-understanding-the-potential-impact-of-chatbots-and-image-generators-on-online-terrorist-activities/>.

Lamphere-Englund, G. (2025a). *Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces*. GIFCT Year 4 Working Groups. <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-PDR-Surfaces-1.1.pdf>.

Lamphere-Englund, G. (2025b). *2024 Resource List: Violent Extremism, Radicalization, and Gaming*. GIFCT Year 4 Working Groups. <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf>.

Lauren. (2024, December 31). *Mobile App Download Statistics & Usage Statistics*. Buildfire. <https://buildfire.com/app-statistics/>.

Macklin, G. (July 2019). *The Christchurch Attacks: Livestream terror in the viral video age*. Combating Terrorism Center at West Point. Volume 12, Issue 6. <https://ctc.westpoint.edu/christchurch-attacks-livestream-terror-viral-video-age/>.

Moerking, E. (2023, September 27). *Milk Parties and Soyjaks: Understanding the Alt-Right's metapolitical appropriation of milk*. GNET Insights. <https://gnet-research.org/2023/09/27/milk-parties-and-soyjaks-understanding-the-alt-rights-metapolitical-appropriation-of-milk/>.

Nelu, C. (2025, February 24). *Harnessing AI for Online P/CVE efforts: tools, challenges, and ethical considerations*. GNET Insights. <https://gnet-research.org/2025/02/24/harnessing-ai-for-online-p-cve-efforts-tools-challenges-and-ethical-considerations/>.

Saltman, E. & Gilmore, S. (2025). *Artificial Intelligence: Threats, Opportunities, and Policy Frameworks for Countering VNSAs*. GIFCT & Konrad Adenauer Stiftung.

Saltman, E. & Johnson, S. (eds.). (2023). *Playbook on Positive Intervention Strategies Online: GIFCT Blue Team Working Group 2022-2023*. GIFCT Working Groups. <https://gifct.org/wp-content/uploads/2023/11/GIFCT-23WG-1023-Playbook-1.1.pdf>.

Saltman, S. & Winter, C. (2014). *Islamic State: The Changing Face of Modern Jihadism*. Quilliam Foundation.

Thorley, T. (2023). *GIFCT Red Team Working Group: Executive Summary*. GIFCT Working Groups. <https://gifct.org/wp-content/uploads/2023/11/GIFCT-23WG-1023-ExecSummary-1.1.pdf>.

Schurig, S. (2024, November 22). *Terrorgram and youth radicalisation: Understanding Brazil's online extremist landscape*. GNET Insights. <https://gnet-research.org/2024/11/22/terrorgram-and-youth-radicalisation-understanding-brazils-online-extremist-landscape/>.

Sonderby, C. (2019, November 7). *Update on New Zealand*. Meta Blog. <https://about.fb.com/news/2019/03/update-on-new-zealand/>

Tech Coalition | What we do. (2024, January 12). Tech Coalition. <https://www.technologycoalition.org/what-we-do>.

United Nations Security Council Consolidated List | Security Council. (n.d.). <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>.

Verney, A. (2016, December 6). “Partnering to help curb the spread of terrorist content online”. *Google Blog*. <https://blog.google/around-the-globe/google-europe/partnering-help-curb-spread-terrorist-content-online/>.

Wachtel, H. (2024). “Assessing the Utility of the UN’s Terrorism Sanctions Regime 20 Years after 9/11”. *Securing the Future Initiative: Policy Briefs*. The Soufan Center. <https://thesoufancenter.org/wp-content/uploads/2024/12/Assessing-the-Utility-of-the-UNs-Terrorism-Sanctions-Regime-20-Years-after-911.pdf>.

Who We Are - Global Network Initiative. (2024, March 26). Global Network Initiative. <https://globalnetworkinitiative.org/who-we-are/>.

Zeiger, S. & Gyte, J. (2021). “Prevention of Radicalization on Social Media and the Internet”. Chapter 12 in Schmid, A.P. (ed.). *Handbook of Terrorism Prevention and Preparedness*. https://icct.nl/sites/default/files/2023-01/Handbook_Schmid_2020.pdf.