

# 2022 GIFCT Annual Report



**GIFCT**  
Global Internet Forum  
to Counter Terrorism

<b>Table of Contents</b>	<b>Page</b>
Letter from Interim Executive Director, Dr. Erin Saltman	<b>3</b>
Letter from GIFCT 2022 Operating Board Chair, Leslie Miller	<b>5</b>
Letter from Independent Advisory Committee Chair, Dr. Ghayda Hassan	<b>7</b>
Overview	<b>10</b>
GIFCT 2022 Membership Updates	<b>16</b>
GIFCT's Commitment to Human Rights	<b>19</b>
GIFCT Working Groups	<b>23</b>
GIFCT Strategic Pillar: Prevent	<b>29</b>
GIFCT Strategic Pillar: Respond	<b>34</b>
GIFCT Strategic Pillar: Learn	<b>38</b>
GIFCT 2022 Financials	<b>45</b>
What to Expect in 2023	<b>47</b>

## Letter from Interim Executive Director, Dr. Erin Saltman

Dear GIFCT Members, Partners, and Stakeholders,

It has been a pleasure and privilege to act as GIFCT's Interim Executive Director as our inaugural Executive Director, Nicholas Rasmussen, was called back to government service in the United States. While he leaves big shoes to fill, GIFCT looks forward to solidifying new leadership in 2023 and carrying on the crucial work needed to effectively counter terrorism and violent extremism online.

There is much to reflect on as GIFCT wraps up 2022, five years since its launch as a tech-led initiative in 2017 and two years since GIFCT began operating as an independent NGO. Progress has not been without its trials and tribulations as every organization has felt both the impact of a global pandemic and its subsequent realities. However, GIFCT has been able to sustain and evolve to deliver on its mission of preventing terrorists and violent extremists from exploiting digital platforms.

In 2022, we were able to increase our membership, enhance the technical and thematic scope of our tools, advance our efforts to incorporate human rights within our policies and practices, increase our global partnerships, and further solidify our governance structures.

This year GIFCT welcomed a diverse set of new companies with ClubHouse, GIPHY, Google, and Niantic joining as members. A strong and sustained partnership with Tech Against Terrorism has been critical in mentoring companies looking to reach GIFCT's membership criteria to gain access to our network, programs, and tools. Through this process eight companies have developed their first or enhanced their existing transparency reports and 12 have first developed or strengthened their public commitment to human rights. In 2023, GIFCT looks to diversify further both the type and geography of tech platforms working with GIFCT.

We have also advanced the scope and utility of tools available to member companies to facilitate awareness of terrorist and violent extremist activities online. Acting on international feedback received in 2021, we operationalized the inclusion of attacker manifestos and URL hashing capacities within its hash-sharing database. We also incorporated greater communications processes and human rights oversight within our Incident Response Framework (IRF), facilitating awareness of over 135 events in 2022.

Committing to human rights in counterterrorism and counter-extremism efforts is an iterative and constantly evolving process, relying on a diverse set of perspectives and partnerships. Working with our partners at Business for Social Responsibility (BSR), GIFCT is proud to publish a Human Rights Policy this year and advance a number of recommendations made by our Human Rights Impact Assessment (HRIA) published last year, as outlined in this report. We look forward to this work continuing in 2023.

GIFCT's governance structures have also made significant progress this year. GIFCT relies on guidance from its Operating Board and Independent Advisory Committee to calibrate priorities and receive feedback on key strategic objectives. We have been grateful for the leadership and guidance

presented by the 2022 Operating Board Chair Leslie Miller and the YouTube team, who have helped GIFCT increase its transparency and focus our efforts on growing support for incoming and existing members to stay true to GIFCT's mission.

Our Independent Advisory Committee has also matured in its processes and structure, updating the IAC Terms of Reference, bringing in new international members, and producing its first formal written feedback to GIFCT that serves as guidance for evolving the sustainability and impact of Working Group outputs. In 2022, GIFCT formalized an IAC secretariat and welcomed Dr. Ghayda Hassan as our new IAC Chair and Anjum Rahman as our inaugural IAC Vice Chair.

GIFCT succeeds most when embracing engagement with multi-stakeholder networks and global perspectives. Participants in GIFCT's newly relaunched Year 3 Working Groups are based in 43 countries, adding their cross-sector expertise to critical discussions and output. This year GIFCT was able to increase engagement in West Africa through our Workshop in Accra in partnership with the Ghana Cyber Security Authority. GIFCT looks forward to similar engagements in Asia next year.

Going into 2023, GIFCT will continue to support its academic wing, the Global Network on Extremism and Technology (GNET), as it brings in expert insights from around the world to keep us aware of adversarial shifts in extremist networks online. Notably, GIFCT will continue to partner and lend our support to other networks and efforts, whether government-led initiatives like the EU Internet Forum, UN CTED, and Christchurch Call to Action, or academic-run networks such as the Extremism and Gaming Research Network (EGRN) and Accelerationism Research Consortium (ARC).

As the threat evolves, GIFCT must continue to learn from experts and partners to understand adversarial shifts. GIFCT must expand efforts to prevent the spread of terrorism and violent extremism online, and respond to real-world incidents that tactically exploit digital platforms. We have our work cut out for us, but GIFCT's partners, programs, and tooling have set us up for an innovative and productive 2023.

Wishing all our members and stakeholders the best in the coming year,



Erin

## Letter from GIFCT 2022 Operating Board Chair, Leslie Miller

I hope all of you are in good health and will have time with your loved ones over the coming weeks. As outgoing Operating Board Chair, I want to express my gratitude for the work that this organization has done and continues to do. Bringing everyone together again in person for GIFCT's Global Summit earlier this year was a reminder of the value of our collaboration and the diversity of thought across GIFCT, the IAC, government stakeholders, civil society organizations, and academia working in this space.

At the beginning of my Chairpersonship of GIFCT's Operating Board, I committed to five key priorities to support the advancement of GIFCT's strategic plan: 1) thought leadership, 2) membership expansion, 3) crisis response, 4) increasing transparency, and 5) improving governance communication within the structure of GIFCT. As we wrap up this year, I want to reflect on the areas where we've made progress against those commitments and where we have room to do more in 2023.

### Highlights

First, I want to highlight progress in our efforts to affirm GIFCT's thought leadership—in particular developing the Definitions and Principles Framework for Terrorism and Violent Extremism to advise tech companies and the global counter-terrorism and counter-extremism community in understanding, developing, and applying definitions of terrorism and violent extremism. Industry stakeholders have long grappled with how best to collectively define and act against terrorism and violent extremism content without a universally accepted definition of terrorism or violent extremism. The new framework will help us all navigate this challenge. In addition, the Global Network on Extremism and Technology (GNET), with GIFCT's support, continues to release cutting-edge research. This year, the initiative published 116 insights, which cover existing and emerging terrorist and violent extremist issues. One particularly provocative series from this year focuses on Gender and Online Violent Extremism, which explores the cause and effect of gendered online messaging and trends. These insights serve as guide posts, not only for the future direction of GIFCT's work, but also for the global multistakeholder community, and I look forward to seeing what comes next.

Second, I am proud of the work we have done this year to enhance coordination among member platforms and put processes in place to better respond to different types of content. Our Content Incident Protocol (CIP) has proven effective in coordinating members' responses to perpetrator-produced, livestreamed content, but we recognized that terrorist and violent extremist content (TVEC) is not confined only to livestreams. The updated comprehensive Incident Response Framework—which includes the CIP—ensures that GIFCT members are equipped to respond to other forms of perpetrator-produced content, such as video and images.

Finally, related to the CIP work, we've also made great progress on the CI/CIP debrief process to improve communication across organizations and with the public. The debrief conversations have been instrumental in improving response time and global coordination. GIFCT also publishes a blog once the CI/CIP has concluded, reporting on the incident response and hash contributions,

which ensures that the organization can continue to iterate and improve its response while keeping stakeholders and the public informed.

### **Areas for improvement**

While I'm pleased to see that membership increased by over 20%, in 2023 it will be critical for GIFCT to prioritize small and medium-sized platforms and those headquartered outside the US. We will all benefit from more diverse insights and participation as we evolve our efforts to prevent terrorists and violent extremists from exploiting digital platforms. GIFCT must focus on cultivating new members and strengthening the relations with existing members in order to keep pace with the changing threat landscape online.

In addition, the Board asked GIFCT to enhance its risk mitigation and management strategy as part of the membership expansion effort. It's imperative that the organization ensures it's protected against the risk that comes with sharing confidential information. The Board welcomes the collaboration between GIFCT and the IAC to develop a policy that takes into account the challenging geo-political landscape, and the Secretariat we established this year will be critical in facilitating this collaboration. We've already seen the IAC more directly involved in providing feedback to GIFCT on new initiatives, priorities, and opportunities to enhance processes to deliver greater organizational impact.

On behalf of the Board, we appreciate the work of this organization and the meaningful collaboration of the GIFCT stakeholders. This work is not easy and the stakes are high, but I am confident in this forum's ability to lead the global community in the fight against terrorist and violent extremist content on online platforms, and I look forward to all that is to come.

With gratitude,

Leslie Miller

## Letter from Independent Advisory Committee Chair, Dr. Ghayda Hassan

Two years into its development, the Global Internet Forum to Counter Terrorism (GIFCT) has succeeded in ensuring functionality as an independent entity with strong transparency standards and a sustained deep commitment to protecting human rights while minimizing violent extremist and terrorist use of the internet.

As a founding member and the appointed chair of the Independent Advisory Committee (IAC) for the two years to come, I fully understand the magnitude of the challenges that GIFCT faces on many fronts, particularly in relation to establishing its unique niche in the world of PVE/CVE, and in relation to the diversity of partners and stakeholders that contribute to GIFCT's efforts and highlight the necessity of understanding the various tech, academic, civil society, governmental and intergovernmental points of view and competing priorities.

The IAC plays an essential role in supporting GIFCT to achieve its mission and encourage true multi-stakeholder collaboration to ensure that each partner is recognized for its unique expertise and point of view. Through the lens of its multi-sectoral body composed of Government, Academia, Civil Society and Non-Governmental organizations, the IAC advises on programming and strategic goals and objectives and provides ongoing feedback and global perspective. IAC supports rigor and consistency in GIFCT work to set a clear and coherent thread connecting its mission to its objectives and their operationalization as well as their evaluation in terms of impact and contribution to the mission of GIFCT.

During the last few months, the IAC has become more diverse and robust, adequately resourced, well structured, with an effective communication model. The IAC has provided constructive and benevolent criticism to the Operating Board (OB) and GIFCT carrying voices from civil society, community grassroots and human rights organizations working with marginalized communities. In addition, the IAC is working to develop ongoing feedback mechanisms to ensure accountability for GIFCT and its Operating Board and continue to follow up on progress.

During the past year, GIFCT has achieved notable progress on many fronts, showing its agility in adapting to the ever-changing landscape of violent extremist and terrorist use of technology and platforms. Notably, GIFCT has established its expanded taxonomy for the hash-sharing database to include hashed PDFs of attacker manifestos. It has improved the transparency of the hash-sharing database and it has swiftly activated and refined its Incident Response Framework. GIFCT's table top exercises have been a precious initiative to pool in the rich and diverse expertise of stakeholders and develop some line of action to tackle the delicate balance between the technological capacities and human rights.

As it strives to become a more diverse and inclusive multi-stakeholder forum, GIFCT will continue benefiting from IAC guidance and support on two key issues that are at the core of its mission: 1- Becoming a more diverse and inclusive GIFCT; and 2- Implementing impactful actions and ensuring



engagement of its member platforms.

To become the true multi-stakeholder forum it seeks to be, GIFCT has to take a step back from its North America and Europe centric approach and expand its membership by welcoming more platforms from around the globe and by opening up to multiple languages. IAC will support GIFCT in developing a robust and flexible membership onboarding, support and member performance evaluation tools with adequate risk assessment and mitigation measures. In the past four months, IAC has provided insight and guidance on these areas, through feedback and recommendations on GIFCT's 2022 Global Summit and its multi-stakeholder forum, on Working Groups and on platform expansion. We expect these recommendations will help GIFCT better guide its future members and leverage their capabilities as well as support its current members in continuing to honor their engagements, particularly when faced with structural or resourcing challenges, as well as in the context of an ever evolving economic and political landscape.

While GIFCT has provided important support for its member platforms and continues to expand its membership, the contribution, role, and input of member platforms to GIFCT's mission, objectives, activities and multistakeholder forum as well as the Working Groups leaves room for improvement. To ensure sustained and impactful engagement of its members, IAC will support GIFCT to develop participation models that are innovative and supportive of the ideas, talents and resources that each member has to bring to the table. By engaging more proactively, we hope members will improve their commitment to GIFCT's mission, as well as invest in their reactivity and technical capacity, while making their transparency and commitment to human rights and protection of impacted communities a top priority.

Looking forward to the coming year, IAC will support GIFCT in hiring and onboarding a new Executive Director in addition to continued support of our common vision and objectives. We will continue to support GIFCT staff in the implementation of recommendations for Working Groups and membership expansion, particularly risk mitigation. IAC will provide the needed support and guidance to GIFCT to ensure that member platforms take a proactive part in setting GIFCT priorities and shaping the conversation around needs and gaps as they pertain to platform design, policies, processes etc.

We would encourage GIFCT to engage more with member platforms as a multi-stakeholder body and to prioritize development of a systemic operating function so that sustainable, nuanced and impactful changes can be made not just to individual technology platforms, but to how the industry considers issues of security and safety. Emphasis on a macro system will allow focus on these platforms as part of a digital ecosystem that is interconnected to both online and offline life of individuals and communities. GIFCT thought leadership should lead these efforts through innovative programming for Working Groups for example.

The IAC will support GIFCT in bringing about a cultural shift in the industry that emphasizes protection of the fundamental right to safety and life for individuals and communities. We will encourage expansion and profit to co-exist in coherence, not as oppositional, to the reintroduction of ethics in the evolution of the online world and in ensuring the safety of all humans with special attention to children and teenagers.



In conclusion we believe that thought leadership for GIFCT should be through support of ethical core operating values for member platforms, the encouragement of an integrated, true multistakeholder and global system where education on e-safety, prevention of violent extremist and terrorist use of the internet and protection of impacted persons and communities are designed and coordinated in a coherent manner consistent with the needs of communities. We must dare to take on this challenge and the IAC is here to accompany GIFCT on this path to excellence.



Ghayda Hassan,  
IAC Chair

## Overview

### GIFCT's Mission, Vision, Values, and Strategic Pillars

GIFCT works to fulfill its mission and achieve its vision guided by its values and organized by its strategic pillars.

Our Mission: To prevent terrorists and violent extremists from exploiting digital platforms.

Our Vision: A world in which the technology sector marshals its collective creativity and capacity to render terrorists and violent extremists ineffective online.

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

GIFCT approaches and defines these values accordingly:

- **Transparency:** GIFCT is committed to transparency surrounding all of our work streams, from joint tech innovation to information-sharing efforts. We prioritize clear and open communication with members and stakeholders and seek to increase transparency through regular assessments of the impact of our work.
- **Inclusion:** GIFCT has an open-door policy with respect to constructive input and innovation. Engaging with a wide array of voices and perspectives from across the globe is a core organizational value, and GIFCT is always seeking to expand and diversify our stakeholder community.
- **Respect for Human Rights:** GIFCT believes that respect for universal and fundamental human rights must be central to and embedded throughout our work in order to fulfill our mission of preventing terrorist and violent extremist exploitation of digital platforms.

Our Strategic Pillars:

- **Prevent:** Equipping digital platforms and civil society groups with awareness, knowledge, and tools to develop sustainable programs to disrupt terrorist and violent extremist activity online.
- **Respond:** Bringing together key stakeholders to mitigate the impact of a terrorist or violent extremist attack.
- **Learn:** Supporting cutting-edge practical research efforts at the intersection of extremism and technology.

### The Global Internet Forum to Counter Terrorism: 2017 - 2022

This month marks two and a half years since the Global Internet Forum to Counter Terrorism (GIFCT) became an independent entity with our own staff of counterterrorism and technology experts

working with GIFCT's Independent Advisory Committee (IAC) and the organization's Operating Board. Since then, GIFCT has grown to a team of ten full-time and contractor staff of counterterrorism and technology experts working with the now 22 technology companies that it supports as members.

GIFCT is a tech-led initiative with the mission to prevent terrorists and violent extremists from exploiting digital platforms. It was originally founded in 2017 by Facebook, Microsoft, Twitter, and YouTube as a consortium of tech companies that recognized the need for combating terrorist and violent extremist activity online and the significant impact working together could have towards that end. At the time, companies were driven by the urgent imperative to respond to the growing use of social media platforms by groups such as the Islamic State. As a result, in-house teams at GIFCT's member companies initially focused on developing cross-platform tools (including the hash-sharing database to share "digital fingerprints" of identified terrorist content) and establish a forum where tech, governments, academia, and civil society could discuss the current online threat landscape, share insights, and produce solutions. GIFCT also made important progress during its first three years establishing GIFCT's membership criteria, creating an ongoing mentorship program with Tech Against Terrorism, launching a GIFCT-funded academic network, and developing its first counterspeech campaign toolkit for practitioners in partnership with the Institute for Strategic Dialogue.

Following the terrorist attacks in Christchurch, New Zealand in March 2019, GIFCT's founding members saw an even greater need for the tech industry to marshal its collective creativity and capacity to render terrorists and violent extremists ineffective online. In May 2019, companies signed the [nine-point action plan](#) of the Christchurch Call to Action led by New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron. As part of this plan, companies committed to undertake a series of measures that included developing tools to prevent the downloading of terrorist and violent extremist material, combatting the causes of violent extremism, improving transparency in the detection and removal of content, and ensuring that the algorithms designed and used by online platforms do not direct users towards violent extremist content.

In order to best support these commitments, GIFCT's four founding members announced in September 2019 at the United Nations General Assembly that GIFCT would evolve from a consortium of tech companies to an independent nonprofit organization with its own team of professionals working with member tech companies towards its mission to prevent terrorist and violent extremist exploitation of digital platforms. Since then, GIFCT has continued collaborating with the Christchurch Call network on shared goals and objectives.

In 2022, GIFCT achieved meaningful progress through sustained engagement with its members, the IAC, and the broader stakeholder community - all while managing leadership transitions and responding to significant developments in the terrorism and violent extremism threat landscape. In July, GIFCT successfully convened the first in-person GIFCT Global Summit as an independent GIFCT, bringing our members and IAC together in California to discuss current progress and future objectives. In September, GIFCT and Tech Against Terrorism hosted their 14th Regional Workshop in Accra, Ghana, convening experts on the threat landscape in the West African region both in person and virtually to discuss its online manifestations and explore solutions. This was the first GIFCT Workshop to take place on the African continent and the first in-person workshop since the start of

COVID-19.

These in-person convenings were important efforts amid GIFCT's sustained work to advance our mission and respond to significant terrorist and mass violent events. In 2022, GIFCT activated the highest levels of our Incident Response Framework (IRF), the Content Incident Protocol (CIP) and the Content Incident - in response to mass violent and terrorist attacks where the perpetrators either live-streamed their violence or shared content depicting their attack online after the violence took place. In response to these horrific events, GIFCT convened its members in order to share situational awareness and contribute hashes of identified content produced by these perpetrators to GIFCT's hash-sharing database, including video and image content as well as manifestos. Once the critical needs of the initial online response to these events had been met, GIFCT worked to further engage its members, IAC, and stakeholder community to share assessments of the information gathered and receive feedback on where further improvements and iterations can be made to strengthen our response in the future.

2022 also saw leadership transitions across GIFCT's three governance bodies. Each year, GIFCT's Operating Board transitions its chair role, and GIFCT welcomed YouTube's Vice President of Public Policy, Leslie Miller, as this year's Operating Board Chair. In July, GIFCT's IAC saw its first chair transition since its establishment and four new representatives from civil society join the committee. Dr. Ghayda Hassan became the new chair after Bjorn Ihler concluded his time as inaugural chair and GIFCT welcomed Anjum Rahman as inaugural Vice Chair - a new role for the IAC to support its leadership and the continuity of the committee. The IAC Chair and Vice Chair are determined by a majority vote amongst the IAC membership and are expected to serve an approximately two-year term.

At the end of September, GIFCT also saw the departure of its inaugural Executive Director, Nicholas Rasmussen, and the appointment of Dr. Erin Saltman as interim Executive Director. GIFCT is truly grateful to Nicholas for his leadership, vision, and expertise as he built the initial team at GIFCT, grew GIFCT's tech company membership, commissioned our Human Rights Impact Assessment (HRIA), and represented our vital work to stakeholders and leaders - all contributing to our progress and success.

## **GIFCT Today**

Interim Executive Director Erin Saltman and the team of experts leading GIFCT's programming, technological, and strategic initiatives manage the day-to-day operations as an independent nonprofit organization. An Operating Board made up of senior executives from GIFCT's founding members - Facebook, Microsoft, Twitter, and YouTube - governs the organization. The Operating Board is advised by an IAC composed of representatives from civil society, academia, government, and intergovernmental organizations and is currently chaired by Dr. Ghayda Hassan, clinical psychologist and professor of clinical psychology at Université du Québec à Montréal (UQAM). