



GIFCT

Global Internet Forum
to Counter Terrorism

Global Internet Forum to Counter Terrorism

Annual and Transparency Report 2023

Published April 2024



Table of Contents

Executive Summary	3
Introduction	5
Letter from Executive Director, Naureen Fink	6
Letter from 2023 Operating Board Chair, Neil Potts	8
Letter from Independent Advisory Committee Chair, Dr. Ghayda Hassan	10
Membership	12
How We Work With Members	13
Mentorship Towards Meeting GIFCT Criteria	14
Advancing Our Mission	15
Prevent	16
Introduction to the Hash-Sharing Database	16
Taxonomy for the Hash-Sharing Database	18
Labels	19
Feedback on Hashes	22
Developments in 2023	22
Law Enforcement Requests	23
Respond	23
Incident Response Framework	23
Levels of Response	25
2023 Activations	26
Hashing and the Incident Response Framework	26
Improvements to Our Readiness in 2023	27
Adapt	28
Events	28
Global Network on Extremism and Technology	29
GIFCT Working Groups	30
Bespoke Knowledge Products Developed and Delivered to Members	33
GIFCT E-Learnings in Partnership With Tech Against Terrorism	33
Human Rights Commitment and Due Diligence	34
2023 Developments	34
2023 Financials	35
Financial Support and Contributions	35
Expenses	36
The Year Ahead	37



Executive Summary

In 2023 we welcomed our **new Executive Director, Naureen Chowdhury Fink**, continued to grow our membership, and adapted to significant new developments in the online threat landscape for terrorism and violent extremism. **Five tech companies became members**, bringing the total number of [GIFCT members](#) to 27. Our members, having met our membership criteria and committed to our mission, work together towards our vision of a world in which the technology sector marshals its collective creativity and capacity to render terrorist and violent extremists ineffective online. We are grateful to Meta, our 2023 Operating Board Chair, for their ongoing support throughout the year and for hosting the Global Summit and several of our events.

Terrorists and violent extremists also made renewed efforts in 2023 to exploit digital platforms and geopolitical conflicts that significantly contributed to new risks and threats. Through our [Incident Response Framework](#) (IRF), GIFCT and our members initiated communications in response to **over 175 terrorist/mass violence events or significant online terrorist or violent extremist developments** to share situational awareness and emerging information to identify attempts of online exploitation on our members' platforms. **GIFCT activated the Content Incident Protocol and Incident levels of the IRF** in 2023 in response to a live-streamed shooting in [Louisville, Kentucky, United States](#), and to the [Hamis attack on October 7](#). These activations enabled swift and collaborative action amongst GIFCT's members to share information and address content relating to these events that violated their platform policies.

To disrupt and prevent the spreading of identified terrorist and violent extremist content online, GIFCT and our members continued to strengthen our leading cross-platform technical tool, GIFCT's [hash-sharing database](#). We grew the number of hashes to approximately **390,000 distinct items of terrorist and violent extremist content in the forms of images, videos, and texts**. GIFCT hosted workshops with members to increase the adoption of labeling and feedback mechanisms, and improved the process and functionality to add new hashes and analyze the composition of the database.

The year saw GIFCT's team work with members and stakeholders, including the Operating Board and the Independent Advisory Committee, to adapt to emerging methods that terrorists and violent extremists use to exploit the internet. Through our research arm, the Global Network on Extremism and Technology (GNET), we offered members and stakeholders **over 150 research Insights, 10 reports, and 12 events**. GIFCT published a [report](#) on borderline content, bespoke member knowledge products, and—by convening its **multi-stakeholder Working Groups**—[handbooks, reports, playbooks, and video explainers](#) on valuable topics related to preventing and countering terrorism and violent extremism. We also convened our members and global community of stakeholders at several events over the course of the year, including our **2023 Global Summit, GIFCT Workshops in Ottawa, Singapore, and Tokyo, and our annual event in New York City during the U.N. General Assembly**.

Our mission is global; no single sector can alone address these threats. As such, GIFCT is proud to work with industry, government, and civil society partners to ensure that our



work is informed by diverse perspectives from around the world. GIFCT remains committed and reaffirms our goal to work collaboratively, transparently, and in a manner that fosters respect for human rights to prevent terrorists and violent extremists from exploiting digital platforms.



Introduction

The [Global Internet Forum to Counter Terrorism](#) (GIFCT) is a 501(c)(3) nonprofit with a staff of counterterrorism and technology experts working with member tech companies and stakeholders in government, industry, academia, and civil society to prevent and disrupt terrorist and violent extremist exploitation of digital platforms.

Established in 2017 to address the exploitation of social media platforms by terrorist organizations such as the Islamic State, GIFCT's founding members saw an even greater need for the tech industry to marshal its collective capacity to render terrorists and violent extremists ineffective online following the 2019 terrorist attacks in Christchurch, New Zealand.

Today, GIFCT operates as an independent nonprofit organization conducting programmatic, technological, and strategic initiatives with our [27 tech company members](#). An Operating Board made up of GIFCT's founding members—Meta (formerly Facebook), Microsoft, X (formerly Twitter), and YouTube—is advised by an [Independent Advisory Committee](#) composed of representatives from civil society, academia, government, and intergovernmental organizations.

GIFCT delivers a unique multi-stakeholder setting to identify and solve the most important and complex global challenges at the intersection of terrorism and technology by bringing together key stakeholders—from industry, government, civil society, and academia—to foster essential collaboration and information-sharing to counter terrorist and violent extremist activity online.

See what GIFCT's leadership has to say about our progress to date and what informs our work in the next section.



Letter from Executive Director, Naureen Fink

As we reflect on the accomplishments of 2023 and set our sights on the opportunities ahead, I am humbled by the warm welcome and support I have received from its remarkable community on assuming the role of Executive Director of GIFCT.

Having dedicated nearly two decades to addressing international counterterrorism issues with various stakeholders, I am deeply inspired by the unique role GIFCT plays at the intersections of technology, terrorism, and counterterrorism. The challenges we face in these domains are complex and ever-evolving, yet they present us with unparalleled opportunities to drive meaningful change in the realms of policy, practice, and innovation.

I am grateful for Dr. Erin Saltman's invaluable contributions as Interim ED and to the entire GIFCT team for their tireless efforts and remarkable progress throughout the year. Their dynamism and dedication have been instrumental in advancing our mission and fostering collaboration across sectors and borders.

One of our proudest achievements has been consistently expanding our membership since our inception, from four at the start to 27 organizations by the end of 2023, reflecting the diverse and dynamic nature of the tech industry. We are pleased to have welcomed Bitchute, Yubo, Twitch, Meta, and Dailymotion as our newest members this past year.

As we continue to grow, it is clear that no single sector or state can tackle the scourge of terrorist and violent extremist content alone. Over 2023, we confronted a range of challenges within the tech ecosystem, from navigating legal frameworks and definitions to adapting to emerging technologies and addressing terrorist acts in the context of armed conflicts. Terrorist and violent extremist content is transnational and cross-platform, and terrorists and violent extremists are opportunistic and evolve their use of technology and resources to advance their goals. It is therefore crucial that our members represent a range of different types of organizations, bringing in critically valuable perspectives and experiences.

Our commitment to a multi-stakeholder approach remains unwavering. The GIFCT team has engaged global leaders, international practitioners, researchers, and experts to ensure that our work and our support to members is informed by a 360-degree understanding of the terrorism threat landscape and its many dimensions.

Our work with the European Union Internet Forum, the Aqaba Process, Raisina Dialogue, Global Security Forum, and the United Nations reflects this. Our work with partners like the Global Network on Extremism & Technology, Tech Against Terrorism, and BSR, and the many experts with whom we work, demonstrates our commitment to connect current and potential GIFCT member companies with knowledge, expertise, and solutions. Through the diligent year-long multidisciplinary gatherings of our 2023 Working Groups, we offered crucial insights and strategies for companies and stakeholders alike.



I am deeply grateful for the trust and support of the Operating Board, and to Meta as our 2023 Operating Board Chair. I am very much looking forward to working with Microsoft as our 2024 Board Chair. Thank you also to the Independent Advisory Committee and Chair Ghayda Hassan, whose advice and feedback are invaluable to informing our work and activities.

Looking ahead to 2024, I am excited for the opportunities that lie ahead. With your continued collaboration and support, I am confident that we will build upon the successes of the past year and continue to drive meaningful progress in our collective efforts to combat terrorism and violent extremism.

Thank you for your dedication to our shared mission.

Warm regards,

Naureen C. Fink
Executive Director



Letter from 2023 Operating Board Chair, Neil Potts

As the 2023 Board Chair of the Global Internet Forum to Counter Terrorism (GIFCT), I reflect on our progress and milestones with a sense of accomplishment. GIFCT has demonstrated its pivotal role in addressing the violent extremist abuse of the internet in a year marked by increased violence, conflict, and extremism. Our collective efforts have yielded numerous achievements, strengthening GIFCT and broadening our impact.

Key Achievements:

- The appointment of our new Executive Director, Naureen Chowdhury Fink, stands out. Her wealth of experience, leadership, strategic thinking, and deep understanding of online terrorism and extremism complexities have driven GIFCT initiatives forward. I am confident that GIFCT will continue to make significant strides under her leadership.
- We have provided robust technical support to smaller platforms, hosted hackathon sessions, and made our content moderation software, Hasher Matcher Actioner, openly available.

Membership:

- In 2023, GIFCT expanded its membership base with five new members from diverse industries, notably the gaming sector. This expansion has enriched our collective expertise and perspective, enabling us to address the evolving landscape of online terrorism and extremism more effectively.

Sustainable Funding:

- A significant milestone this year was the expansion of GIFCT's funding structure. This financial diversity is crucial for the sustainability and effectiveness of the organization, enabling us to scale our efforts and impact.

Technical Support:

- We prioritized understanding our partners' technical needs, hosting a Hackathon with 14 GIFCT member companies to enhance the adoption and utility of our hash-sharing database. These sessions focused on strengthening tech companies' abilities to combat online harms through hash-matching technology.

Global Presence:

- GIFCT's international workshops and Global Summit fostered meaningful dialogue and collaboration, deepening our understanding of the challenges we face.

Looking ahead, we see opportunities for further growth and impact. The use of AI presents a significant challenge and opportunity. GIFCT will continue to explore AI and other technologies to enhance our capabilities. We also plan to expand our member base and encourage the Independent Advisory Committee (IAC) to outline potential extremist threats proactively.

As I hand over the chairmanship to Microsoft, I am confident that GIFCT will continue to



make significant strides in our shared mission. I look forward to our continued collaboration and remain committed to supporting GIFCT in any capacity I can.

