GIFCT TRANSPARENCY REPORT 2022

2022 GIFCT Transparency Report

GIFCT
Global Internet Forum
to Counter Terrorism

Table of Contents	Page
Overview	3
GIFCT Members & Mentorship	5
GIFCT Human Rights Impact Assessment	9
GIFCT Working Groups	16
GIFCT Strategic Pillar: Prevent	22
GIFCT Strategic Pillar: Respond	37
GIFCT Strategic Pillar: Learn	44
Conclusion	48

Overview

The mission of the Global Internet Forum to Counter Terrorism (GIFCT) is to prevent terrorists and violent extremists from exploiting digital platforms. GIFCT believes that by working together and sharing technological and operational elements of our individual efforts, GIFCT members can have a greater impact on decreasing the threat of terrorist and violent extremist activity online. This is GIFCT's fourth annual Transparency Report and represents output and metrics from June 1, 2021, through October 31, 2022. This report also reflects the progress made in GIFCT's two and half years as an independent 501(c)(3) non-governmental organization, registered in the United States with an independent Executive Director and staff. More information about the structure of GIFCT and its mission, vision, and values can be found on its website.

It is somewhat unique for a nonprofit organization to release an annual transparency report. However, since GIFCT manages and builds tools that help to facilitate and strengthen tech companies' efforts to counter terrorism and violent extremism, and because we require member companies to produce a transparency report on at least an annual cadence, GIFCT holds itself accountable to the same standard. GIFCT has also worked to highlight member companies' transparency reports in the Member Resources Guide so that they are more easily accessible to the broader community.

At the July 2020 GIFCT Global Summit, inaugural Executive Director Nicholas Rasmussen identified transparency as one of three primary values that guide the organization's work, particularly as it began to develop its infrastructure and operations in the first year as an independent organization. Today, transparency operates as one of three core values that direct GIFCT's work to advance its mission. Reporting of this nature encourages an open and inclusive internet and multi-stakeholder approach.

This year, GIFCT delayed its 2022 Transparency Report by six months to enable a greater investment of time and effort to enhance the transparency of our work, and to align its publication with our Annual Report. GIFCT sees these reports as a meaningful opportunity to identify where greater transparency can offer our cross-sector community the ability to understand our approach, the efforts we take to address the current threat landscape online, and how we are advancing our mission.

Here are key advancements and enhancements we have made to the 2022 Transparency Report within each section:

Members and Mentorship:

- Greater depth and insights from previously available information about GIFCT membership criteria and the mentorship process
- New metrics about the progress tech companies have made as a result of pursuing GIFCT membership and through the Tech Against Terrorism mentorship process with regard to transparency reporting, human rights commitments, and updates on enforcing policies and terms of service prohibiting terrorist and violent extremist activity

- The introduction of GIFCT's membership criteria annual review process led by Tech Against Terrorism to ensure existing GIFCT members continue to fulfill membership criteria

Human Rights Impact Assessment:

- Detailed accounting of GIFCT's progress on the recommendations in the 2021 published Human Rights Impact Assessment (HRIA) of GIFCT. Notable achievements in 2022 include the publication of a human rights policy and the incorporation of human rights questions into multiple outputs from Year 2 Working Groups

Working Groups

- List of organizational affiliations of the participants in Year 3 GIFCT Working Groups, taking place during 2022-2023 (Year 2 Working Group Participant Affiliations were included in the 2021 Annual Report; going forward, this information will be provided in GIFCT's Transparency Report).

Strategic Pillar: Prevent

- Updates on the completed transition of Management and Oversight of the hash-sharing database to GIFCT's team (a legacy from GIFCT's previous formation as a member consortium).
- Enhanced metrics and insights on the latest composition of content corresponding to hashes in GIFCT's hash-sharing database.
- Enhanced information about how members use the hash-sharing database and the processes and procedures to address questions and inaccuracies in the database.
- Delivery of findings from GIFCT's first sampling and review exercise of hashes to ensure quality and reliability of the hash-sharing database for members.

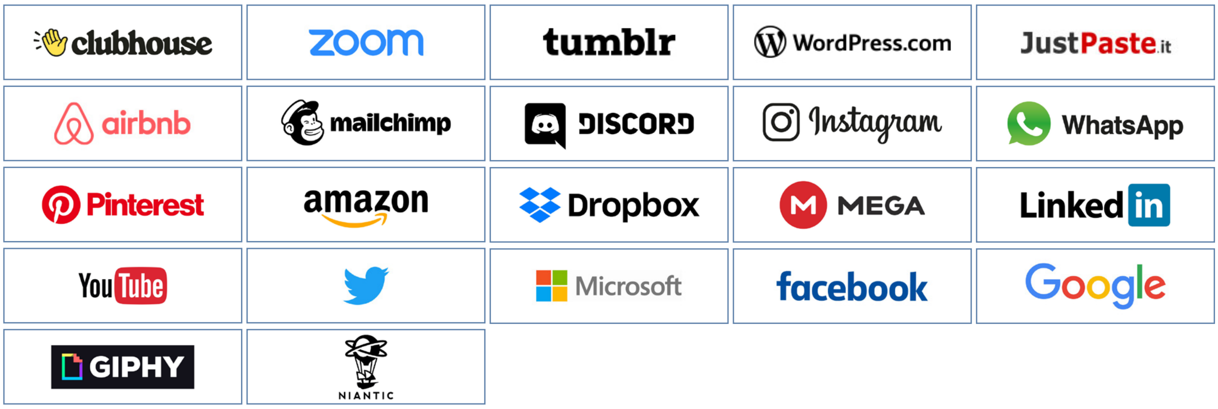
Strategic Pillar: Respond

- Enhanced granular details and results of GIFCT's efforts with and among its members to share situational awareness and information in response to offline violent events in an effort to identify any online dimensions tied to the event.
- Introduction of GIFCT's debriefing process for the Content Incident Protocol (CIP) and initial findings from debriefs that took place in 2022.
- Focused list of areas for further improvements to GIFCT's Incident Response Framework (IRF) in 2023.

GIFCT believes in transparency and the accountability it applies and looks forward to the feedback we gain from our community in response to this report that enables us to further improve in the year to come.

GIFCT Members and Mentorship

There are currently 22 GIFCT Members: Airbnb, Amazon, Clubhouse, Discord, Dropbox, GIPHY, Google, Facebook, Instagram, JustPaste.It, LinkedIn, Mailchimp, MEGA, Microsoft, Niantic, Pinterest, Tumblr, Twitter, WhatsApp, WordPress.com, YouTube, and Zoom.



Tech companies seeking to join GIFCT can apply online and need to fulfill our membership criteria. For tech companies seeking membership, GIFCT provides guidance and connects companies with our partner, Tech Against Terrorism (TAT) whose mentorship program facilitates the development of best practices around transparency in ways that work for the specific platform, and helps the company work towards achieving the GIFCT membership criteria.

Throughout the year, GIFCT engages directly with prospective and existing members to review policy updates, discuss findings and research from our academic network, the Global Network on Extremism and Technology (GNET), and support individual company responses to terrorist and mass violent events. To provide direct, One-on-one support to tech companies pursuing and fulfilling GIFCT's membership criteria, we work with our partner Tech Against Terrorism.

Tech Against Terrorism provides an independent and expert review of tech companies against GIFCT's membership criteria as an initiative launched and supported by the United Nations Counter Terrorism Executive Directorate (UN CTED) working with the global tech industry to tackle terrorist use of the internet while respecting human rights.

GIFCT's Membership Criteria

- 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 both 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

Tech Against Terrorism's Mentorship Program - a service supported by GIFCT - assesses and provides recommendations on a platform's overall transparency efforts and measurement against GIFCT's membership criteria. In a related vein, GIFCT has piloted an extra layer of human rights review with Business for Social Responsibility (BSR) for prospective members to help companies in fulfilling this requirement for membership (see more in the following section regarding our work with BSR).

GIFCT's membership criteria are intended to maintain the integrity of GIFCT while we work toward our mission, promote a culture of multi-stakeholder collaboration, and emphasize the complementary and mutually reinforcing nature of combatting terrorism and violent extremism while ensuring respect for human rights. The criteria are designed to be both meaningful and applicable for the diverse range of technology companies with a role to play in countering terrorism and violent extremism online.

While GIFCT's membership criteria aim to be approachable to tech companies operating a diverse set of digital platforms and online services, the efforts to fulfill the criteria are significant and rigorous such that member companies contribute meaningfully to the health and safety of the online ecosystem. GIFCT membership should be recognized and appreciated as a strong indication of good stewardship for the internet and its users. By fulfilling the membership criteria, tech companies demonstrate their overall dedication to combatting terrorist and violent extremist use of their platforms. As reflected in the criteria, tech companies who are members of GIFCT invest in internal review processes that bring issues around extremist content and use to the forefront of their policies, community guidelines, and terms of service. These companies further explicitly showcase their commitment to those values through public transparency reporting and pledge to respect human rights in accordance with the United Nations Guiding Principles on Business and Human Rights (UNGPs).

The following metrics help to illustrate the significant and rigorous efforts required to join GIFCT and the important work of our partner, Tech Against Terrorism, to mentor companies in fulfilling GIFCT's membership criteria:

Mentorship to Reach Membership:

In 2022, **4** companies achieved GIFCT membership by meeting GIFCT's membership criteria and were approved to join GIFCT. The four following companies are the newest members of GIFCT:

1. Clubhouse
2. GIPHY
3. Niantic
4. Google

Currently, **14** companies are receiving mentoring from Tech Against Terrorism through the established Mentorship Program that GIFCT funds. This includes the companies who applied and began receiving mentorship in 2022 and earlier.

Producing a First Transparency Report:

4 Companies in the Tech Against Terrorism Mentorship Program have produced inaugural transparency reports in an effort to join GIFCT and as a result of Tech Against Terrorism support.

4 Additional companies are currently in the process of producing inaugural transparency reports as they continue in the mentorship program on the path to GIFCT membership.

Enforcement Tactics Improved:

3 Companies currently undergoing mentorship have improved their tools to enforce their community standards and/or terms of service.

Establishing a Human Rights Commitment:

6 Companies have established and publicly articulated their commitment to human rights as a result of pursuing GIFCT membership. 3 of these companies have since become GIFCT members while the other 3 continue in their mentorship processes with Tech Against Terrorism.

Enhanced Human Rights Commitment:

6

Companies who previously had an initial publicly stated human rights commitment have enhanced their commitments as a result of pursuing GIFCT membership. 4 of these companies have since become GIFCT members while the other 2 continue in their mentorship processes with Tech Against Terrorism.

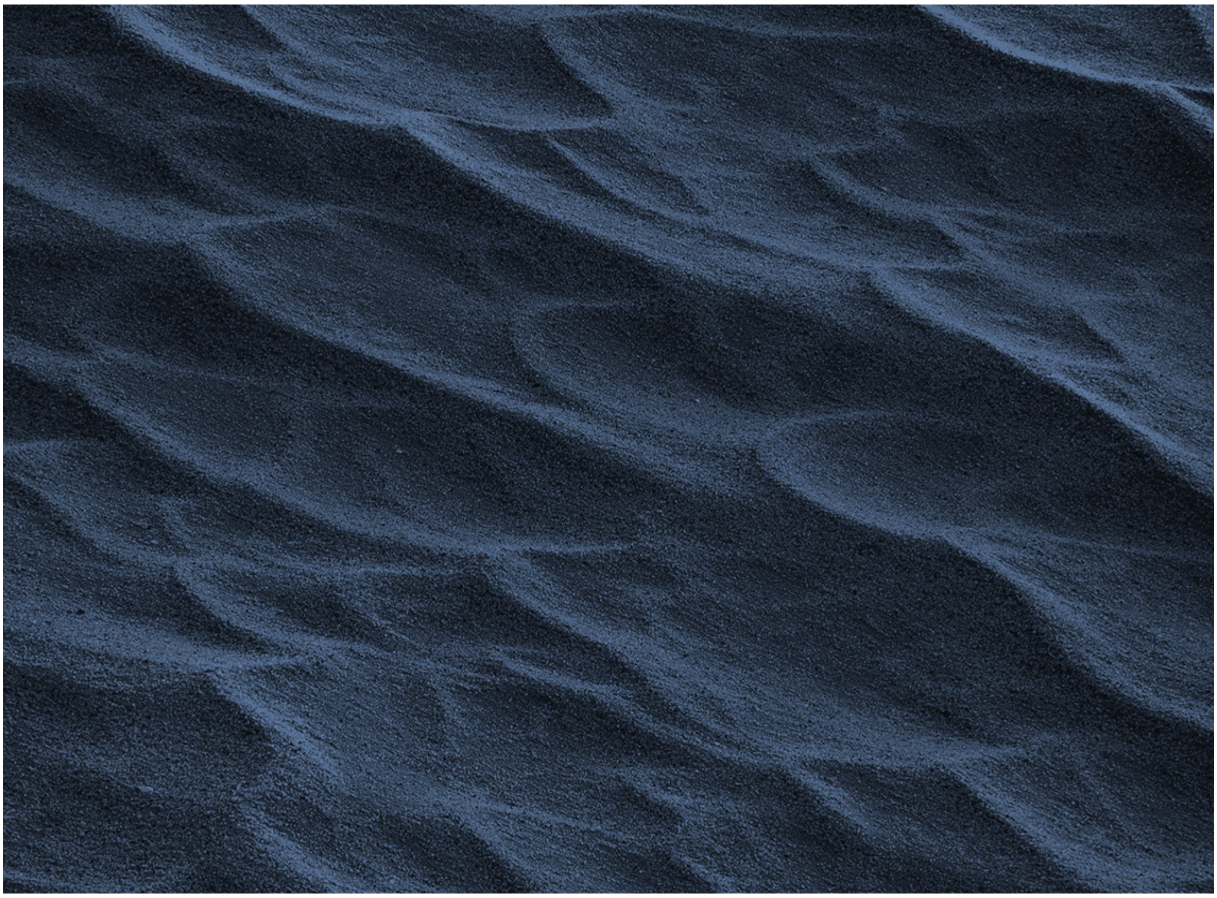
Inaugural Annual Membership Reviews:

In 2022, GIFCT and Tech Against Terrorism introduced a yearly review process of all **18** members who had joined GIFCT by the end of 2021 to ensure members were continuing to uphold and fulfill GIFCT's membership criteria.

Findings from the first review process have now been gathered and GIFCT will provide updates in the coming year, including insights on lessons learned to improve the process in the future.

Platforms that joined GIFCT in 2022 will be included in the annual review process beginning in 2023.

To learn more about GIFCT's partnership with Tech Against Terrorism to mentor and support prospective member companies in their efforts to join GIFCT, see the 2022 Annual Report.



GIFCT Human Rights Impact Assessment

In the Fall of 2020, GIFCT sought advice from a diverse, global range of stakeholders about how best to proactively incorporate human rights considerations in our workstreams. In December 2020, GIFCT commissioned the non-profit Business for Social Responsibility (BSR) to conduct a Human Rights Impact Assessment (HRIA) of GIFCT, which was published in July 2021 making transparent a set of guidelines to ground GIFCT's work based on the UN Guiding Principles on Business and Human Rights. The assessment is designed to be forward-looking and act as a useful tool for organizations and individuals thinking proactively about human rights at the nexus of terrorism and technology.

The HRIA identifies primary human rights potentially impacted by GIFCT's activities: life, liberty, and security of person; nondiscrimination and equality before the law; access to effective remedy; freedom of opinion, thought, conscience, and religion; freedom of expression; freedom of assembly, and association; and privacy. Significantly, the report notes that GIFCT is often one step removed from direct human rights impacts, as these largely result from potential actions taken by GIFCT member companies rather than from GIFCT itself. However, because GIFCT works with cross-platform tools and communications with its members, the HRIA recommended that GIFCT maintain a system of human rights due diligence, embedding human rights across its activities, and engaging with affected stakeholders.

Our transparency report tracks GIFCT progress across the 47 concrete recommendations made in the HRIA. While some of these recommendations are built for development and completion, others are meant to be ongoing and iterative processes for progress.

Statement from BSR on GIFCT's Ongoing Work

BSR appreciated the opportunity to undertake a human rights impact assessment (HRIA) of GIFCT during 2021, and welcomed GIFCT's decision to publish the assessment in full and respond to each of its recommendations. We especially appreciated GIFCT's foresight for undertaking a HRIA at such an early stage in its evolution as an organization, and for committing to human rights due diligence as an ongoing practice, not a one time activity.

BSR provided advice to GIFCT during 2022 on the implementation of various HRIA recommendations, such as assisting in the development of a GIFCT human rights policy, proposing a framework for human rights due diligence, and further refining GIFCT's membership criteria. We've been impressed by GIFCT's quest to understand how to apply the UN Guiding Principles (UNGPs) in a multi-stakeholder setting rather than their more traditional application to companies acting alone, GIFCT's disciplined approach to tracking progress over time, and GIFCT's desire to diversify stakeholder networks. We welcome the integration of human rights into GIFCT's Prevent and Respond strategic pillars and their workstreams.

The UNGPs emphasize continuous learning and improvement over time. Drawing upon themes raised in our HRIA, we emphasize the following priorities for 2023 and beyond:

- Defining and proactively communicating GIFCT's theory of change as it relates to membership growth, especially when presented with the dilemma of the "highest risk" companies also being the companies that will benefit the most from GIFCT membership.
- Clarifying GIFCT's human rights due diligence framework and using it to establish shared awareness among all GIFCT participants about how human rights are embedded into GIFCT's work on an ongoing basis.
- Continuing to emphasize that human rights should be a deeply embedded, complementary, and reinforcing objective in counterterrorism and violent extremism efforts, rather than something that is "added on" after the fact--and conveying this perspective in research, policy debates, and public dialogue.

2022 Progress Tracker Against HRIA Recommendations

Recommendation	Context
Completed in 2022	
Create a Human Rights Policy for GIFCT *Section 4.2, Rec.1 of the Human Rights Impact Assessment of GIFCT*	Through continued collaboration with BSR engagement with civil society, and approval from the Operating Board, GIFCT created a human rights policy to formalize an enduring GIFCT commitment to human rights. Principle 16 of the UNGPs states that "as the basis for embedding their responsibility to respect human rights, business enterprises should express their commitment to meet this responsibility through a statement of policy." This policy is available on GIFCT's website here.
Embed a commitment to human rights into other relevant GIFCT governing documents *Section 4.2, Rec.2 of the Human Rights Impact Assessment of GIFCT*	GIFCT embedded this commitment into the following governing documents: · Working Group Principles, · Incident Response Framework, · Independent Advisory Committee Terms of Reference, · Hash-Sharing Database Code of Conduct

Progress Ongoing	
Create a framework for ongoing human rights due diligence *Section 5.2, Rec.2 of the Human Rights Impact Assessment of GIFCT*	GIFCT will look to publish a due diligence framework in 2023 in line with the Human Rights Policy published in 2022.
Ensure that addressing the full range of GIFCT human rights impacts is embedded into GIFCT's work plan *Section 5.2, Rec.1 of the Human Rights Impact Assessment of GIFCT*	GIFCT has embedded human rights due diligence into its three-year strategic plan and its objectives and key results framework, guiding the direction and progress of the organization from 2022 through 2024, approved by its Operating Board. Examples include: · The inclusion of human rights advocacy networks in 2022-2023 Incident Response and Transparency Working Groups; · Adding pro/con and risk mitigation analyses to the Definitions and Principles Framework project; and · Layering human rights analysis into the lifecycle of an incident through tabletop exercises, GIFCT Working Group outputs, and targeted stakeholder feedback.
Convene multi-stakeholder discussions to advance acceptance and adoption of legal carve-outs for evidentiary content *Section 7.2, Rec.1 of the Human Rights Impact Assessment of GIFCT*	The Legal Frameworks Working Group produced a report on Privacy and Data Protection/Access as a primary output in 2022. Discussions are ongoing and will continue through the vehicle of Year 3 Working Groups (taking place 2022–2023) with the goal of contributing to the development of cross-sector best practices.
Use a GIFCT "common understanding" of terrorist and violent extremist content to determine inclusion in the hash-sharing database in the medium to long term. *Section 7.2, Rec.5 of the Human Rights Impact Assessment of GIFCT*	GIFCT undertook several interrelated initiatives in this regard: · GIFCT has expanded the taxonomy of the hash-sharing database to include behavioral parameters for the inclusion of hashes relating to attacker manifestos and URLs hosting perpetrator-produced content depicting their violent attacks. · In July 2022, GIFCT launched the Definitions and Principles Framework Project, offering tech companies a consolidated resource to compare and contrast definitions of terrorism and violent extremism, including the pros, cons, and risk mitigations around employing government designation lists. · The Legal Frameworks Working Group published a report on the Interoperability of Terrorism Definitions.
Introduce and expand transparency and oversight mechanisms alongside the extension of content in the hash-sharing database. *Section 7.2, Rec.6 of the Human Rights Impact Assessment of GIFCT*	Management and oversight of the hash-sharing database has been successfully transferred from Meta to GIFCT. In addition, in 2022 GIFCT enhanced the transparency of the hash-sharing database with greater and more detailed metrics (see the section of this report on the Strategic Pillar: Prevent).
Establish a multi-stakeholder process to develop metrics on how the hash-sharing database is used. *Section 7.2, Rec.13 of the Human Rights Impact Assessment of GIFCT*	For further consideration with GIFCT's Operating Board and Independent Advisory Committee in 2023.

Develop position statements based on GIFCT's expertise on the rights-based laws, policies, regulations, and strategies needed to more effectively address the exploitation of digital platforms by terrorists and violent extremists. *Section 8.2, Rec.1 of the Human Rights Impact Assessment of GIFCT*	This year, building off of recommendations from the 2021 GIFCT Taxonomy Report, GIFCT developed the Definitions and Principles Framework, a critical resource for tech companies and wider stakeholder community developing definitions of terrorism and violent extremism. The Framework includes: · Risks and risk mitigation approaches in using government designations list; and · A Global Legislative Map, created by the 2022 Legal Frameworks Working Group, mapping emerging and current legislation with a focus on the obligations placed on technology companies. Among the policies the map tracks include metrics of data retention, proactive and reactive requests, and employee and company liability. It also includes proposals and technical papers across 24 countries relating to the moderation of violent extremist and terrorist related content online, highlighting conflicting/competing requirements upon technology companies as well as showcasing extensive and limited regulatory states. Outputs from GIFCT in 2022 adding to wider policy and regulatory dialogues include: · A position paper by GIFCT's Director of Technology and Director of Programming on combining behavioral signals to identify terrorist content online that they presented at the Terrorism and Social Media (TASM) conference at the University of Swansea in June 2022. · 2022 Working Group outputs include human rights-informed positions on issues such as: › Algorithm Evaluation Methods - technical safeguards, oversight, and best-practices needed to ensure safety by design and protection of human rights while member companies carry out tools-based internal operations › Transparency Reporting: Good Practices and Lessons from Global Assessment Frameworks › Human Rights Life Cycle of a Terrorist Incident Online GIFCT also added its voice to key strategic multi-stakeholder events: · UNGA, G7, the EU Internet Forum, Aqaba Process, and Raisina Dialogue convenings.

Proactively express this point of view with relevant governments, policy makers, and regulators. *Section 8.2, Rec.2 of the Human Rights Impact Assessment of GIFCT*	GIFCT presented its expertise and point of view in several forums: · GIFCT's Executive Director, Nicholas Rasmussen, submitted a written statement of proposed testimony to the United States House of Representatives Committee on Homeland Security, providing GIFCT's expertise on the current dynamics of the terrorism and violent extremism threat landscape and the need for multi-stakeholderism in addressing it. · GIFCT, in partnership with Meta, hosted a side-event during the week of September 19–23 in New York City around the UN General Assembly: "The Future of Terrorism & Violent Extremism Online: Threats & Risk Mitigations." · On September 7, GIFCT and Tech Against Terrorism convened their 14th Global Workshop since its founding in 2017. This was the first workshop in Sub Sahara Africa, hosted by the Kofi Annan Foundation in Accra, Ghana, and the Cyber Security Authority working in partnership with Tech Against Terrorism. GIFCT was then recognized at the following: · GIFCT was mentioned by numerous heads of state and tech companies at the Christchurch Call side-event at the 2022 UN General Assembly on 9/20/2022. · GIFCT and its partner Tech Against Terrorism were the only two NGOs mentioned in the UN Counter Terrorism Committee Delhi Declaration, passed on October 29, 2022.
Establish a tiered membership structure for GIFCT. *Section 9.2, Rec.3 of the Human Rights Impact Assessment of GIFCT*	GIFCT announced a membership tiering structure in its 2021 Annual Report, implementing this suggested funding framework for members in 2022.
Establish a process to (1) expel companies not living up to their membership commitments and / or (2) alter a company's membership tier. *Section 9.2, Rec.4 of the Human Rights Impact Assessment of GIFCT*	In July 2022 GIFCT launched an annual, proactive compliance review process for all GIFCT members in partnership with Tech Against Terrorism to prevent backsliding from GIFCT membership criteria. This included a reactive review process to evaluate members if stakeholders flag concerns about a company's commitment to GIFCT membership criteria.
Actively recruit new member companies, especially from non-US locations. *Section 9.2, Rec.5 of the Human Rights Impact Assessment of GIFCT*	GIFCT has worked to recruit a diversified range of member companies. There are a number of non-US companies in the Tech Against Terrorism Mentorship Program that we hope to advance to members in 2023.
Actively recruit new member companies from elsewhere within the technology "stack". *Section 9.2, Rec.6 of the Human Rights Impact Assessment of GIFCT*	GIFCT expanded the diversity of its members by admitting ClubHouse (audio), Niantic (gaming), and GIPHY (short-form media), and Google (search engine online advertising, cloud computing, computer software, quantum computing, e-commerce, artificial intelligence, and consumer electronics). GIFCT further looked to expand membership to parent companies that house a wide variety of platforms. Google joining GIFCT speaks to this effort.

Provide technical assistance to smaller companies to address human rights risks. *Section 9.2, Rec.7 of the Human Rights Impact Assessment of GIFCT*	GIFCT continued to partner with Tech Against Terrorism and their mentorship program, designed to support smaller companies with improving their content standards, human rights compliance, transparency, and content moderation in line with GIFCT's Membership Criteria. The Tech Against Terrorism Mentorship Program and ongoing work from GIFCT to members has contributed to: · four companies producing their first transparency report; · three companies improving tools for enforcement and terms of service; · six companies increasing inaugural commitments to human rights; and · six companies enhancing public-facing commitment to human rights.
Establish and maintain closer relationships with the United Nations system. *Section 10.2, Rec.2 of the Human Rights Impact Assessment of GIFCT*	GIFCT participated in a series of significant convenings led by the United Nations this year including: · GIFCT participated as a guest of UN CTED in Delhi at the Special Meeting of the Counter-Terrorism Committee of the United Nations Security Council on "countering the use of new and emerging technologies for terrorist purposes" where the Delhi Declaration was passed. Specifically, the Declaration "takes note of the industry-led Global Internet Forum to Counter Terrorism (GIFCT) initiatives; and reiterates its call for GIFCT to continue to increase engagement with governments and technology companies globally." · Presented at the Open Meeting of the United Nations Security Council's Counter Terrorism Committee on "Countering terrorist narratives and preventing the use of the Internet for terrorist purposes" · Moderated and guided the discussion by the United Nations Office of Counterterrorism on Safeguarding the Metaverse, Exploring Opportunities for CT/PCVE in the Metaverse · In partnership with Meta, GIFCT hosted a side-event during the week of September 19 - 23 in New York City around the UN General Assembly: "The Future of Terrorism & Violent Extremism Online: Threats & Risk Mitigations." Speakers included representatives from GIFCT, Meta, the United Nations Counter Terrorism Executive Directorate (UNCTED) and the Accelerationism Research Consortium (ARC). The panel's discussion intentionally incorporated the perspective of UN CTED and wider UN bodies in the role international governing bodies play in preventing terrorist use of the internet and the critical need to understand how tech companies and NGOs can best work with UN infrastructure, with UN representatives attending the conversation and providing audience input.
Train GIFCT participants in principles of good stakeholder engagement. *Section 10.2, Rec.3 of the Human Rights Impact Assessment of GIFCT*	GIFCT created Working Group Principles and the Hash-Sharing Database Code of Conduct to guide both internal and external multi-stakeholder workstreams.

Consider geographic diversity when rotating government membership of the Independent Avdisory Committee (IAC). *Section 10.2, Rec.4 of the Human Rights Impact Assessment of GIFCT*	While this rotation has yet to happen, the IAC is building this consideration into plans for transitioning government membership in 2023.
Institute a system of formal recommendations from the IAC to the Operating Board, and formal responses from the Operating Board to the IAC. *Section 11.2, Rec.1 of the Human Rights Impact Assessment of GIFCT*	The IAC produced its first formal recommendations to the Board and GIFCT about advice on GIFCT Working Groups in September 2020.
Publish summaries of minutes of Operating Board and IAC meetings. *Section 11.2, Rec.3 of the Human Rights Impact Assessment of GIFCT*	Minutes are now formally shared between the Operating Board, GIFCT and IAC.
Task the IAC with publishing an annual statement about the performance of GIFCT. *Section 11.2, Rec.2 of the Human Rights Impact Assessment of GIFCT*	The IAC has embraced this task and will begin submitting to the Operating Board a statement about the performance of GIFCT in 2023.
Create a diversity, equity, and inclusion ambition for (1) GIFCT staff and (2) GIFCT participants. *Section 12.2, Rec.1 of the Human Rights Impact Assessment of GIFCT*	GIFCT became a registered Cap Exempt organization within the United States to be able to sponsor H1-B visas, bringing in two new international employees through this channel. In addition, to ensure an increasingly diverse expert perspective contributing to outputs and impact: · Year 2 Working Groups (2021–2022) had 175 participants from 35 countries; and · Year 3 Working Groups (2022–2023) have 207 participants from 43 countries.
Continue enhancing GIFCT staff support for the IAC and Working Groups. *Section 12.2, Rec.3 of the Human Rights Impact Assessment of GIFCT*	GIFCT supported the IAC and Working Groups on a variety of topics: · To enhance support to the IAC, GIFCT worked with the Operating Board to transition the IAC chair role from a volunteer to a compensated role. · GIFCT supported the IAC in creating an inaugural vice chair role and a compensated Secretariat. · GIFCT enhanced support to Year 3 Working Groups (2022–2023) by ensuring GIFCT staff provide leadership of the five entities (based on detailed IAC feedback).

GIFCT Working Groups

Since GIFCT's July 2021 Transparency Report, GIFCT launched and successfully concluded the second year of GIFCT Working Groups, which convened global stakeholders on the challenges at the nexus of technology and terrorist and violent extremist activity. GIFCT then launched Year 3 GIFCT Working Groups this fall that are currently ongoing.

Year 2 GIFCT Working Groups: 2021-2022

In 2021-2022, Year 2 GIFCT Working Groups convened 178 experts and practitioners from across the world, holding more than 60 meetings with representatives from 19 tech companies, 36 governments and international governing bodies, 60 civil society organizations, and 25 research and academic institutions.

Year 2 Working Group outputs were presented at GIFCT's 2022 Global Summit and output from each Working Group can be found on GIFCT's website. Working Group themes and their output are listed below:

Crisis Response Working Group

The GIFCT Working Group on Crisis Response (CRWG) fed directly into improving and refining GIFCT's IRF as well as posing broader questions about the role of law enforcement, tech companies, and wider civil society groups during and in the aftermath of a terrorist or violent extremist attack. CRWG produced three outputs:

1. The largest of the three was an immersive virtual series of *Crisis Response Tabletop Exercises*, hosted by GIFCT's Director of Technology, Tom Thorley. The aim of the tabletop exercises was to build on previous Europol and Christchurch Call-led Crisis Response events, with a focus on human rights, internal communications, and external strategic communications in and around crisis scenarios. To share lessons learned and areas for improvement and refinement, a summary of these cross-sector immersive events is included in the 2022 collection of Working Group papers.
2. The second output from the CRWG was a paper on the *Human Rights Lifecycle of a Terrorist Incident*, led by Dr. Farzaneh Badii (Digital Medusa). This paper discusses how best GIFCT and relevant stakeholders can apply human rights indicators and parameters to crisis response work based on the 2021 GIFCT HRIA and UN frameworks. To help practitioners integrate a human rights approach, the output highlights which and whose human rights are impacted during a terrorist incident and the ramifications involved.
3. The final CRWG output was on *Crisis Response Protocols: Mapping & Gap Analysis*, led by the New Zealand government in coordination with the wider Christchurch Call to Action. The paper maps crisis response protocols of GIFCT and partnered governments and outlines the role of tech companies and civil society within those protocols. Overall, the output identifies and analyzes the gaps within protocols and points of overlap among them, and provides a set of recommendations for moving forward.

Positive Interventions and Strategic Communications Working Group

The Positive Interventions and Strategic Communications Working Group (PIWG) focused on further outlining processes, practices, and challenges of designing, delivering, and measuring positive interventions online within countering violent extremism and counter terrorism operational contexts. PIWG developed two outputs:

1. The first was a paper led by Munir Zamir (University of South Wales) on *Active Strategic Communications: Measuring Impact and Audience Engagement*. This analysis highlights tactics and methodologies for turning passive content consumption of campaigns into active engagement online. The analysis tracks a variety of methodologies for yielding more impact-focused measurement and evaluation.
2. The second was also a paper, led by Kesa White (Polarization and Extremism Research and Innovation Lab PERIL), Jacob Davey (Institute for Strategic Dialogue), and Galen Lamphere-Englund (Love Frankie Agency), entitled *Good Practices, Tools, and Safety Measures for Researchers*. The paper discusses approaches and safeguarding mechanisms to ensure best practices online for online researchers and activists in the counter-terrorism and counter-extremism sector. Recognizing that researchers and practitioners often put themselves or their target audiences at risk, the paper discusses do-no-harm principles and online tools for safety-by-design methodologies within personal, research, and practitioner online habits.

Technical Approaches Working Group

Responding to an increase in public discourse about the relationship between algorithms and violent extremism, the Technical Approaches Working Group (TAWG) considered questions at the nexus of these two phenomena. The Working Group considered technical solutions to prevent and/or mitigate unintended consequences of algorithms and AI, how tooling and tactics can be implemented for smaller platforms, and what technical safeguards, oversight, and best practices are needed to ensure safety by design and protection of human rights while member companies carry out tools-based internal operations. TAWG developed two outputs:

1. Building on a Year 1 Working Group output that identified the types of algorithms that pose major concerns to the countering violent extremism and counter terrorism sector, GIFCT's Director of Technology Tom Thorley in collaboration with Emma Llanso (Center for Democracy and Technology) and Dr. Chris Meserole (Brookings Institution) produced a longer report in Year 2, *Methodologies to Evaluate Content Sharing Algorithms & Processes*. It explores research questions at the intersection of algorithms, users, and terrorist and violent extremist content, the feasibility of various methodologies, and the challenges and debates facing research in this area.
2. To further this technical work into Year 3, TAWG has worked with GIFCT to release two Research Calls for Proposals funded by GIFCT. These calls for proposals are on *Machine Translation* and *Multimedia Content Classifiers*. Specifically, they will allow third parties to develop tooling based on the gap analysis from last year's TAWG gap analysis and design a system that will classify content in a contextualized and explainable manner.

Transparency Working Group

The Transparency Working Group (TWG) produced two outputs to guide and evolve the conversation about transparency in relation to practitioners, governments, and tech companies:

1. The first output, led by Dr. Joe Whittaker (Swansea University), focused on researcher transparency in analyzing algorithmic systems. The paper *Recommendation Algorithms and Extremist Content: A Review of Empirical Evidence* reviews how researchers have attempted to analyze content-sharing algorithms and indicates suggested best practices for researchers in terms of framing, methodologies, and transparency. It also contains recommendations for sustainable and replicable research.
2. The second output, led by Dr. Courtney Radsch (Center for Media, Data and Society) reports on *Transparency Reporting: Good Practices and Lessons from Global Assessment Frameworks*. The paper highlights the need for broader framing for questions around transparency reporting, the needs of various sectors for transparency, and questions around what meaningful transparency looks like.

The Legal Frameworks Working Group

The Legal Frameworks Working Group (LFWG) produced three complementary outputs mapping current global legislation:

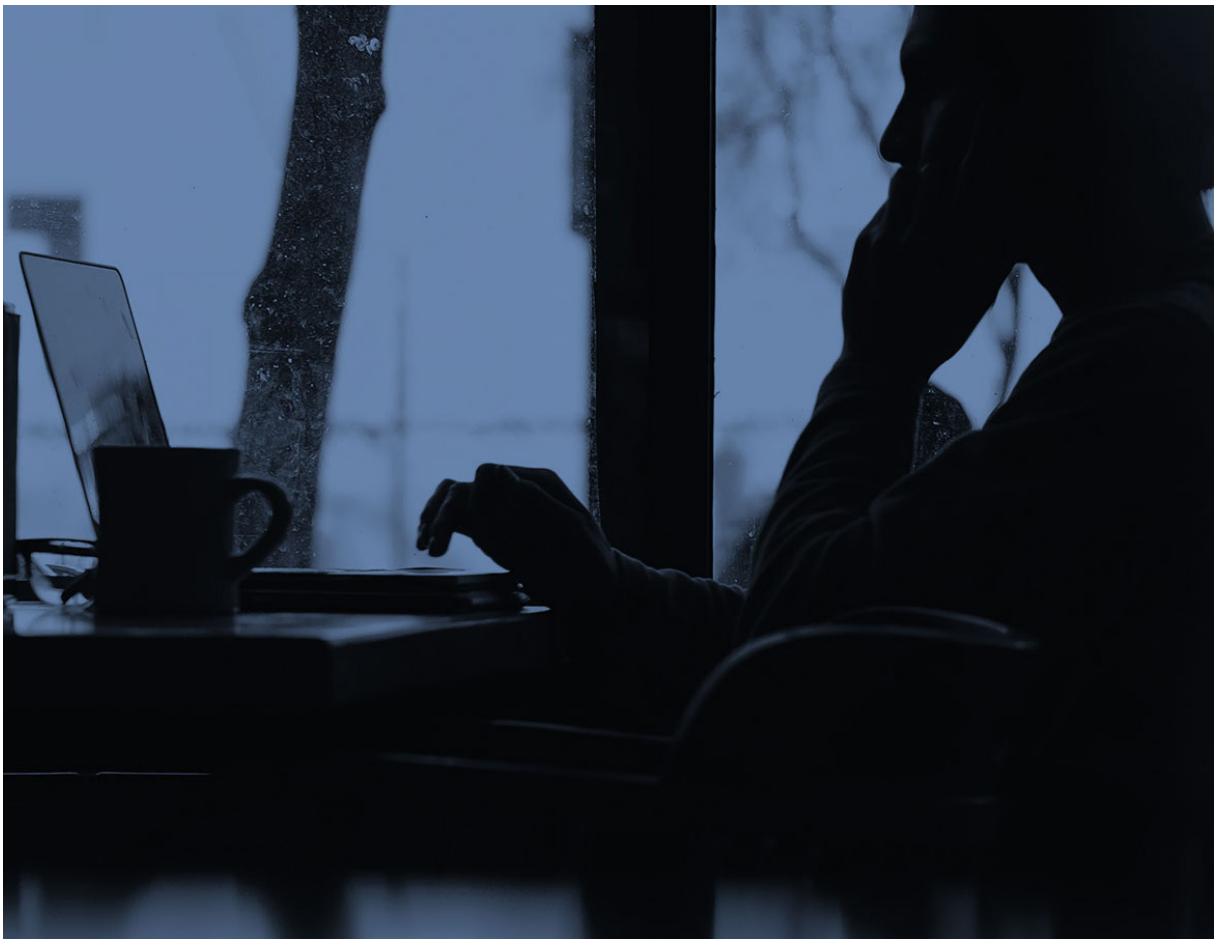
1. The first LFWG output, led by Dia Kayyali (Mnemonic), was about *Privacy and Data Protection/Access* This White Paper reviews the implications and applications of the EU's Digital Services Act (DSA) and the General Data Protection Regulation (GDPR). This includes case studies on Yemen and Ukraine, a data taxonomy, and legal research on the Stored Communications Act.
2. The second LFWG output focused on terrorist definitions and compliments GIFCT's wider Definitional Frameworks and Principles work. This output, led by Dr. Katy Vaughan (Swansea University), was on *The Interoperability of Terrorism Definitions*. The paper focuses on the interoperability, consistency, and coherence of terrorism definitions across a number of countries, international organizations, and tech platforms. Notably, it highlights legal issues around defining terrorism based largely on government lists and how they are applied online.
3. The final output, led by Vanessa Christophers, was a Legislative Map, created to better understand and follow the rapidly evolving legislations impacting how tech companies enforce their content policies across the globe. This tool maps emerging and current legislation (including proposals and technical papers) relating to the moderation of violent extremist and terrorist related content online, with a focus on the obligations placed on technology companies. The tool explores proposals and legislation in 24 countries (focusing on those countries that impact internet companies the most in their ability to counter terrorism and violent extremism).

Research on Algorithmic Amplification

Finally, due to the increased concern from governments and human rights networks about the potential links between algorithmic amplification and violent extremist radicalization, GIFCT commissioned Dr. Jazz Rowa to sit across three of GIFCT's Working Groups to develop an extensive paper providing an analytical framework through the lens of human security to better understand the relationship between algorithms and processes of radicalization. Dr. Rowa participated in the Transparency, Technical Approaches, and Legal Frameworks Working Groups to gain insight into the real and perceived threat from algorithmic amplification. This research looks at the contextuality of algorithms, the current public policy environment, and human rights as a cross-cutting issue. In reviewing technical and human processes, the paper also looks at the potential agency played by algorithms, governments, users, and platforms more broadly to better understand causality.

Year 3 GIFCT Working Groups: 2022-2023

This fall, GIFCT ran an open and public application process for Year 3 Working Groups that will take place from 2022-2023. Between September and October 2022, GIFCT received 292 applications, 70.2% of which were new applicants who had never participated in a GIFCT Working Group before. Through a rigorous, four-stage review process, GIFCT staff selected a total of 207 participants for five thematic Working Groups. GIFCT selected applicants based on their subject matter expertise, sector diversity, geography, and perspective. Working Group participants come from 43 countries across six continents, with 59% drawn from advocacy organizations, academia or practitioners, 18.4% representing governments, and 22.7% in tech.



Year 3 Working Group Participant Affiliations

Government and Intergovernmental Organizations	Tech Companies	Advocacy Organizations	Academia	Practitioners and Researchers
Aqaba Process	Airbnb	Anti-Defamation League (ADL)	American International University	Accelerationism Research Consortium (ARC)
Australian Department of Home Affairs	Amazon	ARTICLE 19	Georgia State University	Africa Peace Building Club
Australian eSafety Commissioner	BitChute	Australian Muslim Advocacy Network	Harvard University	Alliance Nationale des Consommateurs et de l'Environnement (ANCE-Togo)
Australian Government (Department of Home Affairs)	Checkstep Ltd	Center for Democracy and Technology	International Institute for Counter Terrorism (ICT)	Brookings Institute
Australian Home Affairs	Clubhouse	Digital Grassroots	Kenyatta University (Center for AI and Digital Policy)	Building Blocks for Peace Foundation
Australian Parliament	Discord	Digital Medusa	Leiden University	Center for Monitoring
Canadian Government	Dropbox	Dignity in Difference	Northwestern University	CIVIPOL
Commonwealth Secretariat	Google	Education Endowment Foundation	Ozyegin University	Cyber Security Experts Association of Nigeria
Council of Europe (Criminal Law and Counter-Terrorism Division)	JustPaste.it	European Center for Not-for-Profit Law (ECNL)	Presbyterian University Ghana	CyberPeace Institute
NZ Government (Department of the Prime Minister and Cabinet)	MEGA	European Jewish Congress (Security and Crisis Center)	Rongo University	Digital Industry Group Inc
European Union Directorate General for Migration and Home Affairs	Meta	Extremely Together	Royal United Services Institute	European Forum for Urban Security
Europol	Microsoft	Federation of Islamic Associations of New Zealand (FINAZ)	Sapienza University	Extremism and Gaming Research Network (EGRN)
Government of Slovakia (Counter Terrorism Unit)	Niantic	Future of India Foundation	South Asian University	Glitterpill
Iraqi Prime Minister Office	TikTok	Global Network Initiative	Swansea University	Global Center on Cooperative Security
Kenyan Police	Tremau	IKM Advocates	The University of Edinburgh	Global Network on Extremism and Technology (GNET)
PEReN - French Government	Twitch	Internet Society (ISOC)	University of Auckland	GoodBot
Public Safety Canada	Twitter	Internet Society of Nigeria	University of California, Berkeley	Helsinki Deaconess Foundation
Romanian Ministry of Internal Affairs	Uber	Netsafe	University of California, Los Angeles (UCLA)	Helsinki Deaconess Foundation
Royal Canadian Mounted Police	YouTube	Platform for Peace and Humanity	University of Cape Coast	Human Digital

U.K. Government Ofcom	Zoom	Southern Poverty Law Center	University of Ghana	Institute for Strategic Dialogue (ISD)
U.S. Agency for International Development		Take This	University of Leeds	International Center for Counter-Terrorism (ICCT)
U.S. Department of Homeland Security (Science & Technology Directorate)		The Action Coalition on Meaningful Transparency	University of Limoges	KizBasnia
U.S. Department of State		WMM Advocates	University of Maryland (START)	La Conviviencia
U.S. House of Representatives			University of Neapolis Pafos-Cyprus	Lafayette Group
UNCTED			University of Paris	Love Frankie
UNHCR			University of Professional Studies Ghana	M&C Saatchi
UNODC			University of South Wales	Memetica
			University of Waterloo	Moonshot
			University of Waterloo Peace Research Institute Frankfurt	Mythos Labs
			Victoria University of Wellington	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 Center for the Study of Radicalization
				The Peacemaker Corps Foundation Kenya
				Tiaki Akoako
				Tony Blair Institute
				Wahid Institute
				Wasafiri
				Xcyber Group

GIFCT Strategic Pillar: Prevent

GIFCT's Hash-Sharing Database

The largest cross-platform technical tool supported by GIFCT 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 agreed upon taxonomy 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 cannot be reverse-engineered 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 (among other things) their own terms of service, how their platform operates, and how they utilize technical and human resources.

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 here.

How the Hash-Sharing Database Works

Each GIFCT member who has completed the process to receive access to the database can engage with it as best they see fit so long as their use complies 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 new hashes does not prompt any direct or automatic action on another member's platform, such as removing content. Each member must deliberately (and independently to any other member) select hashes, based on the information provided in the labeling, in order to see if content on their respective platform matches the hash. Each member then also determines independently what potential action to take on content that matches a particular hash, in line with their respective policies and terms of service.

Hashes added to the database must fit within GIFCT's Taxonomy (otherwise understood as inclusion criteria). This taxonomy addresses content based on a terrorist or violent extremist entity producing the content and the type of content the entity produced (or behavioral elements within it) (for details see below on Page 25 the section titled "Current Taxonomy and Composition of the Database").

GIFCT maintains a series of tools and procedures to address potential errors and concerns about hashes in the database corresponding to content that does not meet GIFCT's required taxonomy. Within the database itself, GIFCT provides a feedback tool so that members can share feedback on a hash put in the database by another member. This feedback is prompted when members have questions based on the content that matches to the hash on their platform and whether it meets GIFCT's taxonomy and/or is labeled correctly. The feedback on a particular hash is available to all members so that others can determine whether or not to use the hash, and help the member who added the hash identify where they may need to revisit the hash's labeling or overall inclusion in the database (for more detail see below on Page 32 the section titled “*Feedback on Hashes*”).

GIFCT also maintains a communications system between its team and members that enables further robust discussion about the hash-sharing database. Through this system members and GIFCT can share pertinent updates about the database, raise questions, and facilitate discussion as needed. To date, these procedures and systems have been used to address questions and mistakes in the database (for more detail see below on Page 35 in the section titled “Improvements and Assessments of the Hash-Sharing Database”).

Access to the Hash-Sharing Database

Access to the hash-sharing database is provided only to GIFCT member companies that have fulfilled GIFCT’s membership criteria and completed the information-sharing agreement sign-up process with GIFCT. Governments and other non-tech company organizations do not have access to the hash-sharing database.

Hash-sharing database access is currently given to: Discord, Dropbox, Facebook, Instagram, JustPaste.it, LinkedIn, Mailchimp, MEGA, Microsoft, Pinterest, Twitter, and YouTube.

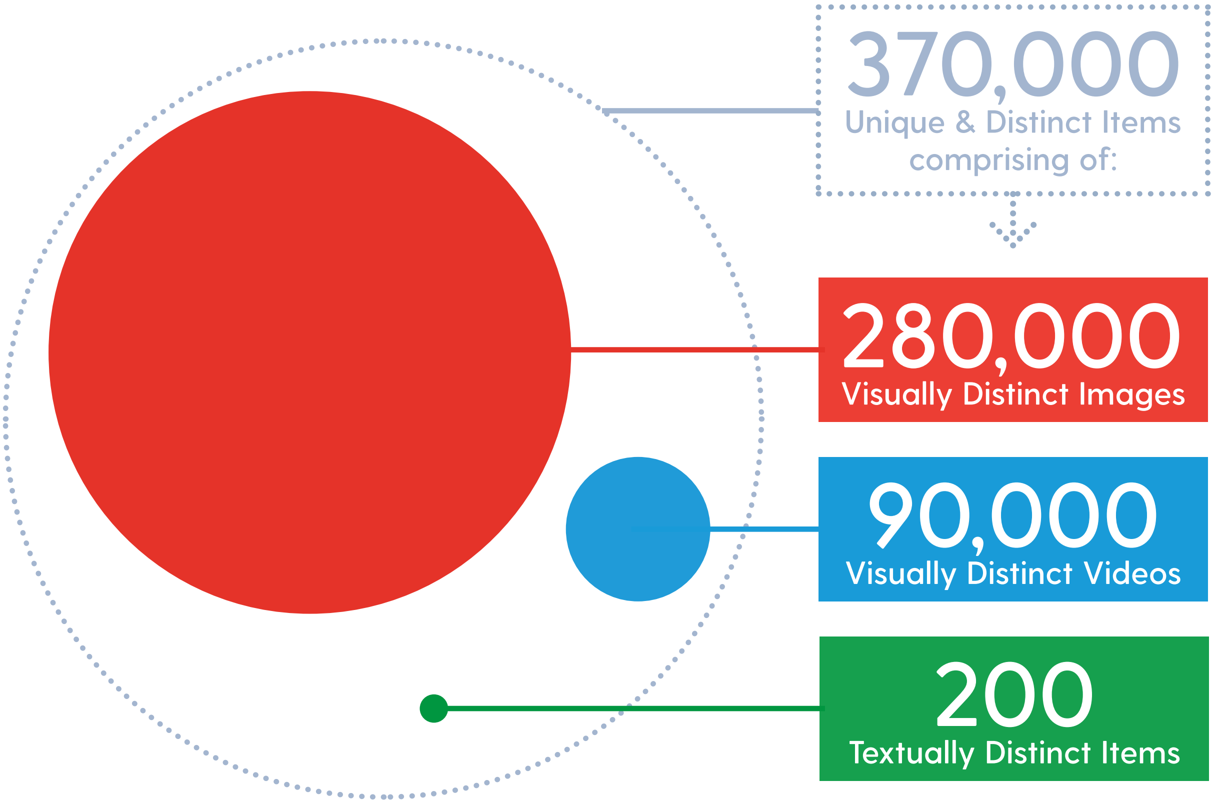
GIFCT members are not required to use the hash-sharing database, but are expected to follow GIFCT’s Code of Conduct when choosing to do so.

In 2022, GIFCT completed the transition process to assume full management and oversight of the hash-sharing database. This change prompted the signing of a new information-sharing agreement (ISA) between GIFCT and each member company, ensuring that only current members of GIFCT were provided access to the database. The hash-sharing database was initially established for the tech company consortium prior to fully establishing GIFCT and its membership criteria. The legacy of this initial stage of the hash-sharing database saw several tech companies with access to the database that had not formally joined GIFCT and demonstrated their ability to fulfill GIFCT’s membership criteria. As part of the final transition process for GIFCT to assume management of the database and sign an ISA with each company, GIFCT offered these companies the option to sign the ISA and maintain access to the hash-sharing database on the condition they begin the formal process to pursue GIFCT membership. Companies that chose not to pursue GIFCT membership were not provided the ISA to sign and their access to the hash-sharing database was rescinded.

From the 14 companies with access to the database as of the 2021 Transparency Report in July 2021, five of these companies were non-members whose legacy access has now been rescinded. Nine companies are GIFCT members that had gained access to the database prior to GIFCT beginning the ISA process and have completed the ISA sign-up process with GIFCT. Three additional member companies who joined GIFCT after this transition process began have now been able to complete the ISA sign-up process and have gained access to the database.

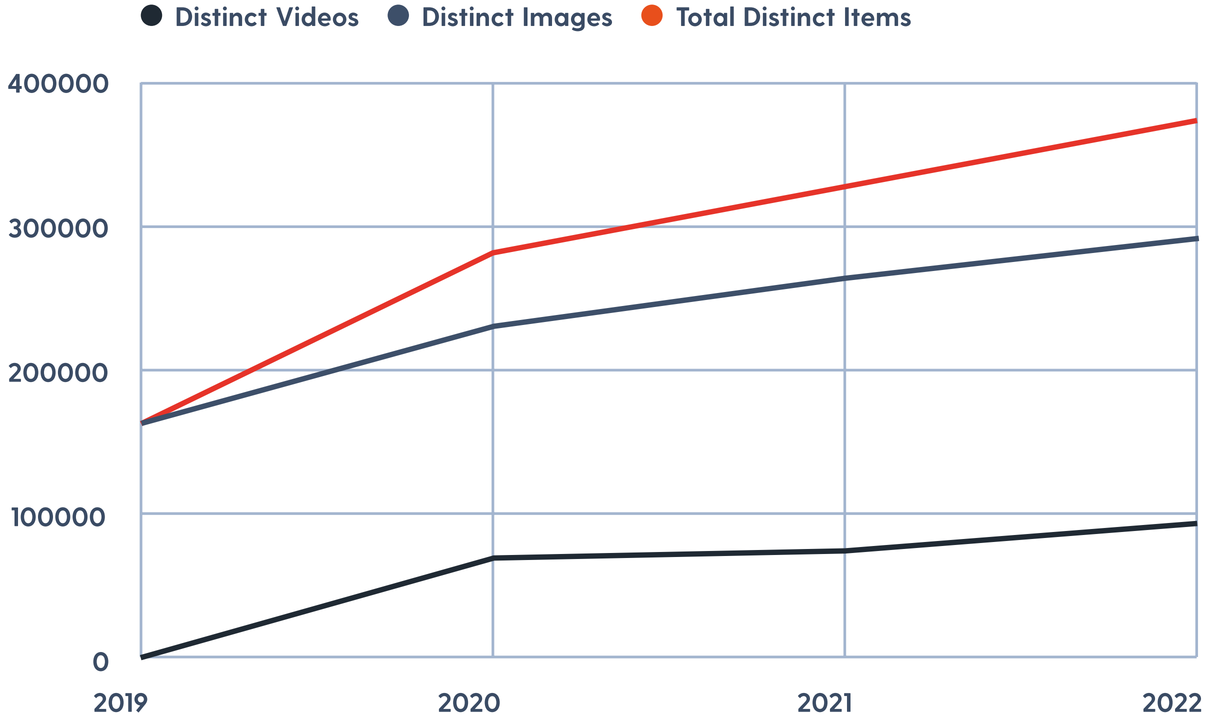
Contents of the Hash-Sharing Database

To date, the hash-sharing database contains approximately **370,000** unique and distinct items relating to approximately **280,000** visually distinct images, **90,000** visually distinct videos, and **200** textually distinct items related to PDFs.



The reason the number is approximate is because "distinct items" represent clusters of hashed content that are visually identical or near-identical to the human eye. It is important to provide the number of distinct items because this metric best informs on the volume and composition of GIFCT's hash-sharing database. There are **2.1 million hashes** in total making up the **370,000 unique items**. Since the 2021 Transparency Report, the number of visually distinct items in the database has increased and the total number of hashes has decreased as a result of improvements made for precision of hash-matching (for more detail see below on Page 35 the section titled "*Improvements and Assessments of the Hash-Sharing Database*" and the specific portion on "*Hash Removals*").

Number of distinct items by type



Current Taxonomy and Composition of the Database

Similar to other sectors, tech companies often have slightly different operational definitions of “terrorism” or what constitutes “terrorist content.” For tech companies, their respective definitions for “terrorism” and “terrorist content” 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 address terrorist and violent extremist content 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. This taxonomy contains a series of parameters for inclusion in the database that takes into account:

- the producers of the content being terrorist and violent extremist entities
- the types of terrorist or violent extremist behavior associated with the content and/or the offline violence the content depicts and/or relates to
- the form of the content in terms of images, videos, PDFs, and URLs

The current taxonomy of the database reflects several evolutions and expansions over time. The taxonomy originally addressed images and videos produced by entities on the United Nations Security Council’s 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. Most recently, in response to GIFCT’s 2021 Taxonomy Report, comprising recommendations from global experts and tech company members, the taxonomy has expanded to include terrorist and violent extremist attacker manifestos, publications, and URLs that direct people to where the content addressed in GIFCT's taxonomy is hosted (for more detail see below on Page 29 the section titled "Expanding GIFCT's Hash-Sharing Database's Taxonomy").

GIFCT also maintains a granular system for the labeling of hashes in the database that provides members with information about the hash in relation to GIFCT's taxonomy as well as the ideology associated with the content. Similar to the design of GIFCT's taxonomy, this labeling system is intended to make the database approachable and useful to members in line with their policy and terms of service enforcement practices.

Terrorist and Violent Extremist Entities

GIFCT does not follow a specific government list or maintain its own list of terrorist and violent extremist entities. Instead, GIFCT's taxonomy takes into account the United Nations Security Council's approach in addition to the behavior of entities and individuals who have directly carried out or attempted to carry out violence. Currently, GIFCT's taxonomy addresses entities on the United National Security Council's Consolidated Sanctions List, the perpetrators of terrorist and mass violent attacks who live-streamed or recorded their violence, and terrorist and violent extremist attackers who produced and shared manifestos online in advance of carrying out attacks.

Behavioral Labels

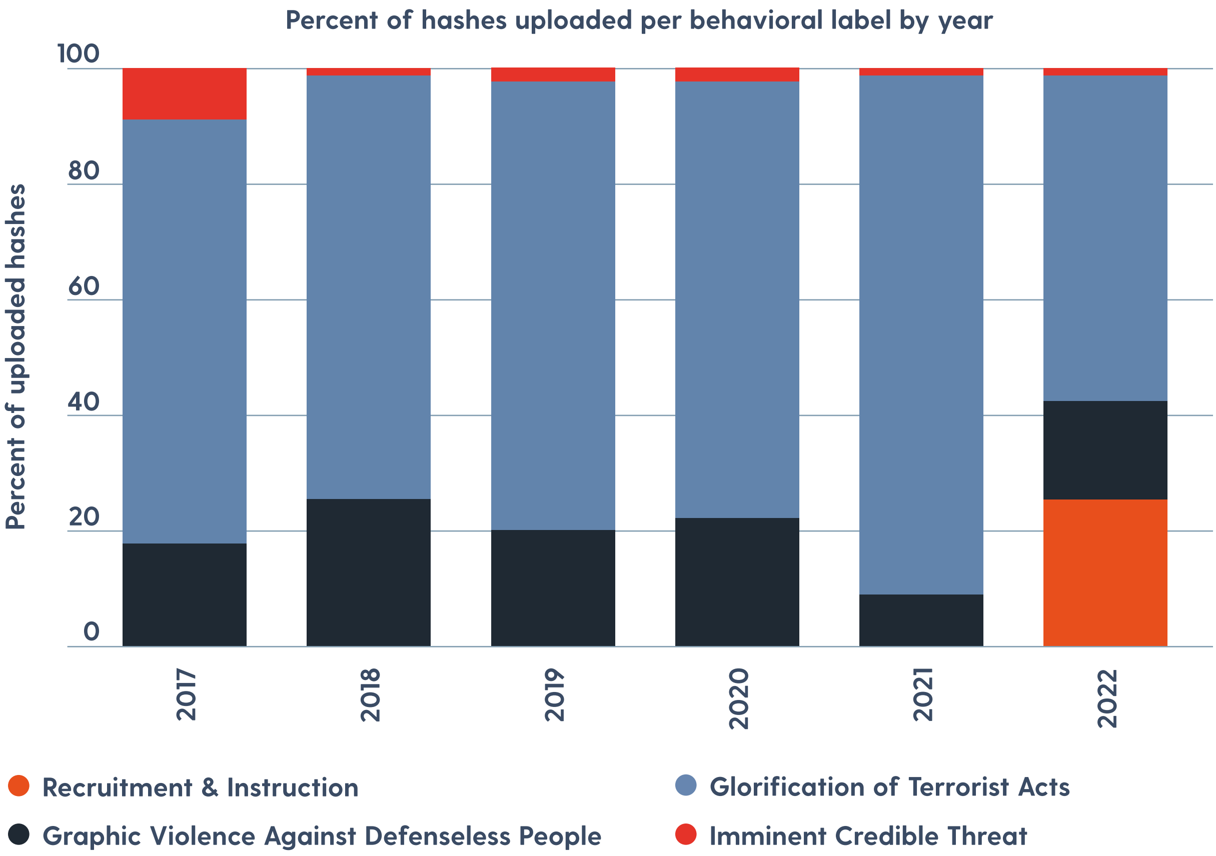
Labels that explain and classify the behavior of the content are added to hashes related to the UN Consolidated Sanctions List and other hashes as applicable in order to assist platforms in how they might triage and review content that matches the hash. These behavioral labels (otherwise known as severity framing labels) are used to categorize the hashes shared in terms of the types of terrorist or violent extremist behavior associated with the content. Labels are applied based on the subject matter expert's review of the content when adding hashes to the database, which can result in differing assessments by experts across GIFCT members of which label or multiple labels to apply. GIFCT is continuing to develop its labeling system and guidance to be approachable and consistent for all members.

GIFCT's Behavioral Labels are as follows:

- **Recruitment and Instruction (R&I):** Content and online materials that seek to recruit followers, give guidance, or instruct them operationally
- **Graphic Violence Against Defenseless People (GVADP):** Content depicting the murder, execution, rape, torture, or infliction of serious bodily harm on defenseless people (prisoner exploitation, obvious non-combatants being targeted)
- **Glorification of Terrorist Acts (GTA):** Content that glorifies, praises, condones, or celebrates attacks after the fact
- **Imminent Credible Threat (ICT):** Content that contains a public posting of a specific, imminent, credible threat of violence toward civilians or non-combatants and/or civilian infrastructure

Of the total number of hashes currently in the database, the percentage of these hashes that have been given a behavioral label is as follows:

Hash Taxonomy Behavioral Label	Percent of Total Hashes
Recruitment and Instruction	0.85%
Graphic Violence Against Defenseless People	15.62%
Glorification of Terrorist Acts	65.23%
Imminent Credible Threat	1.93%



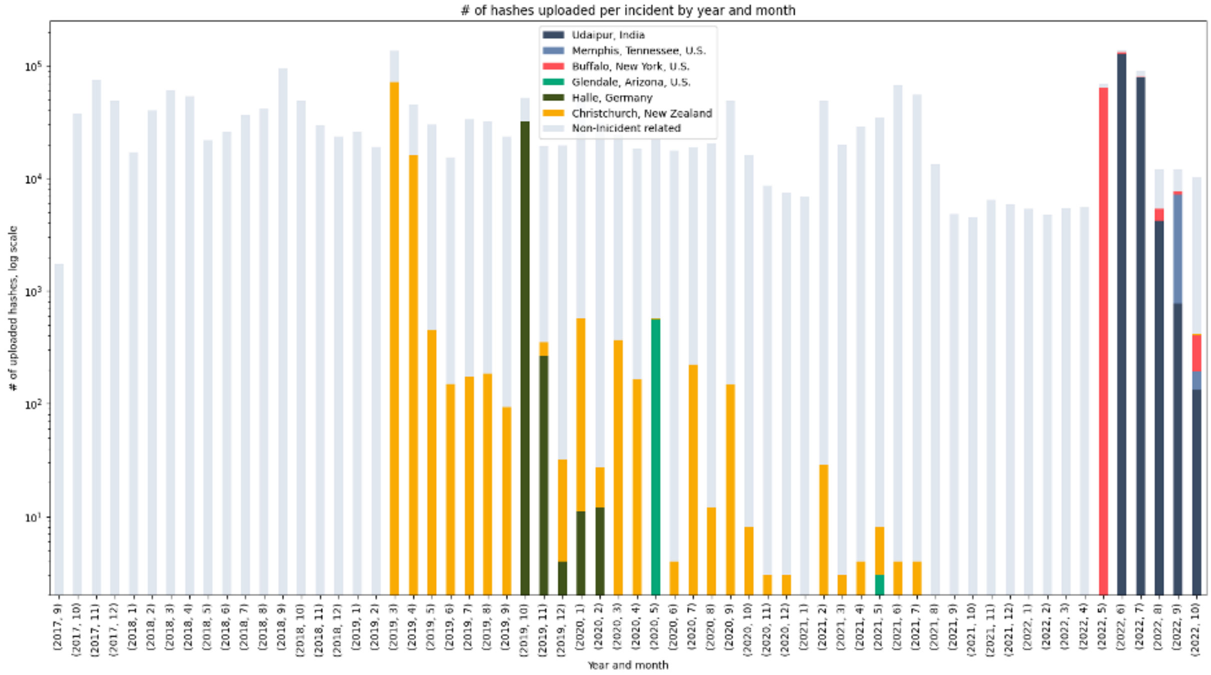
Incident Labels

The first expansion to the taxonomy of the hash-sharing database took place in 2019 following the terrorist attacks in Christchurch, New Zealand in order for GIFCT to include hashes of live-stream content produced by the perpetrators of such attacks. Today the criteria to add such hashes to the database requires that they correspond and prompt the activation of GIFCT's Content Incident (CI) or Content Incident Protocol (CIP) within GIFCT's IRF. As a result, the labels for these hashes in the database directly correspond to the offline terrorist or mass violence attack during which the perpetrators or the accomplices produce content depicting their violence and are referred to as Incident Labels. The following six attacks involved perpetrator-produced content and therefore resulted in GIFCT enabling hash-sharing with the following incident labels for hashes:

- **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 CIP was activated following an attacker live-streaming his attack on a synagogue.
- **Glendale, Arizona, United States:** On May 20, 2020, the CIP was activated following an attacker live-streaming his attack on the Westgate Entertainment District.
- **Buffalo, New York, United States:** On May 14, 2022, the CIP was activated following an attacker live-streaming his attack on a supermarket.
- **Udaipur, India:** On June 28, 2022, the CI was activated following 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 following an attacker live-streaming his attack on a store as part of a series of attacks throughout Memphis.

Of the total number of hashes currently in the database, the percentage of these hashes related to content produced by perpetrators or accomplices of terrorist or mass violence attacks are as follows:

Hash Taxonomy Incident Label	Percent of Total Hashes
Christchurch, New Zealand, Perpetrator Hashes	4.40%
Halle, Germany, Perpetrator Hashes	1.56%
Glendale, Arizona, U.S., Perpetrator Hashes	0.03%
Buffalo, New York, U.S., Perpetrator Hashes	3.37%
Udaipur, India, Perpetrator Hashes	10.27%
Memphis, Tennessee, U.S., Perpetrator Hashes	0.32%



Expanding GIFCT's Hash-Sharing Database's Taxonomy

GIFCT launched a multi-stakeholder effort in February 2021 to develop an expanded taxonomy framework for the hash-sharing database based on research and recommendations generated by global experts and tech company members. This effort sought to balance important concerns from human rights activists about over-censorship and the limitations of list-based approaches with the need for maintaining refined parameters for the database that are operational and useful to tech companies. GIFCT sponsored five proposals from international experts to develop approaches for the expansion of hash-sharing efforts that ensure increased parity and understanding of how terrorist and violent extremist content manifests online.

The result of this effort was the 2021 Taxonomy Report that concluded by identifying expansions to the taxonomy of the hash-sharing database that address the latest types of terrorist and violent extremist content spreading online while ensuring it was globally informed and proportionate, and that GIFCT could manage this with accountability. GIFCT has accordingly begun implementing expansions corresponding to the following terrorist and violent extremist content:

- **Attacker Manifestos:** There have been numerous cases of attackers who have posted their manifestos online in advance of carrying out attacks. This material is often intended for virality and shared among sympathizers. Hashed images and hashed text extracted from PDFs of violent extremist and terrorist attacker manifestos will also be included in the database.
- **TCAP URLs:** In an effort to build on the utility, efforts, and impact of the Terrorist Content Analytics Platform (TCAP), GIFCT will include hashes of URLs that TCAP flags to tech companies that correspond to content produced by entities on the United Nations Security Council's Consolidated Sanctions List and content that activates GIFCT's Content Incident and CIP.

- **Branded Publications:** Terrorist and violent extremist publications are developed with the specific aim of reaching wider audiences online – communicating with existing members and recruiting new members. GIFCT will begin hashing PDFs of branded publications from terrorist and violent extremist entities in 2023, recognized based on the content espousing a hate-based core ideology that calls for violence to advance an ideologically-drive mission.

As part of this taxonomy expansion work, GIFCT has also built new technical capabilities to enable the hashing of text, PDFs, and URLs. Advancing beyond video and image hashing allows GIFCT and its members to address adversarial shifts in attempts to share terrorist and violent extremist content on digital platforms and enables more platforms (namely those not hosting recorded image and video content) to harness GIFCT's collective capacity in line with their respective policies and enforcement practices.

GIFCT has added hashes related to PDFs of terrorist and violent extremist attacker manifestos compiled in coordination with global expert academics. GIFCT has also completed the technical work to add hashes from Tech Against Terrorism of URLs from the Terrorist Content Analytics Platform (TCAP) tied to entities on the United Nations Security Council's Consolidated Sanctions list and content that activates GIFCT's Content Incident and CIP. Hashing of branded terrorist and violent extremist publications will become operational next year. GIFCT looks forward to sharing further updates about this effort in 2023.

Ideology Labels

To further help members navigate the hash-sharing database, GIFCT also included ideology labels as a secondary optional label that can be applied to provide further context to a hash. Content hashed must first meet our inclusion taxonomy. Ideology Labels are then applied on a voluntary basis and assist in indicating the overarching ideological justification the content that was hashed is aligned with. These labels provide greater detailed granularity for members and help GIFCT measure and analyze the hash-sharing database over time. Provided below is the list of ideology labels currently available in the hash-sharing database with links to where GIFCT provides further contextual resources about each ideology within our Definitions and Principles Framework microsite.

- **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 that will inevitably provoke an anti-capitalist revolt.
- **Antisemitism:** Sometimes, particularly with lone attackers, the only ideological motivation apparent is violent extremism based on antisemitism (i.e., hate-based violence focused on Jewish populations or targets). This has to do primarily with Zionist 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 factions take these concepts to a point of targeted violence based on targeting those that might limit these values or hold opposing ideologues. Left wing 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 factions take these concepts to a point of 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 or even extreme nationalist sentiments are not of concern in and of themselves. But there are extreme Hindu fundamentalist factions who 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 celebrate" (incel) community and more broadly groups pertaining to 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 focuses on targeting women as the cause of personal and societal ills and takes particular umbrage with feminism and feminist movements, believing that women should be naturally subservient to men.
- **Islamist Extremism:** Islamist extremism is an ideology coupling strategic violence with an adherence to an extreme reading of Islamic scripture. Islamist extremism 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 fall under 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 key tenets: 1) white individuals and/or populations have a natural, often genetic, dominance over people of other backgrounds and 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; 4) white people are genetically superior to other people.

Of the eight new ideology labels, GIFCT has so far added hashes belonging to six of these labels. Hashes with ideology labels account for 0.05 percent of the total hashes in the database.

Ideology Taxonomy Expansion	
% of total hashes with ideology labels	0.05%
Hash Taxonomy Ideology Label	**Percent of those Hashes with Ideology Labels**
Accelerationism	0.71%
Antisemitism	0.06%
Far-Right	1.11%
Incel/Misogyny-based Violence	0.04%
Islamist Extremism*	96.56%
White Supremacy	1.60%

*The high percentage of hashes with an ideology label of Islamist Extremism is a result of GIFCT's hash-sharing database initially operating with a taxonomy specific to the United Nations Security Council's consolidated sanctions list. GIFCT expects this percentage to change overtime based on greater use of ideology labels and additions of new hashes to the database from other categories of terrorist and violent extremist content within GIFCT's taxonomy.

Feedback on Hashes

Additional functionality was added to the hash-sharing database in 2019, allowing GIFCT members to give feedback on hashes shared within the database. Members can provide feedback on hashes in a number of ways and feedback is visible to GIFCT and all members with access to the database so that each can consider it when deciding to utilize a hash for their enforcement efforts on their own platform. To date, this feature has not been used extensively, but plans are in place to accelerate the adoption and use of this function as part of GIFCT's newly completed transition to oversight of the database.

So far GIFCT has received feedback twice or more on approximately 9,000 visually distinct items representing 34,014 total hashes, approximately 1.63 percent of all hashes. (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.)

Feedback is not evenly sampled across all hashes. Therefore any conclusions drawn from this data should be treated with caution and not be considered statistically significant (e.g., using these figures for extrapolation to the full database is not methodologically sound).

Feedback Metrics	
Number of hashes with feedback (i.e. two or more responses)	34,014
Percent of hashes with feedback	1.63%
Percentage of the 34,014 Hashes with Feedback Supporting Positive Matches	
% of hashes with feedback that indicates a positive match for terrorist and violent extremist content that meets GIFCT's taxonomy	94%
% of CI & CIP-related hashes that indicate a positive match for terrorist and violent extremist content that meets GIFCT's taxonomy	100%
False Positives	
% of hashes with feedback that indicates an item does not meet GIFCT's taxonomy - this is often the result of variations and differences between member companies' policies and reviews of content against their specific criteria for terrorist content.	6% of hashes with feedback, otherwise understood as approximately 0.097% of the total number of hashes in the database

Improvements and Assessments of the Hash-Sharing Database

As part of the initial efforts within GIFCT's management and oversight of the hash-sharing database, during 2022 several GIFCT members were asked to conduct a sampling and review exercise of hashes that they had previously put into the database. This was a first step in a broader ongoing effort for GIFCT to gain greater assurance that hashes included in the database are aligned with the taxonomy – both in the types of content that hashes relate to and that the hashes are labeled correctly in order to be useful and reliable to others. GIFCT is neither a tech company nor a social media platform and does not have any access to source content to determine what the hash corresponds to. For this reason, GIFCT needed to work with members on this sampling and review exercise.

Members were asked to randomly sample three different types of hashes:

1. Hashes that were added because the content was created by an entity on the UN Security Council's Consolidated Sanctions List and met the behavioral framework for content that is included in GIFCT's hash-sharing database taxonomy

2. Hashes that were included in the database as part of a CI or CIP response
3. Hashes that have feedback from another member indicating a disagreement with either labeling or alignment with the taxonomy

After completing this sampling and review exercise, members reported that no significant quality errors were found and in the vast majority of cases, hashes were both appropriately included in the database and appropriately labeled against GIFCT's taxonomy. Members also reported that there was no difference in the quality and accuracy of hashes between those included in response to a CI or CIP, and those included because the content was created by entities on the UN Consolidated Sanctions List.

As a result of a rigorous approach to this exercise, members did find a very small number of hashes were incorrectly labeled and an even smaller number did not meet the taxonomy for inclusion. As a result, the labels have been corrected and any hashes that did not meet the taxonomy have been removed from the database. When hashes are removed from the database by the member who previously added them, another member will see that the hash has been removed the next time they access the database.

The findings of this exercise, including where improvements needed to be made, supported the current tooling in the database and methodology behind this exercise. This was determined based on the fact that the prevalence of the identified inaccuracies was slightly higher for hashes that had received feedback from another member than those without feedback.

Further details of the findings and reconciling inaccuracies is discussed below:

Reconciling Hash Labeling

In the few instances identified of inaccuracies in how hashes were labeled, the cause centered on the behavioral labels used in the hash-sharing database. As a hypothetical example, a document such as the manifesto from the attacker in Buffalo, New York in May 2022 contains both glorification of terrorist acts and recruitment and instructional material. These are different labels in the hash-sharing database and hashes relating to content that overlaps these categories may be labeled by GIFCT members with one or both of these labels, leading to feedback that appears to be disagreement between members. Even within a single company, making these nuanced labeling decisions is not always uniform across different subject matter experts. GIFCT is in the process of updating guidance for member companies on labeling to provide a clearer approach. In the very rare cases where a member could definitively identify an inaccurate label these hashes were re-labeled.

Hash Removals

In a few instances, hashes were found to correspond to content that did not meet GIFCT's inclusion criteria. In all cases the content corresponding to these hashes was related and linked to terrorist or violent extremist material but did not fit GIFCT's taxonomy. GIFCT's taxonomy can be more limited than individual member company's policies that identify and prohibit terrorist content. This is because GIFCT's taxonomy is designed to apply to the greatest number of members, while members have developed different policies and criteria than that used by GIFCT based on the services and platforms that they operate. The types of issues found were finely balanced judgment calls that required deep subject matter expertise and significant context to identify. Some instances reflected both changes in member company policies over time as well as changes in how content is used or reappropriated by terrorist or violent extremist groups. In cases where a member company identified a hash that should no longer be included in the database, the hash was removed. GIFCT is working directly with each member to better understand how their policies, as well as online content itself, evolves over time in order to continually improve the collective capacity to detect with accuracy terrorist and violent extremist content that falls under GIFCT's criteria for inclusion in the hash-sharing database.

Additional hash removals: Separate from the specific sampling and review exercise, hashes were also removed from the database this year in line with standard practices and procedures based on feedback from other members about the content the hashes corresponded to. In this case, feedback on two hashes in the database from another company prompted the member who added the hashes to re-review and determine the content corresponding to the hashes did not meet GIFCT's taxonomy. The content was a music video that was not violent, graphic, or explicit. As a part of this re-review, where hashes were found to be included in the database correctly, they were left, and in the cases where the member no longer retained the records of the original content the hash corresponded to, the member removed the hash out of an abundance of caution.

These hash removals resulted in the overall reduction of total hashes in the database compared to previous GIFCT transparency reports and supported efforts to improve the overall quality and precision of hash-matching in the database.

Data Availability

For a small percentage of hashes reviewed, the member company that added the hash no longer retained the original content. One reason for this is that when content is identified by a company as violating terms of service, typically this content is removed and is no longer accessible to users on the platform or to the public. However, the content **can** still **be** retained for a period based on a number of reasons, including the potential for a user to request an appeal of the decision to remove the content. Each member company has different retention policy periods, but after the period has expired, the original content is no longer held, in compliance with relevant privacy laws. GIFCT policy is that hashes generally remain in the database so that if the same content is uploaded it can still be identified quickly.

As a result of these findings, members determined that this exercise allowed them to confirm that their internal processes for identifying content to hash and applying labels had maintained a high degree of consistency over time. This exercise and members' commitments to participating further indicated GIFCT had developed a successful initial approach to gaining greater understanding and assurance of the quality of hashes in the database. GIFCT is grateful to these members for the extra time and effort they put into quality review processes with GIFCT and we will look to further develop and expand this workstream in 2023.

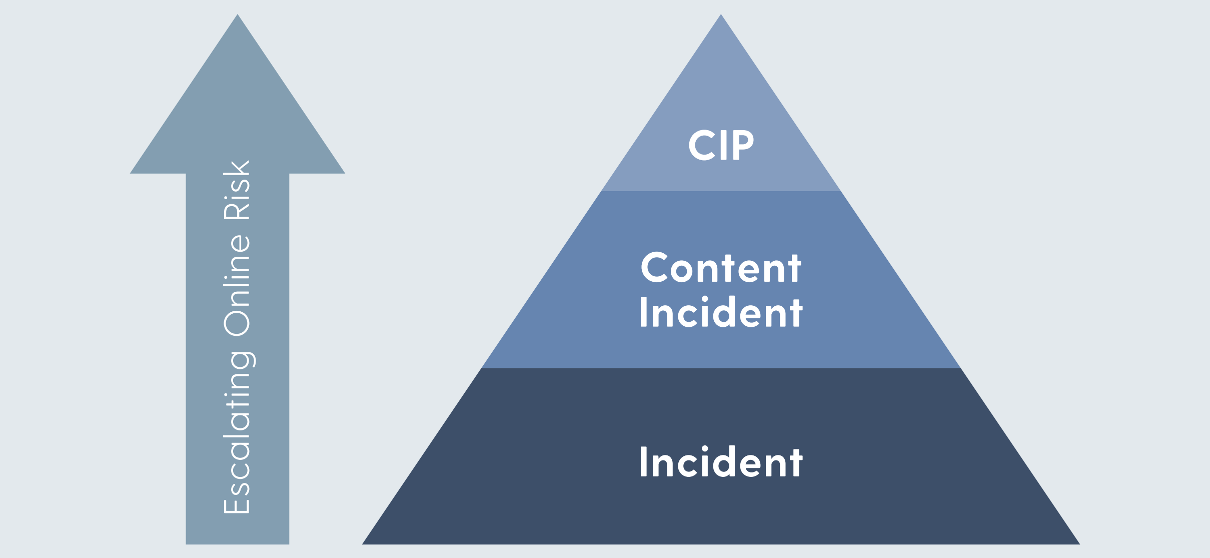
Law Enforcement Requests

Over the last year, GIFCT received no formal requests for data or access from a government entity regarding hashed content in the hash-sharing database. Questions and requests for specific content 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.

GIFCT Strategic Pillar: Respond

GIFCT's Incident Response Framework (IRF) is the set of protocols and processes in place to guide how GIFCT and members respond quickly, effectively, and in a coordinated manner to terrorist and mass violence events with a significant online aspect. The IRF currently contains three 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 take. These Levels are Incident (I), Content Incident (CI), and Content Incident Protocol (CIP).

Levels of GIFCT's Incident Response Framework



The criteria to activate the **Incident** level (the lowest within the IRF) are:

- An ongoing terrorist, violent extremist, or mass violence event, threat, or attempt; **AND**
  - Content related to the terrorist event is circulating online but unclear whether it is depicting murder, attempted murder, or violence, or if it is produced by bystanders of the event **OR**
  - Gaining international media attention **AND** appearing to have a significant online element.

Note: GIFCT's taxonomy for the hash-sharing database does not permit hashes relating to bystander footage of offline violent events, only hashes related to content produced by terrorist and violent extremist entities. Given that in this situation it is unclear whether online content is produced by the perpetrators or accomplices of the offline violent event, this level of the IRF does not prompt GIFCT to enable hash-sharing.

The criteria to activate the **Content Incident** (the middle level within the IRF) are:

- An ongoing terrorist, violent extremist or mass violence event; **AND**
- Content other than live-streamed video (e.g., photo, audio, or text) produced by perpetrator or accomplice; **AND**
- Depicting murder, attempted murder, or violence from the attack; **AND**
- On a member platform (or so broadly available online it will inevitably be shared on member platforms).

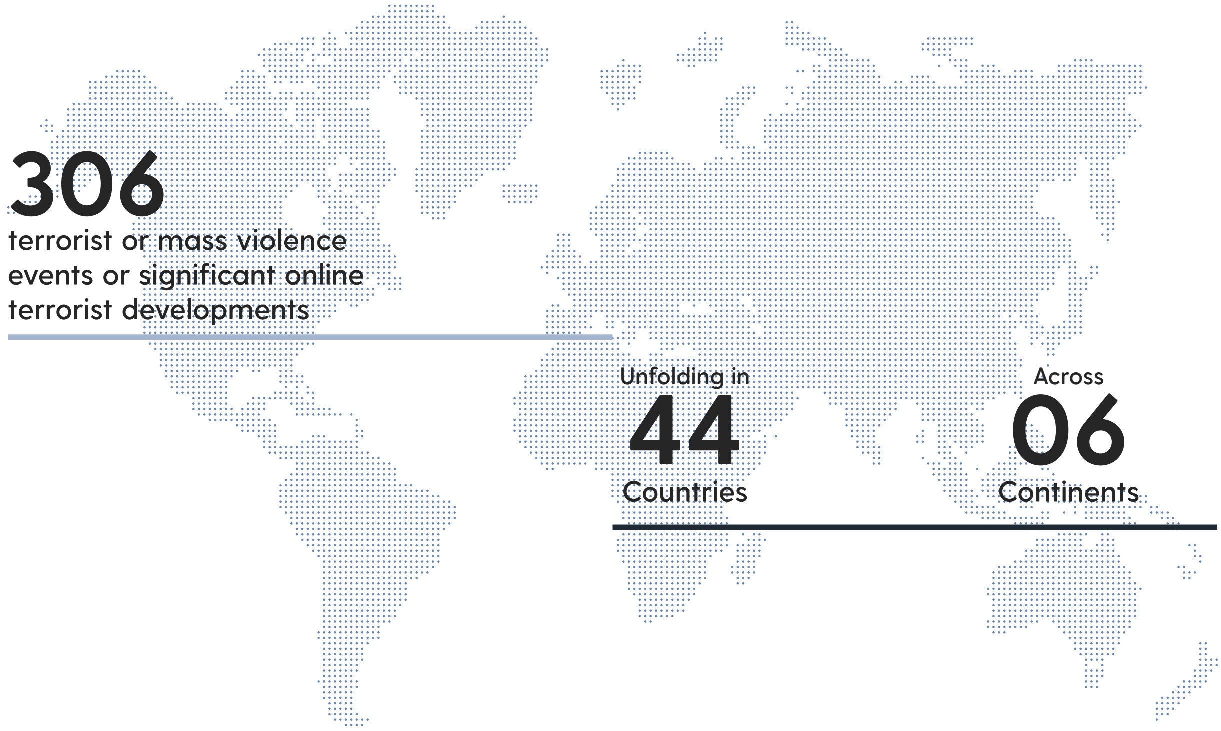
The criteria to activate the **Content Incident Protocol (CIP)** (the highest level within the IRF) are:

- An ongoing terrorist, violent extremist or mass violence event; **AND**
- Live-streamed or recorded video produced by perpetrator or accomplice; **AND**
- Depicting murder or attempted murder; **AND**
- On a member platform (or so broadly available online it will inevitably be shared on member platforms).

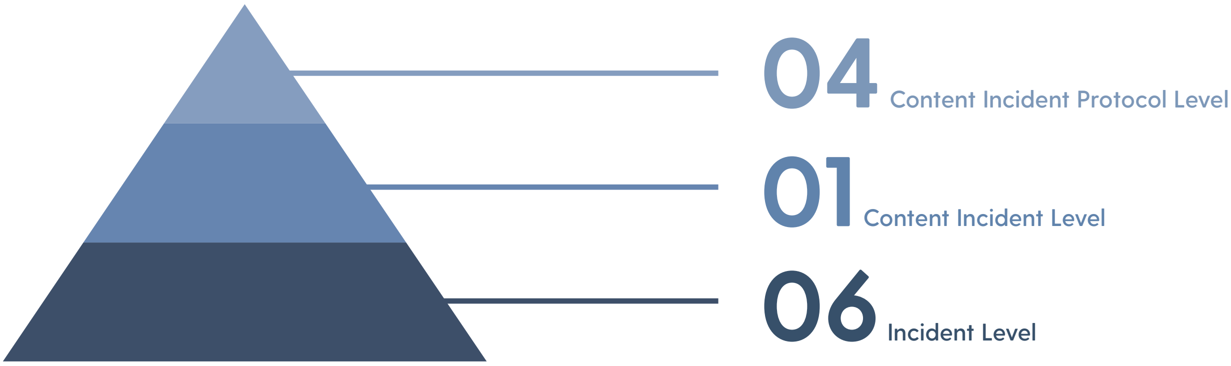
The three levels - Incident, Content Incident, and Content Incident Protocol - reflect an assessment of the severity of the threat of exploitation of digital platforms, and illustrate that GIFCT's critical focus for its response remains on stemming the spread of terrorist and violent extremist content online. In cases where either the Content Incident (CI) or Content Incident Protocol (CIP) levels are activated, GIFCT enables its members to contribute hashes of associated content so that each member can assess instances of the content shared on their platforms as efficiently as possible in line with their respective terms of service. The CIP is the highest level of GIFCT's IRF. This reflects the heightened threat this 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, which may be manipulated for maximized dissemination online. To learn more about how the CIP works visit GIFCT's website here.

GIFCT members began developing the IRF following the terrorist attacks in Christchurch, New Zealand in March of 2019. As part of this effort, members established a centralized communications mechanism 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 among GIFCT and members with enhanced understanding of the event unfolding and how respective platform policies may apply.

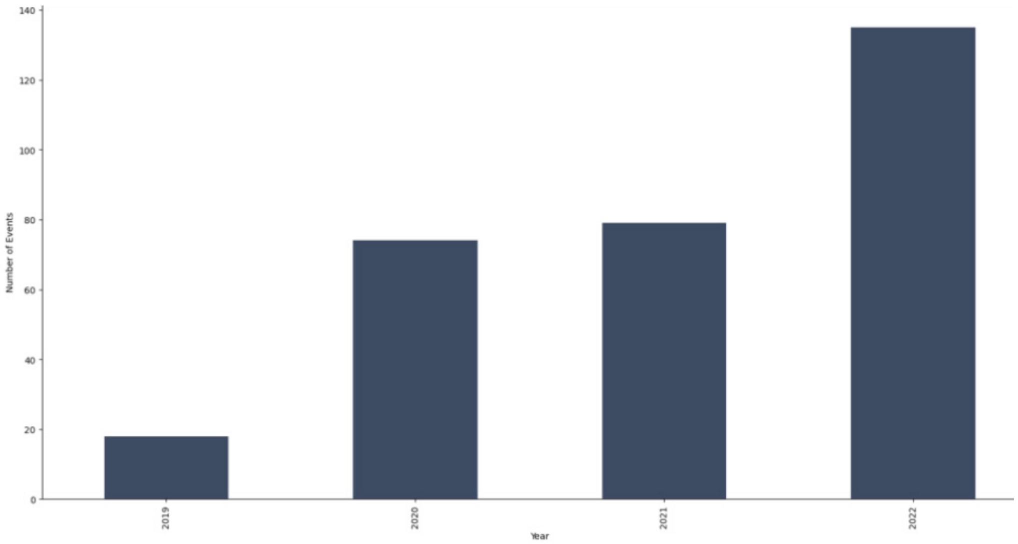
Since the initial development of the Incident Response Framework in 2019, GIFCT and our members have initiated communications to share situational awareness and information in response to:

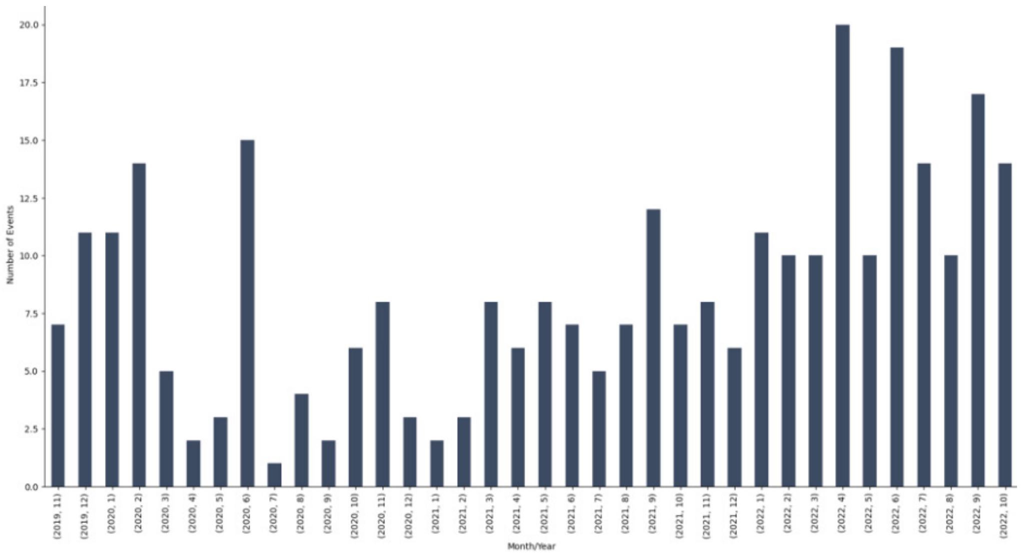

306
terrorist or mass violence events or significant online terrorist developments
Unfolding in
44
Countries
Across
06
Continents

As a result, GIFCT has activated its Incident Response Framework **11 times** at the following levels:

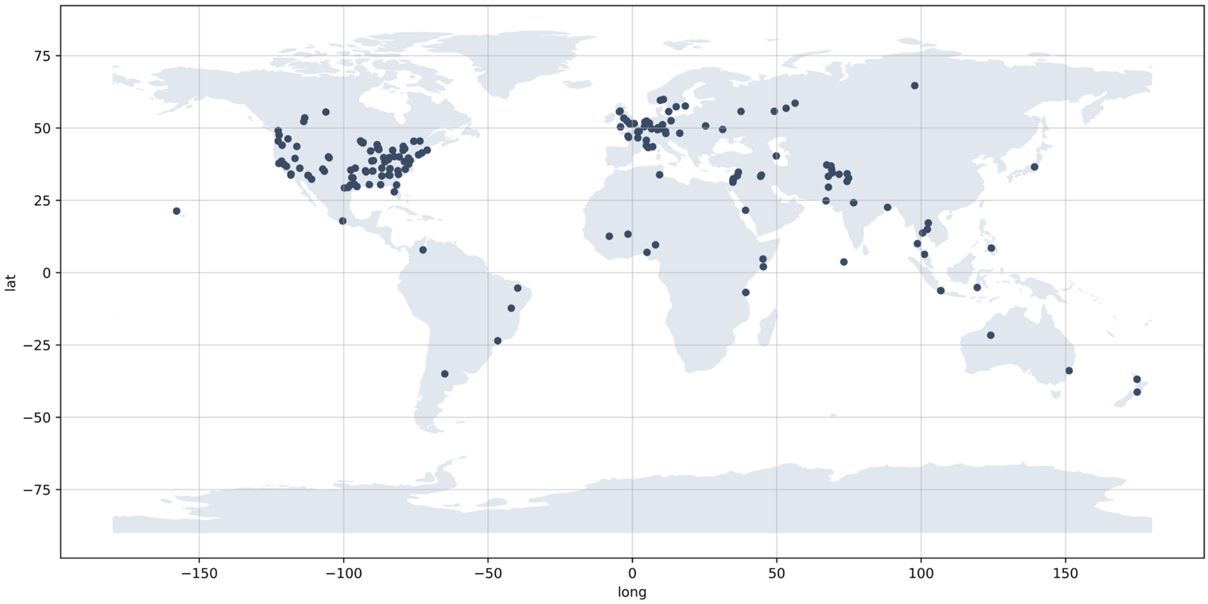


In 2022 alone, GIFCT and our members initiated communications in response to over 135 offline terrorist or mass violence events, or significant online developments in terms of the release and online dissemination of distinct videos, manifestos, or other graphic content by identified terrorist or violent extremist groups. The increase in the number of initiated communications responses this year compared to previous years is both a reflection of 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.





Locations of Offline Mass Violent or Terrorist Events that Initiatied GIFCT and Member Communications



Activations of the Incident Level of GIFCT's IRF since April 2019

Date	Event
October 12, 2022	Bratislava, Slovakia
April 22, 2022	Washington, DC, USA
January 15, 2022	Colleyville, TX, USA
October 08, 2021	Kunduz, Afghanistan
August 26, 2021	Kabul, Afghanistan
July 06, 2021	Amsterdam, the Netherlands

Activations of the Content Incident Level of GIFCT's IRF since April 2019

Date	Event	Number of Visually Distinct Items Shared within the Duration of the Activated Content Incident
June 28, 2022	Udaipur, India	54

Activations of the Content Incident Protocol Level of GIFCT's IRF since April 2019

Date	Event	Number of Visually Distinct Items Shared within the Duration of the Activated Content Incident Protocol
September 7, 2022	Memphis, Tennessee, USA	49
May 14, 2022	Buffalo, New York, USA	870
May 20, 2020	Glendale, Arizona, USA	150
October 9, 2019	Halle, Germany	36
March 15, 2019*	Christchurch, New Zealand*	800*

*The terrorist attacks on March 15, 2019 and the related perpetrator-produced content shared online as part of the attacks prompted the creation of GIFCT's CIP. Therefore, while this event did not activate the yet-to-be established GIFCT IRF, hashes added in response to this attack were the first of this nature and are included in the table above.

When GIFCT activates the CIP, it enables members to share hashes of the perpetrator-produced content to GIFCT's hash-sharing database and following the conclusion of the CIP, the number of visually distinct items added to the database is measured and shared publicly. For example, when GIFCT activated the CIP in response to the attack in Buffalo, NY in May 2022, 870 visually distinct items were added to the database over the course of the CIP's activation. 870 visually distinct items relate to 870 of these clusters of hashes; 870 different signals that GIFCT member companies can use to identify the perpetrator-produced content. While this does not inform on the extent of the content's online reach, how many times it was viewed, or how many times the content was uploaded and shared, this metric does show that there were significant adversarial attempts to produce variants of the original content. Following the conclusion of the CIP's activation, members continue to share additional hashes related to new versions of the content in question as they identify them.

Improving GIFCT's Incident Response Framework Through Stakeholder Feedback

GIFCT continually works to strengthen and refine the IRF with input from members, our IAC, and the stakeholder community. This requires enhancing the transparency of GIFCT's response efforts. In response to the outputs from GIFCT's Year 1 Crisis Response Working Group in 2021 and GIFCT's HRIA, GIFCT has incorporated a formal debrief process as the final step when the CIP is activated.

This process was fully implemented into GIFCT's procedures in 2022 with formal debriefs conducted following the activation of the CIP in May in response to the shooting in Buffalo, NY, USA and September following the shooting in Memphis, TN, USA. These debriefs were conducted in two stages - the first convened only GIFCT and its members, and the second convened members and a wider multi-stakeholder community. These debriefs allow GIFCT to identify where further refinements can be made to systems and processes, provide needed information to governments and civil society organizations about our response, and continue to develop GIFCT's efforts with an understanding of their relation to other international crisis response protocols.

In 2023, GIFCT will focus on the following areas to continue to strengthen readiness and further improve efforts to stem the spread of terrorist and violent extremist content produced as part of an offline violent attack:

- **Human Rights Due Diligence:** Continuing to implement recommendations to remain duly diligent of human rights throughout the process and procedures within the IRF
- **Situational Awareness:** Continuing the implementation of a robust technical system that enables greater real-time alerts and situational awareness
- **Hashes of URLs:** Adding hashed URLs from Tech Against Terrorism's TCAP to provide GIFCT and member companies with greater ability to address attempts to share perpetrator-produced live-streams and other online content when shared on a member platform as a URL where the content is hosted on a non-GIFCT member platform

Engaging with Governments Investigating the Shooting in Buffalo, New York

In an effort to support and help inform government investigators seeking to understand how GIFCT and its members responded to the horrific shooting on May 14 in Buffalo, New York, GIFCT met with the New York State Attorney General's office and Ofcom (the United Kingdom's communications regulator) as part of their respective investigations. In both instances, GIFCT provided information about the IRF and how the hash-sharing database supports members' efforts to respond and address attempts to share the perpetrator produced live-stream and manifesto shared online as part of the attack. Both government investigations found that GIFCT and its members' collective efforts were notable in the industry's response to the stemming of this harmful content. GIFCT appreciated where their respective reports provided insights on how further improvements to our response work can be made.

GIFCT Strategic Pillar: Learn

Action-oriented learning is the third strategic pillar of GIFCT's work with a goal of enabling the exchange of information across sectors about terrorist and violent extremist exploitation of the internet and the solutions to counter it. To carry out this goal, GIFCT produces publicly-available resources in partnership with global experts that 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 latest resources and events GIFCT and its partners produced in 2022.

Definitions and Principles Framework

Developed by GIFCT's team, the Definitions and Principles Framework microsite aims to help tech companies and the wider counterterrorism and counter-extremism community in understanding, developing, and applying definitions of terrorism and violent extremism. Spearheaded by GIFCT's programming team, GIFCT used the definitional elements identified by Schmid and Jongman (1988) along with research by Hedayah in GIFCT's 2021 Taxonomy Report to outline 20 behavioral elements found across legal definitions of terrorism. The microsite classifies and allows for comparisons of a total of 82 definitions of terrorism and violent extremism: 60 national definitions of terrorism, four intergovernmental bodies' definitions of terrorism, and 18 countries' definitions of violent extremism.

Research Insights, Reports, and Convenings from the Global Network on Extremism and Technology

GIFCT has continued to support its academic research network, the Global Network on Extremism and Technology (GNET), led by the International Centre for the Study of Radicalisation (ICSR), based at King's College London. GNET brings together a core international consortium of leading academic institutions and experts with core institutional partnerships from Australia, Germany, India, Morocco, the Netherlands, the United Kingdom and the United States, to study and share findings on terrorist and violent extremist use of digital platforms.

GNET Insights

Throughout the year, GNET publishes short, concise papers that empower experts to probe and explore contentious issues relating to violent extremist behaviors and technology and provide tech companies with actionable research to understand how exploitation can manifest on their digital platforms.

In 2022, GNET:

- Published **116 insights** from
- **120 contributors from 24 different countries:** Afghanistan, Argentina, Australia, Austria, Belgium, Canada, France, Germany, India, Ireland, Israel, Italy, Malaysia, Norway, Pakistan, Poland, Singapore, Spain, Sri Lanka, Thailand, Turkey, the United Kingdom, Uruguay, and the United States;

- **Published 6 insights** produced by the Accelerationism Research Consortium (ARC), a cross-sector collaboration of researchers, practitioners, analysts, and journalists who are dedicated to understanding and mitigating the threat posed by accelerationist terrorism; and
- **Published 4 insights** produced by the Extremism and Gaming Research Network (EGRN), an organization that brings together world-leading counter-extremism researchers, practitioners, and policy makers together with the private sector to develop solutions for the exploitation of online gaming by terrorists and violent extremists.

GNET Research Papers & Reports

In 2022, GNET produced **six reports** from authors based in **six different countries: Germany, Malaysia, Netherlands, Pakistan, the United Kingdom and the United States**. These reports are available in English with executive summaries provided in French, German, Arabic, Indonesian, and Japanese:

1. Manipulating Access To Communication Technology: Government Repression or Counterterrorism? by Fatima Mustafa (Lahore University of Management Sciences)
2. Offline Versus Online Radicalisation: Which is the Bigger Threat? by Dr. Nafees Hamid (ICSR) and Christina Ariza (King's College London)
3. The Role of Violent Conspiratorial Narratives in Violent and Non-Violent Extreme Right Manifestos Online, 2015-2020 by Dr. William Allchorn, Dr. Andreas Dafnos, and Francesca Gentile (Centre for the Analysis of the Radical Right)
4. Radical Right Activities in Nusantara's Digital Landscape: A Snapshot by Munira Mustaffa (The Chasseur Group)
5. Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies by Dr. Yannick Veilleux-Lepage (International Centre for Counter-Terrorism), Chelsea Daymon (International Centre for Counter-Terrorism) and Dr. Emil Archambault
6. Emergent Technologies and Extremists: The DWeb as a New Internet Reality? by Inga Trauthing (International Center for the Study of Radicalisation) and Lorand Bodo

GNET Workshops & Annual Conference

To further facilitate multi-sector knowledge-sharing opportunities and provide expertise to a range of stakeholders, GNET and GIFCT teamed together with institutional partners in different parts of the world to curate **13 workshops** focusing on the nexus between terrorism and technology. The workshops were held virtually from partner home institutes in Australia, France, Germany, India, Morocco, the Netherlands, Singapore, the United Kingdom, and the United States. Topics included:

1. Far right extremist financing online in Australia (The Lowy Institute)
2. Online governance and right-wing extremism: Addressing challenges in proscription and taxonomy (The International Centre for Counter-Terrorism)
3. Content Preservation: Exploring options to preserve and provide access for evidentiary

social media content (Cyber Threats Research Centre)

4. SLAID: Identifying and disrupting serious cyber-enabled crime and online extremism (Cyber Security Cooperative Research Centre)
5. The digital billion: South Asia, expanding online, and expanding extremism (Observer Research Foundation)
6. Understanding technological resilience of violent extremist networks (Policy Centre for the New South)
7. Platform to platform: Online extremists' reactions to terms of service enforcement (Program on Extremism, George Washington University)
8. The fusion of offline and online interventions against extremism in the Philippines (The Centre of Excellence for National Security)
9. Between broadcasting and hide-and-seek: How extremists use alternative (social) media platforms (The Peace Research Institute Frankfurt)
10. Researcher safety online (The International Centre for Counter-Terrorism)
11. Assessing (and countering?) the threat of incel violence (Cyber Threats Research Centre)
12. OSINT and counter-terrorism: Access to data and (AI) technologies in Africa (Policy Centre for the New South)
13. Examining the Buffalo terrorist attack & response (ARC)

In May 2022, GNET launched its Second Annual Conference. Approximately 300 unique visitors joined both in person and virtually logged into the various sessions throughout the day.

E-Learnings with Tech Against Terrorism

GIFCT partners with Tech Against Terrorism for monthly e-learning webinars that are open to global participants across sectors under Chatham House Rules. Launched in March 2021, e-learnings facilitate multi-sector knowledge sharing by bringing global experts on key topics of interest and tech companies to the virtual stage. This year, sessions included diverse voices from around the world and a variety of tech companies to explore and discuss a range of topics.

GIFCT and Tech Against Terrorism convened nine e-learnings in 2022 on the following topics:

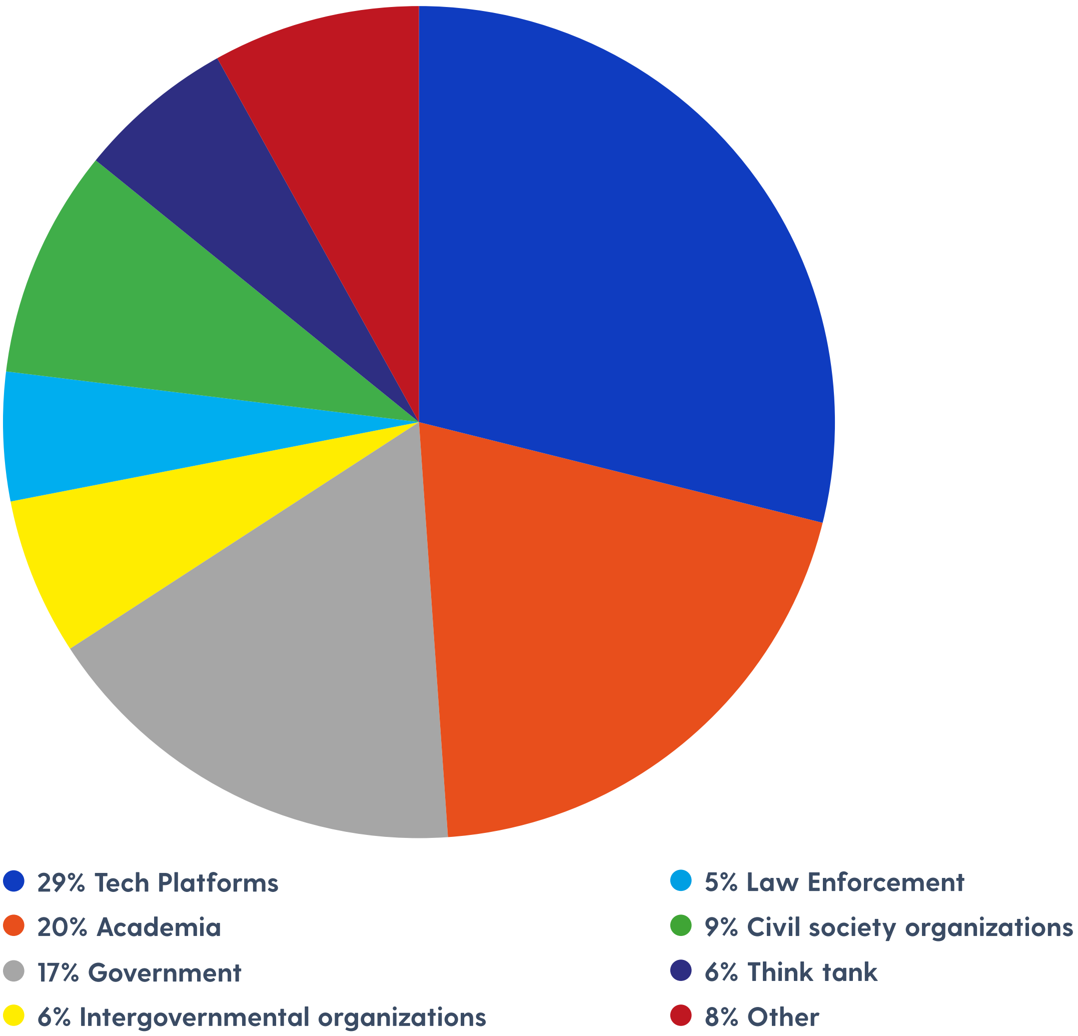
1. Global Challenges in Moderating Far-Right Violent Extremism Online (February 24, 2022)
2. The Gamification of Extremism: Extremist Use of Gaming Platforms (March 24, 2022)
3. Audio Content & Detection: Moderation Challenges and Opportunities with Existing Audio Detection Models (April 28, 2022)
4. Moderation online: Beyond content (May 24, 2022)
5. Live-streaming of Terrorist and Violent Extremist Content: Moderation and Crisis Response (June 23, 2022)
6. Misogynist and Male Supremacist Violent Extremism: Evolving National Security Threats (August 18, 2022)

7. Mental Health Tooling and Support for Researchers and Content Moderators (September 29, 2022)
8. Moderation Online: Beyond Content (November 10, 2022)
9. Year in review: Trends in Terrorist and Violent Extremist Use of the Internet and the Online Counterterrorism Response (December 15, 2022)

Over the course of the 2022 e-learnings series, GIFCT and Tech Against Terrorism convened **446 participants** virtually joining from a variety of sectors to listen to expert discussions and raise questions for further understanding and conversation.

The breakdown of participants by sector is as follows:

Number of Attendees



Conclusion

GIFCT will continue to hold itself to a high standard of transparency as a core value in its mission to counter terrorism and violent extremism online. We hope that the information provided in this report is of value. To compare this year's transparency report to previous years please visit the Resources and Publications page. For more about GIFCT please visit the website and to learn more about the year in review please see GIFCT's 2022 Annual Report.

GIFCT
Global Internet Forum
to Counter Terrorism

Thank You

Once again, GIFCT thanks and applauds all of our member companies committed to our mission for the impact and collective progress we achieved this year. GIFCT is grateful to the diverse array of participants in GIFCT Working Groups and our vital community of global stakeholders for their hard work and important contributions. We are indebted to the governance and guidance provided to us by our Independent Advisory Committee and Operating Board. As YouTube provided momentum to GIFCT's 2022 efforts as Board Chair, we welcome Facebook taking up this position in 2023 to continue our evolution. GIFCT looks forward to the year ahead and the opportunity it will provide to make meaningful progress toward our core mission of preventing terrorist and violent extremist exploitation of digital platforms.