In closing, I extend my heartfelt thanks to each of you for your unwavering commitment, partnership, and leadership. Working alongside you has been a privilege, and I am immensely proud of what we have achieved together.

Here's to another year of progress and achievement at GIFCT.

Best regards,

Neil Potts
Vice President of Trust and Safety Policy, Meta



Letter from Independent Advisory Committee Chair, Dr. Ghayda Hassan

The past year has posed a multitude of challenges for GIFCT, the Preventing Violent Extremism/Countering Violent Extremism (PVE/CVE) field, and the broader web technology sector. The ongoing Russia-Ukraine conflict and the tragic Israel-Palestine situation have underscored deficiencies in technological safety systems (such as safety by design, system, and network), as well as the limitations of policies and resources for moderating violent, extremist, and terrorist content online. Against this backdrop, the capacity of the industry to remove terrorist and moderate violent extremist content has been significantly diminished due to widespread layoffs and constraints in trust, safety, and moderation teams.

Moreover, the rapid evolution of technologies like virtual reality, gaming, and AI has blurred the boundaries between reality and fiction, facilitating the dissemination of hate speech, extremist content, deep fakes, and misinformation across social media platforms. If left currently ungoverned and loosely moderated, this unchecked web ecosystem could further erode trust, democratic dialogue, critical thinking abilities, and our shared sense of reality – all critical components of social solidarity and peace.

GIFCT is uniquely positioned to play a pivotal role in this ecosystem as the sole hub where platform members can collaborate on much-needed solutions to mitigate risks and curb the malicious use of internet technologies. The Independent Advisory Committee (IAC) plays a central role in supporting GIFCT's mission by bringing together governments, civil society organizations, and academia to collectively advise on pressing issues and foreseeable challenges. The IAC's main mission is to foster good governance, diversity and expansion, transparency, and best practices, and policy coordination to enable GIFCT to enhance its mission.

To achieve this, GIFCT must focus on three key priorities: expanding its membership and operating board, promoting true global multistakeholderism, and developing efficient tools to empower member platforms in combating online extremism. Moving forward, it is essential for GIFCT to take ownership of its membership onboarding and compliance processes, fostering inclusivity for small, and less resourced and decentralized platforms operating in diverse languages, while upholding strong compliance standards.

GIFCT should strive to emerge as a leader in the terrorism and violent extremism landscape by transcending the limitations of current terrorism designations and devising innovative solutions for borderline content such as violent extremism, dehumanization, and misinformation. While its daily efforts should concentrate on member platform needs, strategic planning should embrace robust multistakeholderism through working groups, its annual conference, and partnerships with key stakeholders.

As the mounting evidence underscores the detrimental impact of hateful and violent content on internet and social media users, GIFCT is uniquely positioned to encourage, support, and engage member platforms to act responsibly toward their users. Expansion and profitability can be compatible with human rights and ethical considerations, and it



is imperative for GIFCT and its members to prioritize user protection and the well-being of vulnerable communities, particularly children and adolescents.

In conclusion, the appointments of Naureen Fink as GIFCT's new Executive Director and Courtney Gregoire as the Chair of the Operating Board signal a promising year of leadership and collaboration. However, for GIFCT to truly emerge as a pioneering force, member platforms must actively engage in sustained collaboration and forward-thinking initiatives.

By collectively addressing the challenges that impact us individually and collectively as a global human community, GIFCT and its members can steer the digital landscape away from a fragmented space which will accelerate the harmful and disruptive functions of their platforms, and towards a safer, less violent, and more inclusive online space. The IAC stands ready to support GIFCT on this journey towards excellence and, most importantly, a more humane future.

A handwritten signature in black ink, appearing to read 'Ghayda Hassan'.

Ghayda Hassan
IAC Chair



Membership

At its inception, GIFCT consisted of four member tech companies. At the end of 2023, [GIFCT members](#) included 27 companies representing a diverse range of platforms. **Five companies** became GIFCT members in 2023—Bitchute, Dailymotion, Meta, Twitch, and Yubo.

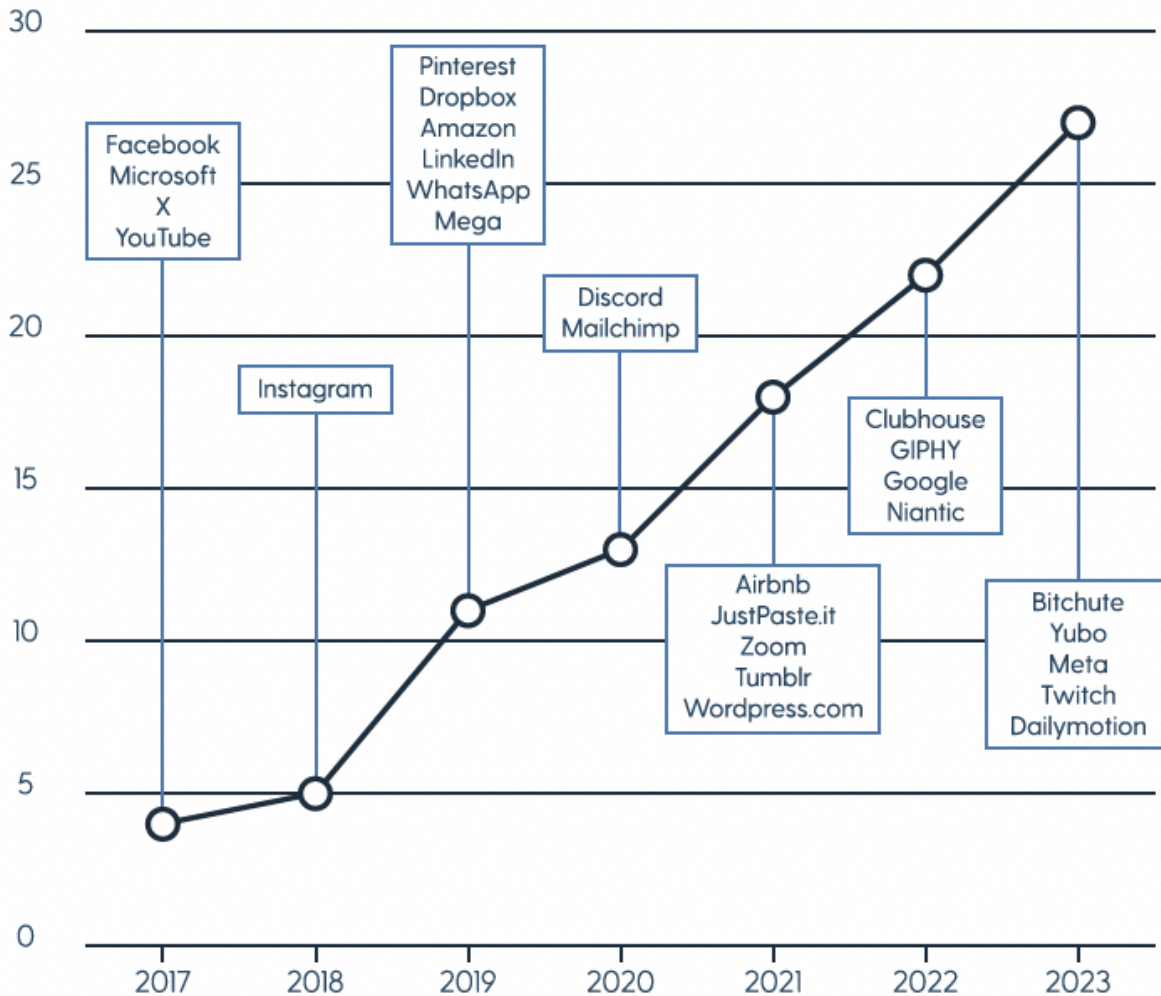
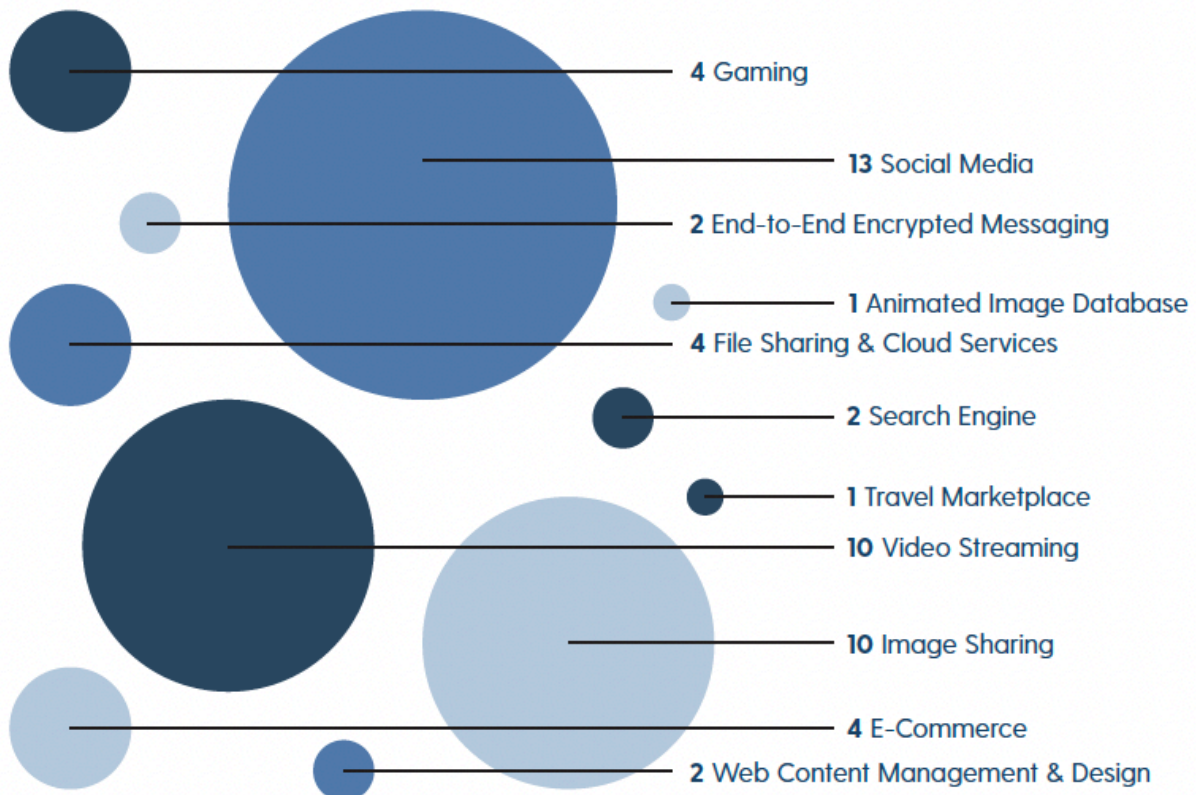


Figure 1: GIFCT members over time

Each member that joins GIFCT brings new technology and expertise to the table, expanding and strengthening our collective capacity. Diversifying GIFCT’s membership also helps GIFCT uphold human rights and ensures a range of voices, global perspectives, and unique challenges are represented, enhancing our collective expertise.

GIFCT members provide different types of services, including:



In 2023, GIFCT expanded its membership base with five new members from diverse industries, notably [1 from] the gaming sector. This expansion has enriched our collective expertise and perspective, enabling us to address the evolving landscape of online terrorism and extremism more effectively.

—Neil Potts, Vice President of Trust and Safety Policy, Meta

How We Work With Members

When tech companies are interested in becoming GIFCT members, they receive mentorship to develop good practices and meet our membership criteria. Once members, companies receive:

- **Cross-platform tech solutions** to detect and prevent the further spread of terrorist and violent extremist content and activities online, including GIFCT's hash-sharing database, tech trials, and other technical innovation programs.
- **Incident response resources and protocols** to strengthen collective responses to the online dimensions of a terrorist or violent extremist attack.
- **Action-oriented research, bespoke tools, and resources** to identify and adapt to the latest trends and emerging developments in online terrorism and violent extremism.
- **Knowledge-sharing opportunities** to work with a global community to scale approaches to online risk mitigation, including events, workshops, and communities of practice.



To achieve its mission, GIFCT continuously convenes and engages with members, individually and collectively, in ad-hoc and scheduled, more formalized meetings and events. Through monthly meetings with GIFCT's full membership, and sometimes with invited expert briefers, we explore the latest developments in tech and the terrorism threat landscape, and facilitate important information-sharing. GIFCT maintains virtual communications systems with its members to quickly and effectively share news about developing offline terrorist and violent extremist events and their online dimensions, enabling robust discussion and situational awareness that strengthens members' collective readiness to deploy technical tooling and activate the [Incident Response Framework](#) when necessary.

GIFCT organizes and hosts virtual and in-person [events and workshops](#) for tech companies and committed stakeholders to share counterterrorism strategies and knowledge specific to a particular world region and impacts to the online threat landscape. GIFCT hosts its [annual conference](#) which formally brings together GIFCT's members, Operating Board, and Independent Advisory Committee, along with key partners and stakeholders, to explore our latest collective advancements and identify the priorities moving forward.

Our partnership strategy is guided by an understanding that terrorism and violent extremism pose direct asymmetric threats to people around the world, which requires an all-of-society approach. GIFCT brings together a community committed to working together to combat the spread of terrorism, violent extremism, and extremist ideologies online. Our ability to partner with other GIFCT members is key to uncovering emerging trends in online extremism and supports our ability to adapt and strengthen our efforts against such threats.

—Collin Barry, Senior Director, Specialized Intelligence Operations, Discord Trust and Safety

Mentorship Towards Meeting GIFCT Criteria

Digital platforms seeking to join GIFCT must meet the following six criteria that allow us to deliver on our mission while maintaining our values:

- Terms of service, community guidelines, or other publicly available policies that explicitly prohibit terrorist and/or violent extremist activity.
- The ability to receive, review, and act on reports of activity that is illegal and/or violates terms of service and user appeals.
- A desire to explore new technical solutions to counter terrorist and violent extremist activity online.
- Regular, public data transparency reports.
- A public commitment to respect human rights in accordance with the United Nations Guiding Principles on Business and Human Rights (UNGPs).
- Support for expanding the capacity of civil society organizations to challenge terrorism and violent extremism.

GIFCT connects companies seeking membership with partners to provide free mentorship towards meeting its membership criteria. In 2023, **seventeen tech**



companies participated in this mentorship process, supported by Tech Against Terrorism and BSR.

Seven new companies applied for GIFCT membership in 2023 and 10 companies continued their work to fulfill GIFCT's membership criteria from 2022.

Among the meaningful efforts from tech companies to join GIFCT and support a safer online ecosystem:

- **Four** companies produced a transparency report for the first time.
- **Six** companies improved their policies prohibiting terrorist and violent extremist activity.
- **Seven** companies improved their platform's tools and operations in order to better enforce their policies and/or terms of service.
- **Seven** companies made a public commitment to respect human rights, in accordance with the UNGPs.

Advancing Our Mission

Providing its members with the tools and resources needed to move the industry forward on how to address terrorist and violent extremist threats online, GIFCT works to:

- PREVENT** **Deliver critical information and technical tools that improve companies' capacity to prevent and disrupt terrorist and violent extremist activity online.** GIFCT develops and enhances cross-platform solutions for coordination and information-sharing that counters terrorists and violent extremists' attempts to exploit technology and digital platforms.
- RESPOND** **Coordinate and strengthen how tech companies respond to terrorist and mass violence incidents and their online dimensions.** GIFCT provides the forum for tech companies to share findings and receive up-to-date information that strengthen their ability to enforce their policies to counter terrorist and violent extremist online activity related to offline violence.
- ADAPT** **Convene industry and cross-sector experts to understand emerging trends relating to technology and terrorist and violent extremist activity so companies can adapt to adversarial evolutions in the online threat landscape.** GIFCT provides members with action-oriented knowledge products and risk mitigation strategies informed by engaging cross-sector practitioners and experts on countering and preventing terrorism and violent extremism.

In every aspect of this work, GIFCT aims to be transparent, inclusive, and respectful of the fundamental and universal human rights that terrorists and violent extremists seek to undermine.



Prevent

To disrupt and prevent the sharing and spreading of identified terrorist and violent extremist content online, GIFCT uses a combination of cross-platform technical solutions and information-sharing with its members.

Introduction to the Hash-Sharing Database

The largest cross-platform technical tool GIFCT supports is the [hash-sharing database](#). The database enables sharing of “hashes” (or “digital fingerprints”) of known terrorist and violent extremist content between GIFCT and its member companies based on a strict [taxonomy](#) (or inclusion criteria) agreed upon by GIFCT and member companies. Content found by a member company is “hashed” in its raw form, ensuring there is no link to any source original platform or user data. Hashes appear as a numerical representation of the original content, which means they are extremely difficult to reverse-engineer to recreate the content.

Each company that is part of the hash-sharing database determines its use of and engagement with the database, depending on their own terms of service, how their platform operates, and how they utilize technical and human resources, among other factors. GIFCT is neither a tech company nor a social media platform and does not own or store any source data or personally identifiable information of any users associated with member platforms. GIFCT provides further explanation of how hashes and the hash-sharing database works below and [in an explainer video](#).

Governments, other non-tech organizations, and tech companies that are not GIFCT members do not have access to the hash-sharing database. Access to the hash-sharing database is provided only to GIFCT member companies that have completed our information-sharing agreement, and their use of the database must comply with our [Hash-Sharing Database Code of Conduct](#). When a member adds hashes to the database, the member labels them in line with our taxonomy and labeling system in order to help other members navigate the database.

The addition of hashes does not prompt any direct or automatic action on another member’s platform, such as removing content. Each member can use the hashes provided through the hash-sharing database to identify content on their respective platform that matches known terrorist or violent extremist content. Each member also determines independently what potential action to take with regards to content on their platform that matches a particular hash, in line with their respective policies and terms of service.

Access to GIFCT’s hash-sharing database in 2023 was available to Discord, Dropbox, Facebook, Google, Instagram, JustPaste.it, LinkedIn, Mailchimp, Mega, Meta, Microsoft, Niantic, Pinterest, X, YouTube, Yubo, and Zoom.

GIFCT ensures that not a single member stands alone in the face of terrorism-related challenges in content moderation. Technology tools like the hash-sharing database quickly raise the effectiveness and performance of efforts in fighting with the spread of



dangerous content. Professional support from more experienced members or GIFCT team allows for the design of the best possible solutions that also take human rights into account.

–Mariusz Żurawek, JustPaste.it

Composition of the Hash-Sharing Database

As of the end of 2023, the hash-sharing database contained approximately **2.3 million hashes**, which represents approximately **390,000 unique and distinct items** made up of roughly 290,000 distinct images, 96,000 distinct videos, and 200 distinct texts (see figures 2 and 3 below).

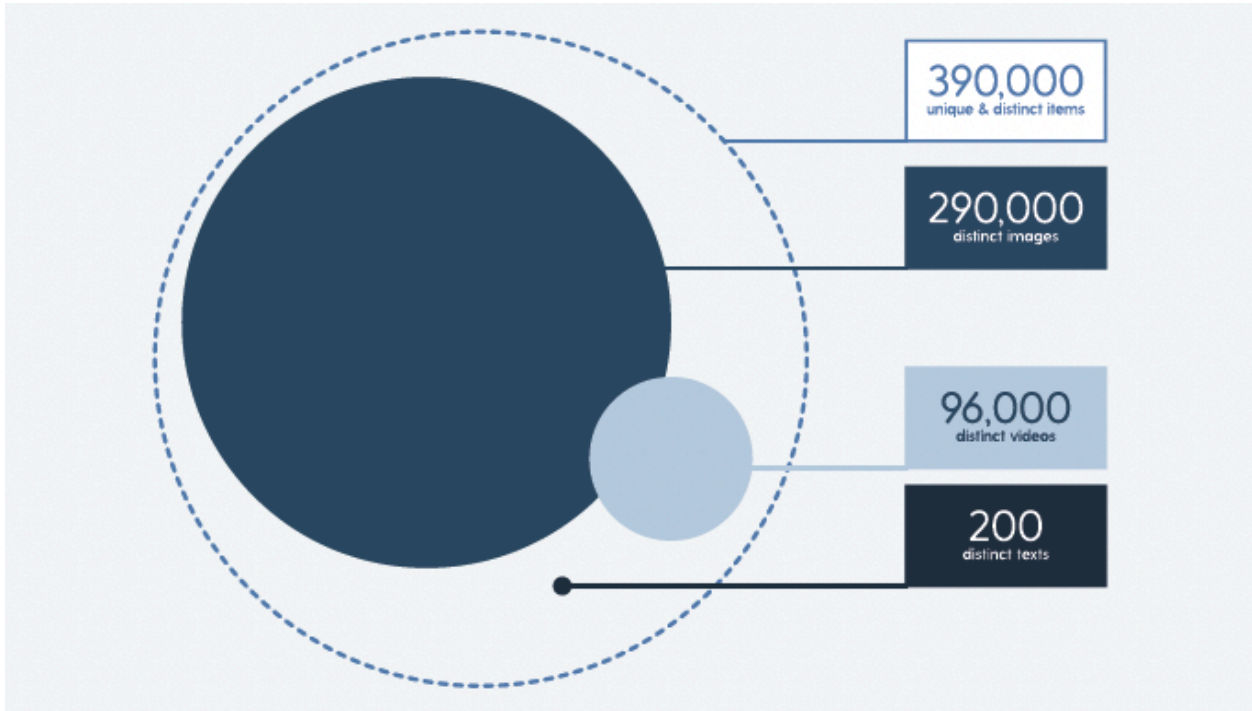


Figure 2: Approximate number of distinct items in the hash-sharing database

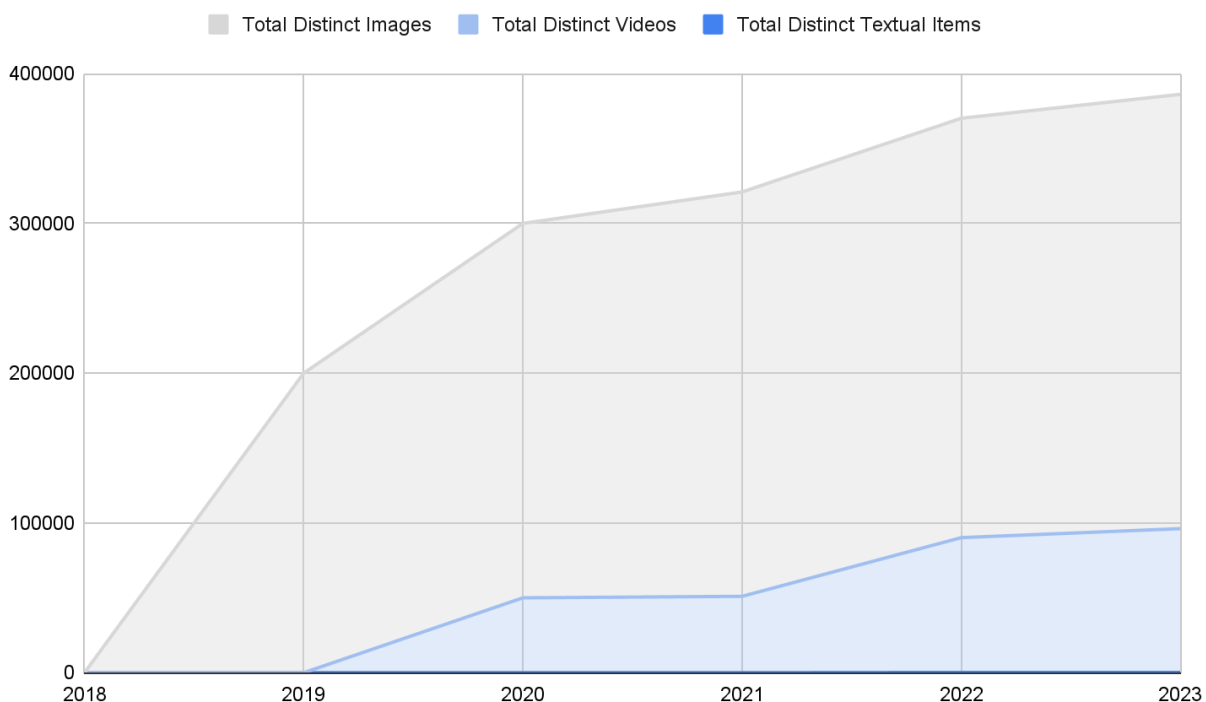


Figure 3 [to be designed]: Approximate number of distinct items in the hash-sharing database
*The number of distinct textual items is not shown because the number is too small (approximately 200 items).

Taxonomy for the Hash-Sharing Database

Tech companies often have slightly different operational definitions of “terrorism” or what constitutes “terrorist content.” These definitions guide them in identifying, reviewing, and taking action on their platforms in line with their policies and terms of service.

[GIFCT's taxonomy](#) is designed to classify terrorist and violent extremist content and activity that individual member company’s policies and terms of service prohibit so that hashes in the database corresponding to this content are useful to members. Hashes added to the hash-sharing database must fit into this taxonomy, which contains parameters for inclusion that take into account:

- the producers of the content being terrorist or violent extremist entities.
- the types of terrorist or violent extremist behavior associated with the content or the offline violence the content depicts or relates to.

GIFCT does not follow a specific government list or maintain its own list of terrorist and violent extremist entities. Instead, in determining whether an entity is a terrorist or violent extremist entity, GIFCT’s taxonomy takes into account the United Nations Security Council’s approach—and in particular, the terrorism sanctions list of designated groups and individuals established associated with Resolution 1267 (1999).



The taxonomy of the database has evolved and expanded over time. The taxonomy originally only included images and videos produced by entities on the United Nations 1267 Consolidated Sanctions List. In 2019, the first expansion was made to include content produced by the perpetrators of an offline attack live-streaming or recording their violence, related to GIFCT’s Incident Response Framework. In response to recommendations made by global experts and tech company members in [GIFCT’s 2021 Taxonomy Report](#), the taxonomy has expanded to include terrorist and violent extremist attacker manifestos and branded publications. In 2021, GIFCT also made it possible to add hashes of URLs and PDFs to the database.

Labels

GIFCT maintains a system to provide more information about the reasons for the inclusion of and the ideology of hashes in the database. Currently, the database operates with the following labels to help categorize and identify hashes corresponding to particular terrorist and violent extremist content:

- **Behavior labels** categorize the hashes by type of terrorist or violent extremist behavior associated with the content.
- **Incident labels** correspond to the offline terrorist or mass violence attack that activated a level of the Incident Response Framework that prompts hashing of identified perpetrator-produced content.
- **Ideology labels** indicate the overarching ideological justification of the hashed content. Content hashed must first meet the inclusion taxonomy and then ideology labels can be applied on a voluntary basis.

Behavioral Labels

At the end of 2023, approximately 85% of the total number of hashes in the database included behavioral labels. Here is the proportion of the four types of behavioral labels in the database:

Behavioral Label	Total percent of hashes with behavioral label
Glorification of Terrorist Acts	62%
Graphic Violence Against Defenseless People	16%
Recruitment and Instruction	6%
Imminent Credible Threat	2%

Table 1: Hash taxonomy behavioral labels distribution

Incident Labels

GIFCT activated levels of the Incident Response Framework that enable hash-sharing for the following seven attacks involving perpetrator-produced content, with the following incident labels:

- **Christchurch, New Zealand:** On March 15, 2019, the need for a separate hash label was declared after an attacker live-streamed his attack on two mosques.



- **Halle, Germany:** On October 9, 2019, the Content Incident Protocol (CIP) was activated after an attacker live-streamed his attack on a synagogue.
- **Glendale, Arizona, United States:** On May 20, 2020, the CIP was activated after an attacker live-streamed his attack on the Westgate Entertainment District.
- **Buffalo, New York, United States:** On May 14, 2022, the CIP was activated after an attacker live-streamed his attack on a supermarket.
- **Udaipur, India:** On June 28, 2022, the Content Incident (CI) was activated after the release of a video by attackers of the killing of an individual.
- **Memphis, Tennessee, United States:** On September 7, 2022, the CIP was activated after an attacker live-streamed his attack on a store as part of a series of attacks throughout Memphis.
- **Louisville, Kentucky, United States:** On April 10, 2023, the CIP was activated after an attacker live-streamed his attack at a bank.

Of the total number of hashes in the database at the end of 2023, approximately 18% included incident labels.

Incident Label	Percent of hashes with incident label
Udaipur, India	9%
Christchurch, New Zealand	4%
Buffalo, New York, U.S.	3%
Halle, Germany	1%
Memphis, Tennessee, U.S.	<1%
Glendale, Arizona, U.S.	<1%
Louisville, Kentucky, U.S.	<1%

Table 2: Hash taxonomy incident label distribution

Ideology Labels

GIFCT increased the adoption and use of ideology labels applied to hashes in the database from less than one percent at the end of 2022 to **seven percent** of the total hashes in the database at the end of 2023.

The list of ideology labels currently available in the hash-sharing database is provided below. GIFCT provides further contextual resources about each ideology within its [Definitions and Principles Framework Project](#).

Accelerationism

Accelerationism is the idea that capitalism and/or liberal democracy (or various processes attached to it) are fundamentally corrupted to a point that complete deconstruction or destruction of the current system should be “accelerated” in order to prompt radical change. Capitalism should be pushed to its worst excesses as soon as possible in order to provoke an



anti-capitalist response. In this basic model, exposing the true evils of late capitalism will inevitably provoke an anti-capitalist revolt.

[Antisemitism](#)

Antisemitism is hate-based violence focused on Jewish populations or targets. This is primarily motivated by conspiracy theories that hold Jewish populations are behind the scenes manipulating society and aiming for global domination.

[Far-Left](#)

This umbrella term refers to political factions or groups with an emphasis on freedom, equality, fraternity, rights, progress, reform and internationalism. None of these notions are of concern in and of themselves but some far-left factions commit targeted violence against those who might limit these values or who hold opposing ideologies. Far-left terrorism tends to be committed with the aim of overthrowing current capitalist systems and replacing them with Marxist-Leninist or socialist societies.

[Far-Right](#)

This umbrella term refers to the more extremist branches of right-wing and hyper “conservative” politics, characterized by an emphasis on notions such as authority, hierarchy, order, duty, tradition, reaction and nationalism. None of these notions are of concern in and of themselves but some far-right factions commit targeted violence based on protected categories (such as race, religion, gender, sexual identity or nationality) or the intolerance of other opposing ideologies.

[Hindutva](#)

The label “Hindutva” is applied to far-right Hindu nationalism and the movements and groups that have grown out of this form of extreme nationalism. Strong nationalist sentiments are not of concern in and of themselves. But there are extreme Hindu fundamentalist factions that have carried out targeted violence in India and the Southeast Asia region, largely against Muslim communities and Islamic targets.

[Incel/Misogyny-Based Violence](#)

Misogyny-based violent extremism includes extreme subsections of the “involuntary celibate” (incel) community and, more broadly, groups in the online “manosphere” where there is overt hate, dehumanization, and violent rhetoric and actions aimed at women (this also contains the music genre of “pornogrind”). Like other forms of violent extremism, incel misogyny targets women as the cause of personal and societal ills and takes particular umbrage with feminism and feminist movements, believing that women should be subservient to men.

[Islamist Extremism](#)

Islamist extremism is an ideology coupling strategic violence with an adherence to an extreme reading of Islamic scripture. This ideology tends to emphasize the military exploits of the Salaf (the early generations of Muslims) to give their violence an even more immediate divine imperative. Groups like al-Qaeda, Daesh/ISIS and Boko Haram adhere to this ideology.

[White Supremacy](#)

White supremacy is a term used to characterize various belief systems central to which are one or more of the following tenets: 1) white individuals and/or populations have a natural, often genetic, dominance over people of other ethnicities, especially where they may co-exist; 2) whites should



live by themselves in a whites-only society; 3) white people have their own "culture" that is superior to other cultures; and 4) white people are genetically superior to other people.

Feedback on Hashes

Members can indicate agreement or disagreement with a hash’s labeling and inclusion in the database. GIFCT and all members with access to the database can see all feedback so that each can consider this additional context when taking enforcement actions on their own platform.

So far, GIFCT has received feedback twice or more¹ on approximately **45,000 hashes, approximately two percent of total hashes** (see Table 3 below for the breakdown on types of feedback received). The majority of hashes with feedback is the result of members agreeing that the hash is labeled correctly and should be included in the database. Those hashes where disagreement exists are mostly a result of members disagreeing on the descriptive labels corresponding to that hash, such as the behavioral label, but agreeing the hash does meet GIFCT’s taxonomy as terrorist or violent extremist content to be included in the database. Where a very small number of hashes contain a feedback label disagreeing that the content corresponding to the hash meets GIFCT’s taxonomy, this disagreement is most often the result of different members’ assessments of whether the content was produced by a terrorist or violent extremist entity.

Among the approximately two percent of total hashes that have received feedback, this feedback can be broken down into the following categories:

Types of Feedback	Percent of hashes with feedback
Positive matches for terrorist and violent extremist content	100%
Positive matches for terrorist and violent extremist content that meets GIFCT’s taxonomy for CI and CIP-related hashes	100%
Disagreement over whether content meets GIFCT’s taxonomy	<0.01%
Disagreement on labeling	5%
Disagreement on labeling CI and CIP-related hashes	None

Table 3: Feedback labels

Developments in 2023

GIFCT continues to enhance cross-platform technical tooling to detect terrorist and violent extremist content in the dynamic online threat landscape through new technical advancements and collaboration with member companies.

¹ All items in the database have one response by definition because in order to add a hash to the database, a member company must assert that the item is within GIFCT’s taxonomy and label it appropriately.



In March 2023, GIFCT [co-hosted a hackathon](#) with 2023 Operating Board Chair, Meta. This hackathon convened 14 GIFCT member companies to support them in increasing adoption of all the resources the hash-sharing database offers, from basic know-how as [the range of terrorist and violent extremist content](#) the database addresses increases, to more advanced tooling to label and provide feedback on hashes. With additional collaborators and partners, including the Tech Coalition, StopNCII, Jigsaw, and Tech Against Terrorism, GIFCT and members sought complementary ways to strengthen tech companies' abilities to use hash-sharing technology to combat a broader range of online harms, including child sexual exploitation and abuse and non-consensual intimate image sharing.

Throughout 2023, GIFCT improved and further developed the infrastructure for the hash-sharing database in order to strengthen the process and functionality to add new hashes and to measure and analyze the composition of the database over time. As a result, GIFCT improved the process for hashing terrorist and violent extremist content in PDF form, advancing efforts to address attacker manifestos and publications created and disseminated to inspire and promote their violent ideologies and activities.

Law Enforcement Requests

Over the last year, GIFCT received no formal requests for data or access to hashed content in the hash-sharing database from a government entity. Questions and requests for specific content or accounts should be directed to member companies since hashes are only numerical representations of source content and cannot be reverse-engineered to recreate the content in question.

Respond

Incident Response Framework

GIFCT's [Incident Response Framework](#) (IRF) is the set of protocols and processes that guide how GIFCT and our members respond quickly, effectively and in a coordinated manner to terrorist and mass violence events with a significant online aspect. GIFCT employs a centralized communications mechanism as part of our incident response efforts with members to share news of ongoing terrorist and mass violence events that might result in the spread of violent content produced by perpetrators. These communications strengthen collective readiness, enabling widespread situational awareness and a more agile response, with better understanding of the event unfolding and how respective platform policies may apply.

In 2023 alone, GIFCT and its members initiated communications in response to **over 175** offline terrorist or mass violence events, or significant online developments in the release and online dissemination of distinct videos, manifestos, or other graphic content by identified terrorist or violent extremist groups.

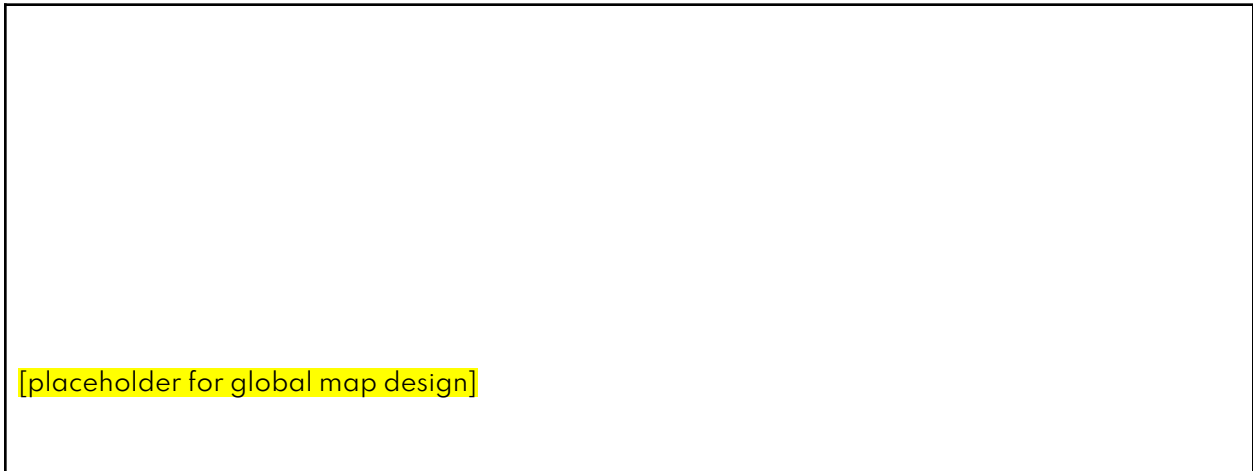


Figure 4: Locations of terrorist/mass violence events or significant online terrorist developments where communications have been initiated with GIFCT members, 2023

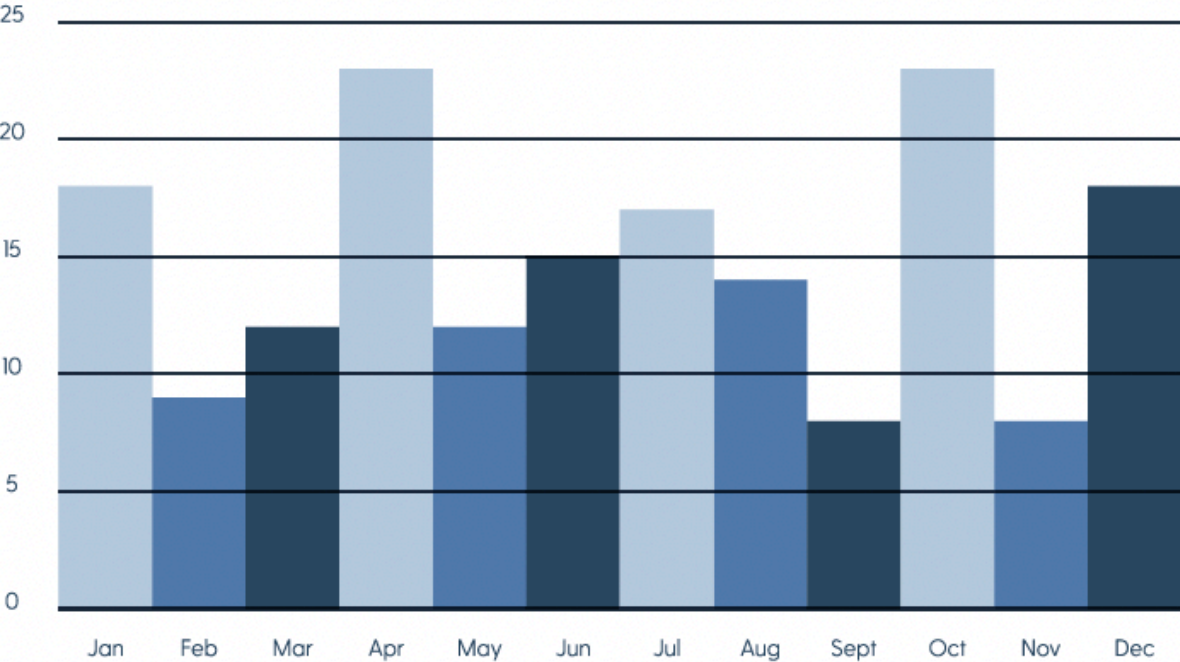


Figure 5: Number of terrorist/mass violence events or significant online terrorist developments where communications have been initiated with GIFCT members, by month, 2023

Since the development of the IRF in 2019 until the end of 2023, GIFCT and its members have shared situational awareness and information in response to **509** terrorist or mass violence events, or significant online terrorist developments unfolding in **59 countries across 6 continents**. There has been a continued increase in the number of initiated communications responses over time (see Figure 6 below), which reflects heightened awareness and stronger response protocols between GIFCT and members, as well as an increase in significant events linked to terrorism and violent extremism where GIFCT’s IRF applies due to significant online dimensions.

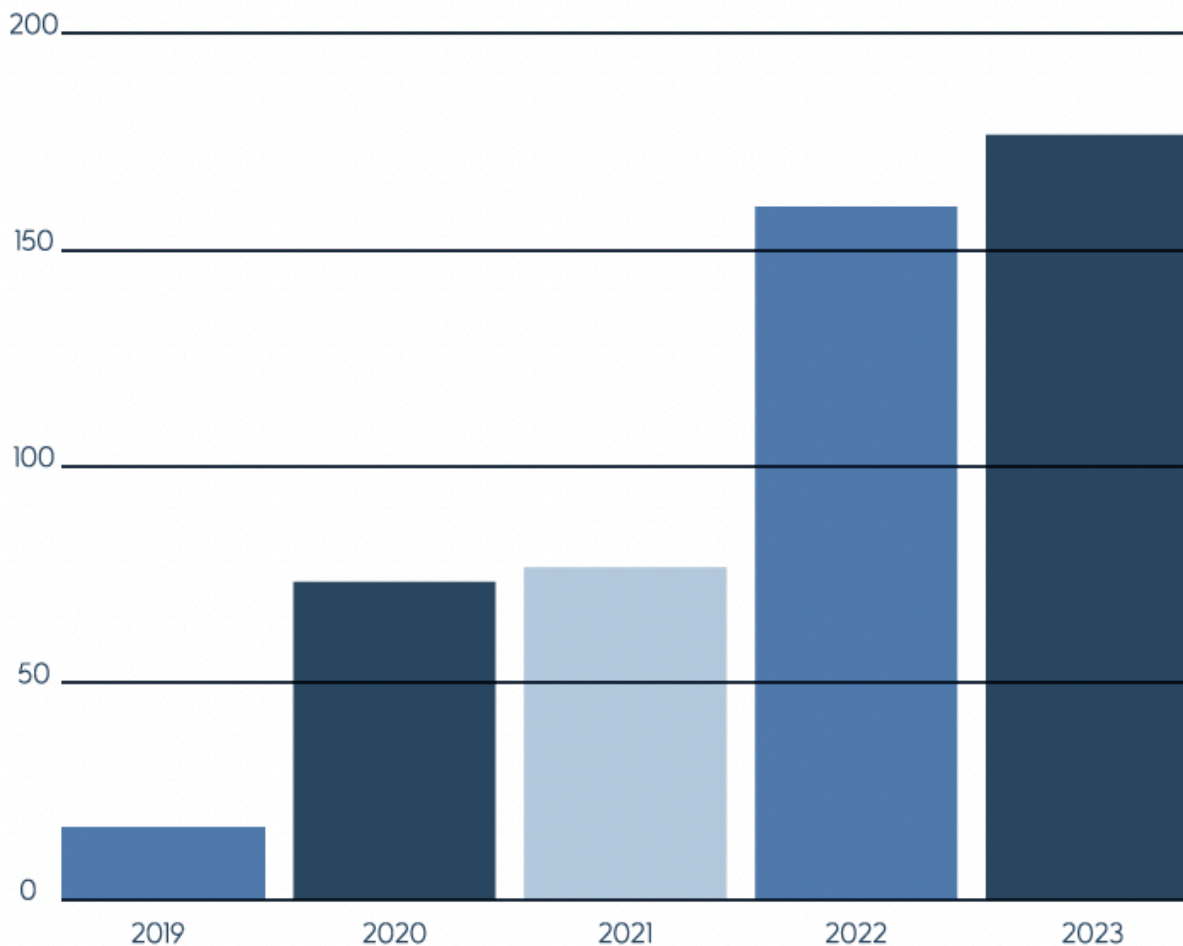


Figure 6: Number of of terrorist/mass violence events or significant online terrorist developments where communications have been initiated with GIFCT members, by year

Levels of Response

GIFCT's IRF contains levels of response that reflect the severity of online exploitation related to the offline terrorist or violent extremist event and the response GIFCT and its members carry out. These levels are Incident, Content Incident (CI), and [Content Incident Protocol](#) (CIP). Activating and distinguishing between these different levels of responses is done to:

- increase the speed at which industry becomes aware of and responds to terrorist and violent extremist content circulating online that relates to an offline terrorist event;
- decrease terrorist and violent extremist content circulating on digital platforms; and
- enhance communications between industry, government, and civil society in response to a terrorist or violent extremist event.



Activating a CIP indicates the heightened threat a situation poses for GIFCT member companies, including potential exploitation of their digital platforms, and GIFCT's urgency to support them in stemming the spread of content associated with the incident.

Since the foundation of GIFCT's IRF in 2019 to the end of 2023, GIFCT has activated these three levels 14 times, representing seven Incident-level activations, one CI-level activation, and six CIP-level activations. More information about how the CIP works is available on [GIFCT's website](#).

2023 Activations

In 2023, GIFCT and its members activated levels of the IRF **twice**. The CIP was activated in response to a shooting in [Louisville, Kentucky, United States](#) live-streamed by the perpetrator. The Incident level of the IRF was activated in response to the attack perpetrated by Hamas on [October 7, 2023](#). While working diligently with members during these activations to detect and address terrorist and violent extremist activity online, GIFCT also maintained communications with government and civil society to understand what other sectors were following and addressing, and how their insights could further inform our continued response.

Hashing and the Incident Response Framework

In cases where either the CI or CIP levels are activated, members can contribute hashes of associated content to the hash-sharing database so that each member can detect and then assess instances of the content shared on their platforms as efficiently as possible. While the CI or CIP activation are concluded when attempts to share the perpetrator-produced content dissipate, allowing GIFCT and members to return to routine information sharing and policy enforcement, new hashes corresponding to new versions of the content continue to be added to the database.

Figure 7 below shows the additions of hashes to the database in 2023, categorized by incident. It illustrates the ongoing adversarial nature of continued attempts to share new versions of perpetrator-produced content and evade detection.

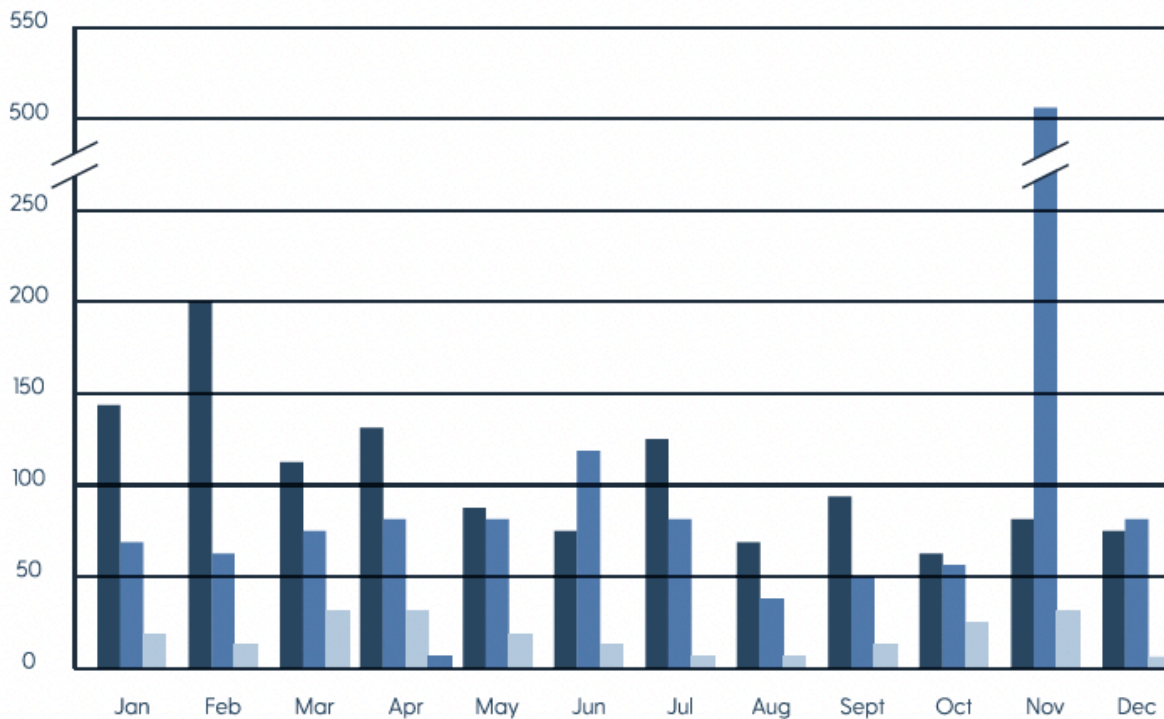


Figure 7: Hashes uploaded per Incident, 2023

[design to be updated and include legend: from left to right, dark blue = Buffalo; gray-blue = Udaipur; light blue = Memphis; fourth bar in April = Louisville]

Improvements to Our Readiness in 2023

In 2023, GIFCT fulfilled a key objective, as stated in our [2022 Transparency Report](#), by implementing Extrac's technical tooling, a robust technical system enabling greater real-time alerts and situational awareness to an emerging mass violent or terrorist incident as it is developing. Greater information about unfolding events ensures a quicker and more effective response to attempts to exploit digital platforms as part of a terrorist or violent extremist incident, minimizing its harmful impacts and potential to inspire further violence.

GIFCT continues to host multi-stakeholder debriefs when the highest level of its framework—the CIP—is activated. This debriefing process ensures that stakeholders are informed of the context and events that prompted the activation of the CIP, as well as the actions carried out as a result. As part of this process, members, as well as civil society and governments, provide feedback on parts of the IRF that are performing well and those areas that are facing challenges, as well as possible solutions to consider.

As a company that prioritizes safety by design at the core of our product and organization, we recognise the Global Internet Forum to Counter Terrorism (GIFCT) as a crucial ally. Their data-driven insights into terrorist and violent extremist trends not only strengthen our safety frameworks but also enhance our proactive measures in addressing contemporary global challenges. Through GIFCT's streamlined onboarding process and in-depth threat intelligence briefings, we are better equipped to fortify our



operational strategies and safety knowledge, enabling a more effective risk mitigation approach. We firmly believe that this collaborative effort is crucial for fostering a safer digital environment for all users.

—Margaux Liquard, Head of Trust and Safety, Yubo

Adapt

GIFCT convenes industry and cross-sector experts to foster deeper understanding among members and stakeholders of emerging trends relating to technology and terrorist and violent extremist activity, and support members in adapting to developments in the online threat landscape.

To support these objectives, GIFCT produces member-only knowledge products and publicly available resources in partnership with global experts. These products advance understanding of the evolution of terrorist and violent extremist activity online, the intersection between online and offline activities, and lessons learned from ongoing counterterrorism and violent extremism work. The following section includes the resources and events GIFCT and its partners produced in 2023.

Events

2023 Global Summit

In June, GIFCT brought together its member companies, Independent Advisory Committee, partner organizations, and stakeholders from industry, academia, civil society, and government for its 2023 Global Summit, hosted by Meta in Menlo Park, California. This meeting focused on improving GIFCT's information sharing and capacity building to better support members in preventing terrorism and violent extremism online. Approximately **100 in-person participants** and hundreds of virtual participants from across the globe attended. GIFCT is grateful to the 2023 Operating Board Chair, Meta, for hosting, and for all those who attended, both virtually and in person. Recordings of the panels are available [on our website](#) and more information about what was covered is on [our blog](#).

United Nations General Assembly Opening, New York City

In September, GIFCT co-hosted with the U.N. Security Council Counter-Terrorism Executive Directorate (CTED) a series of events alongside the formal opening of the U.N. General Assembly to examine the impacts of emerging technology on terrorism and counterterrorism. GIFCT also launched a series of publications and outcomes, products of the year-long multi-stakeholder engagements that took place through the 2023 Working Groups. Read the summary of the day's sessions and watch recordings on [GIFCT's website](#).

GIFCT Regional Workshops

Workshops have been a core part of GIFCT's work since its establishment, serving as critical opportunities to build global partnerships, identify prospective members, and



ensure that GIFCT'S activities are informed and shaped by a range of global perspectives and experiences.

In 2023, GIFCT hosted **three** Workshops located in [Ottawa](#), [Singapore](#), and [Tokyo](#). In addition, GIFCT experts regularly participate in international workshops to foster knowledge exchange and engagement with GIFCT resources, and to identify new members and partners. To date, GIFCT has engaged with more than **155 tech companies, 82 NGOs, and 24 government bodies** through our Workshops across the globe, including in:

- Sydney, Australia
- Brussels, Belgium
- Ottawa, Canada
- Paris, France
- Berlin, Germany
- Accra, Ghana
- New Delhi, India
- Jakarta, Indonesia
- Tel Aviv, Israel
- Amman, Jordan
- Singapore
- Tokyo, Japan
- Abu Dhabi, United Arab Emirates
- London, United Kingdom
- California, United States
- New York, United States

External Events

GIFCT also participated in leading conferences for high-level dialogue on the intersections of technology, terrorism, and counterterrorism. In 2023 these included:

- Paris Peace Forum
- Christchurch Call Leaders' Summit
- Briefings to the U.N. Security Council, the G7, and the U.N.'s CTED Global Research Network and U.N. member states
- Eradicate Hate Summit
- IEEE's Addressing Societal Harms in Digital Platforms Forum
- U.N. Counterterrorism Week
- TrustCon

Global Network on Extremism and Technology

GIFCT's research arm, the Global Network on Extremism and Technology (GNET), provides action-oriented and cutting-edge research on the nexus between technology and extremism.

Funded and supported by GIFCT, led by the International Centre for the Study of Radicalisation, and based at King's College London, GNET brings together an international consortium of leading academic institutions and experts to provide GIFCT members and partners with research and analysis on emerging threats and trends, including ongoing crises and conflicts, and to connect them to a global network of experts and scholars.



GNET Publications and Events

To support GIFCT members and stakeholders, in 2023 GNET commissioned **over 150 Insights**—practical analyses of terrorists and violent extremists’ exploitation of digital platforms—from researchers from around the world.

A selection of the most popular Insights from the **185 contributors in 37 countries** include:

- [How Gnome Hunting Became TikTok’s Latest Antisemitic Dogwhistle](#), by Abbie Richards, Robin O’Lunaigh, and Lea Marchl.
- [Tankies: A Data-driven Understanding of Left-Wing Extremists on Social Media](#) by Utkucan Balci, Michael Sirivianos, and Jeremy Blackburn.
- [Tradwives: The Housewives Commodifying Right-Wing Ideology](#) by Sophia Sykes and Dr. Veronica Hopner.

GNET commissioned an additional **10 reports** in 2023. These were featured in monthly report launch events that brought together the authors, additional experts, and an impressive audience of **over 350 attendees**. The most popular reports include:

- [Cults and Online Violent Extremism](#), by Suzanne Newcombe, Sarah Harvey, Jane Cooper, Ruby Forrester, Jo Banks, and Shanon Shah.
- [The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts](#), by Galen Englund and Jessica White.
- [The “Webification” of Jihadism: Trends in the Use of Online Platforms, Before and After Attacks by Violent Extremists in Nigeria](#), by Folahanmi Aina and John Sunday Ojo.

The third annual **GNET Conference** included a series of panel sessions spread across two days covering some of the most significant topics of its 2023 research, such as protection of researchers’ mental health, developments in gaming and gaming-adjacent platforms, and gendered approaches to studying online violent extremism. In collaboration with the Center for Research on Extremism, GNET also piloted a successful student training workshop in Oslo on how to study online violent extremism.

GIFCT Working Groups

In November 2022, GIFCT launched its Year 3 Working Groups to facilitate dialogue, foster understanding, and produce outputs to directly support our mission of preventing terrorists and violent extremists from exploiting digital platforms across a range of sectors, geographies, and disciplines.

This year’s five thematic Working Groups convened over **200 participants** from 43 countries with approximately 60% drawn from civil society and 20% each from governments and the tech industry. They represented a range of organizations and companies, including:

Category	Affiliation
----------	-------------



<p>Government and Intergovernmental Organizations</p>	<p>Aqaba Process Australian Department of Home Affairs Australian eSafety Commissioner Australian Government (Department of Home Affairs) Australian Home Affairs Australian Parliament Canadian Government Commonwealth Secretariat Council of Europe (Criminal Law and Counter-Terrorism Division) NZ Government (Department of the Prime Minister and Cabinet) European Union Directorate General for Migration and Home Affairs Europol Government of Slovakia (Counter Terrorism Unit)</p>	<p>Iraqi Prime Minister Office Kenyan Police PEReN - French Government Public Safety Canada Romanian Ministry of Internal Affairs Royal Canadian Mounted Police U.K. Government Ofcom U.S. Agency for International Development U.S. Department of Homeland Security (Science & Technology Directorate) U.S. Department of State U.S. House of Representatives UNCTED UNHCR UNODC</p>
<p>Tech Companies</p>	<p>Airbnb Amazon BitChute Checkstep Ltd Clubhouse Discord Dropbox Google JustPaste.it MEGA</p>	<p>Meta Microsoft Niantic TikTok Tremau Twitch Twitter Uber YouTube Zoom</p>
<p>Advocacy Organizations</p>	<p>Anti-Defamation League (ADL) ARTICLE 19 Australian Muslim Advocacy Network Center for Democracy and Technology Digital Grassroots Digital Medusa Dignity in Difference Education Endowment Foundation European Center for Not-for-Profit Law (ECNL) Security and Crisis Centre by EJC Extremely Together</p>	<p>Federation of Islamic Associations of New Zealand (FINAZ) Future of India Foundation Global Network Initiative IKM Advocates Internet Society (ISOC) Internet Society of Nigeria Netsafe Platform for Peace and Humanity Southern Poverty Law Center Take This The Action Coalition on Meaningful Transparency WMM Advocates</p>
<p>Academia</p>	<p>American International University Georgia State University Harvard University International Institute for Counter Terrorism (ICT) Kenyatta University (Center for AI and Digital Policy) Leiden University Northwestern University Ozyegin University</p>	<p>University of California, Berkeley University of California, Los Angeles (UCLA) University of Cape Coast University of Ghana University of Leeds University of Limoges University of Maryland (START) University of Neapolis Pafos-Cyprus University of Paris</p>



	Presbyterian University Ghana Rongo University Royal United Services Institute Sapienza University South Asian University Swansea University The University of Edinburgh University of Auckland	University of Professional Studies Ghana University of South Wales University of Waterloo University of Waterloo Peace Research Institute Frankfurt Victoria University of Wellington
Practitioners and Researchers	Accelerationism Research Consortium (ARC) Africa Peace Building Club Alliance Nationale des Consommateurs et de l'Environnement (ANCE-Togo) Brookings Institute Building Blocks for Peace Foundation Center for Monitoring CIVIPOL Cyber Security Experts Association of Nigeria CyberPeace Institute Digital Industry Group Inc European Forum for Urban Security Extremism and Gaming Research Network (EGRN) Glitterpill Global Center on Cooperative Security Global Network on Extremism and Technology (GNET) GoodBot Helsinki Deaconess Foundation Helsinki Deaconess Foundation Human Digital Institute for Strategic Dialogue (ISD) International Center for Counter-Terrorism (ICCT)	KizBasnia La Convivencia Lafayette Group Love Frankie M&C Saatchi Memetica Moonshot Mythos Labs Online Safety Exchange Organization for Security and Co-operation in Europe (OSCE FoM) Peace Geeks Peace Research Institute Frankfurt Point72 Policy Center for the New South Suli Insights Tech Against Terrorism The Global Disinformation Index The International Centre for the Study of Radicalisation The Peacemaker Corps Foundation Kenya Tiaki Akoako Tony Blaire Institute Wahid Institute Wasafiri Xcyber Group

Table 4: List of Year 3 participant affiliations

At the conclusion of the multi-stakeholder consultations, GIFCT published Year 3 Working Groups' outputs produced by Working Group participants:

- [Refining Incident Response: Building Nuance and Evaluation Frameworks](#), a handbook on how to better measure and evaluate incident response, including considerations around transparency, communication, evaluation metrics, and human rights.
- [Blue Teaming: Alternative Platforms for Positive Intervention](#), a playbook focused on furthering intervention tactics on alternative social media platforms, gaming spaces, online marketplaces, and adversarial platforms.
- Multiple Red Teaming insights assessing new threats and highlighting where safety-by-design efforts should evolve, including [social media](#), [3D printing](#), and [generative AI](#).



- Animated videos on legal frameworks, including the [evolution of the definitions and legal designations](#) of terrorism and violent extremism and their [impact on minority communities](#).
- [Pathways to Meaningful Transparency](#), a report to further the tech industry's commitment to transparency, including the current state of play, barriers and risks, and guidance on how to achieve meaningful transparency.

The multi-stakeholder engagement contributes to improving GIFCT's ability to deliver guidance and solutions to technology companies and practitioners working to counter terrorism and violent extremism. We are grateful to all participants for valuable contributions towards our shared mission.

Bespoke Knowledge Products Developed and Delivered to Members

GIFCT ensures members stay informed on significant threats of terrorist and violent extremist exploitation of digital platforms by delivering assessments, insights, and analysis on specific dynamics of the online threat landscape. GIFCT develops expert analysis and briefings by its in-house experts, publishes research briefs and insights, commissions analysis from GIFCT's network of external experts, and facilitates information-sharing between member companies.

Knowledge products deliver actionable insights and recommendations; some are exclusively for GIFCT members, while others are available to the wider public. This year, in addition to GNET reports, insights, and Working Group publications, GIFCT also produced:

- "[GIFCT Tech Trials: Combining Behavioural Signals to Surface Terrorist and Violent Extremist Content Online](#)," by Dr. Erin Saltman and Tom Thorley, published in *Studies in Conflict and Terrorism*.
- "[Borderline Content: Understanding the Gray Zone](#)," by Dr. Erin Saltman and Micalie Hunt, published as a GIFCT report and with an accompanying [Staff Insight](#), based on their contribution to the European Union Internet Forum's Handbook of Borderline Content in Relation to Violent Extremism.
- "[Advances in Hashing for Counterterrorism](#)," by Tom Thorley, published as a Staff Insight.

GIFCT's resources and community have been extremely valuable to help our team monitor and respond to global incidents and trends.

—Rhett King, Head of Trust & Safety, Clubhouse

GIFCT E-Learnings in Partnership With Tech Against Terrorism

In 2023, GIFCT partnered with Tech Against Terrorism to host five public e-learnings exploring trends in terrorist exploitation of the internet and online counterterrorism responses. Launched in 2021, these e-learnings facilitate knowledge sharing across sectors by bringing together global experts and tech companies to reflect on key topics of interest for our global community.



Over the course of the 2023 e-learnings series, GIFCT and Tech Against Terrorism convened **over 200 participants** from academia, government, civil society, tech, intergovernmental organizations, policy, intelligence, and law enforcement.

Topics included:

- Human Rights and Countering Terrorist Use of the Internet
- Decentralized Platforms and Decentralized Terrorist Financing
- Who has the Right to Data? Access and Barriers to Terrorism Related Data and Data Requests
- Content Moderation Evasion: Tackling Adversarial Shift Online
- 2023 Trends in Terrorist and Violent Extremist Use of the Internet and the Online Counterterrorism Response

Human Rights Commitment and Due Diligence

Promoting and protecting human rights is central to GIFCT's mission to prevent terrorist and violent extremist exploitation of digital platforms. In 2020, its first year operating as an independent organization, GIFCT sought advice from a diverse range of global stakeholders about how best to proactively incorporate human rights considerations in our work. In 2021, GIFCT published a [Human Rights Impact Assessment](#), making transparent a set of guidelines to ground GIFCT's work in the U.N. Guiding Principles on Business and Human Rights. The subsequent [Human Rights Policy](#) adopted by GIFCT notes that, "The participation of both governments and companies in GIFCT means that both the state duty to protect human rights and the corporate responsibility to respect human rights have direct relevance to our work." The assessment continues to be a useful resource that informs GIFCT's ongoing dialogue with current and incoming members, as well as stakeholders in industry, government, and civil society.

2023 Developments

In 2023, GIFCT deepened this commitment to human rights, ensuring that across our work, we engaged a diversity of perspectives and expertise, considered the impacts to fundamental freedoms, and identified ways to strengthen our commitment by broadening it with members. Within the Incident Response Framework, the process that was first developed in 2022 with our [Crisis Response Working Group](#) was implemented to consider potential impacts to human rights when countering and stemming the impacts of our terrorist or mass violence incidence at each stage of response. In the fall, GIFCT and its community of participating experts and practitioners delivered resources exploring human rights impacts from counterterrorism efforts and trust and safety practices across our Working Groups focused on [transparency](#), [incident response](#), and [legal frameworks](#).

In 2023, to support companies seeking GIFCT membership in publicly articulating their commitment to upholding human rights principles in their work, GIFCT partnered with BSR to provide targeted guidance to companies during the mentorship process. Companies joining GIFCT have received feedback either on how to establish their public commitment, or enhance the language and spirit of their existing public commitment. By



centering our respect for fundamental and universal human rights in GIFCT membership criteria, GIFCT ensures that its work to develop technical solutions and resources is grounded in the values of our organization.

We have carried out several rapid human rights assessments of potential new GIFCT members over the past year. This is an important process for ensuring new members meet the human rights criteria for GIFCT membership, as well as a first step in helping new GIFCT members improve their own human rights practices. This all forms an important foundation for helping members take a rights-respecting approach to countering terrorist and violent extremist exploitation, which is critical to GIFCT's mission.






—Lindsey Andersen, Associate Director, Tech and Human Rights, BSR

2023 Financials

Financial Support and Contributions

At the end of 2021, GIFCT introduced a tiered membership donation framework to expand financial contributions beyond its four founding member companies, offering suggested contribution levels based on company revenue. GIFCT is working with the Operating Board on further financial diversification and on implementing agreed principles on fundraising efforts.

In 2023, GIFCT's member contributions totaled **\$3,725,000**.

Tier	GIFCT Members
General (\$1-\$99,999)	  
Cornerstone (\$100,000-\$499,999)	
Principal (\$500,000- \$999,999)	



Visionary (\$1,000,000 or more)	  
---------------------------------	---

Table 5: GIFCT's 2023 GIFCT membership contributions by suggested tier

GIFCT is grateful to our members for their commitment to our mission and their continued support. These contributions allow GIFCT to sustain, grow, and improve the tools and resources we provide our members and partners, and deepen engagement and support with our global multi-stakeholder community.

Expenses

GIFCT 2023 expenses, totalling **\$4,170,000**, break down as follows:

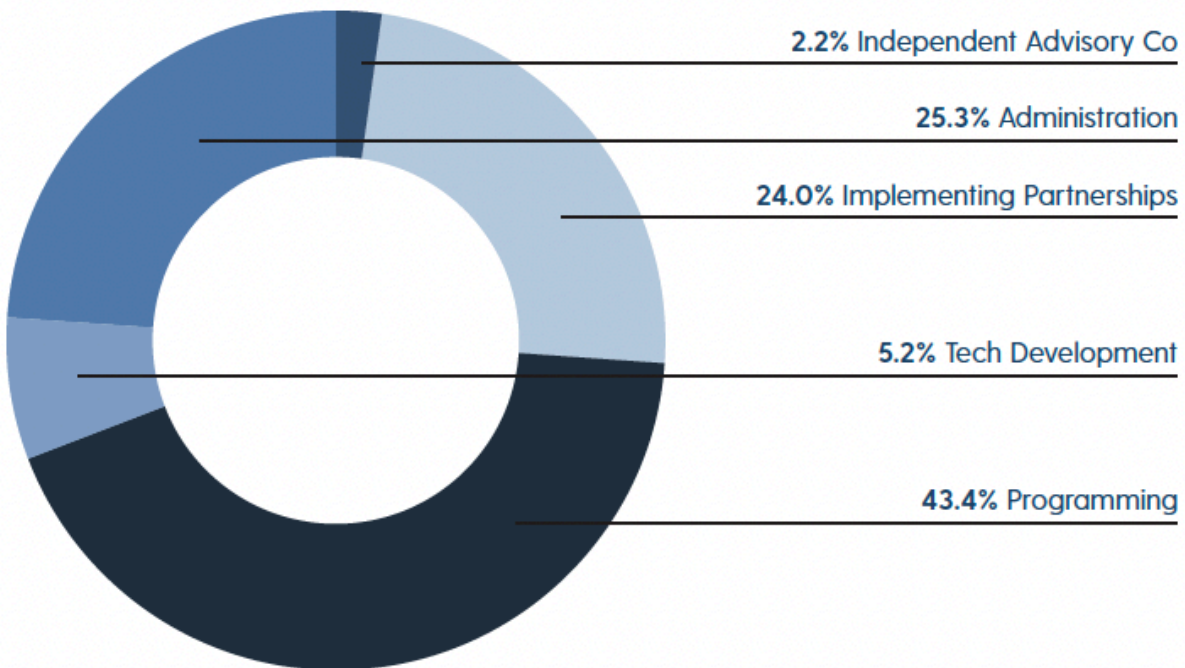


Figure 8: 2023 Total Expenses [design to be updated to include cut-out text]

Category	Total
Independent Advisory Committee	\$90,000
Partnerships	\$1,000,000
Programming	\$1,810,000
Tech Development	\$215,000
Administration	\$1,055,000



Table 6: 2023 expenses by category

While this total for expenses is greater than the total contributions for 2023, GIFCT is not operating at a deficit as a result of investments made by the founding members during the establishment of GIFCT.

The Year Ahead

As we prepare to navigate the complexities of the upcoming year, it will be a crucial period for GIFCT's mission to prevent terrorists and violent extremists from exploiting digital platforms. The projects in 2024 reflect our commitment to working with our global community to address the evolving threat landscape.

- GIFCT will develop its 2025-2027 **Strategic Plan**, which will reflect consultations with our Operating Board, Independent Advisory Committee, and multi-stakeholder network.
- **Supporting our members** remains a primary objective. GIFCT will continue to develop tools, resources, events, and activities that reflect the priorities and needs of our diverse and expanded membership.
- **Diversifying GIFCT membership and fostering international partnerships** are aims that continue to inform GIFCT's activities. GIFCT will engage international partners and seek to broaden its membership to strengthen our collective resilience against emerging terrorist and violent extremist threats.
- As technologies and terrorist and violent extremist tactics evolve, we will continue to **review and refine GIFCT's hash-sharing database**. Among other initiatives, multi-stakeholder efforts to review our inclusion criteria will increase the efficacy of our database and ensure it remains a robust tool to combat terrorism and violent extremism online.
- GIFCT will **review and enhance its Incident Response Framework** to bolster our collective response to online dimensions of terrorist and violent extremist incidents, learning from our partners and stakeholders in government, civil society, academia, and the tech industry.
- By convening the Gaming Community of Practice, GIFCT will **support collaboration and innovation in safeguarding gaming spaces** from exploitation by terrorists and violent extremists, and foster dialogue with diverse stakeholders about the intersections of gaming and terrorist and violent extremist content.
- GIFCT will continue to support members and stakeholders to adapt to emerging technologies, including generative AI. Through research, activities, and convenings that facilitate engagement and innovation, we endeavor to **stay ahead of the curve in safeguarding digital platforms from exploitation**.
- In tandem with our efforts to counter terrorism and violent extremism, GIFCT will **continue to uphold and advance human rights** through our engagements with members and stakeholders, and as a core principle guiding our own work.

In the face of unprecedented challenges, the year ahead encourages us to forge new partnerships, embrace innovation, and reaffirm our commitment to preventing terrorists and violent extremists from exploiting digital platforms. In every aspect of our work,



GIFCT aims to be transparent, inclusive, and respectful of the fundamental and universal human rights that terrorists and violent extremists seek to undermine. We have the power to build a world in which the technology sector marshals its collective creativity and capacity to render terrorists and violent extremists ineffective online.

GIFCT remains critical to combating the exploitation of online spaces by terrorists and violent extremists. As tactics and technologies continue to evolve, GIFCT enables its members to adapt to threats, grow our collective capacity, and leverage safety solutions responsibly, including emerging AI technologies. I look forward to continuing to collaborate with GIFCT, the Independent Advisory Committee, and committed partners in this field to continue working to improve online safety.

—Courtney Gregoire, Chief Digital Safety Officer, Microsoft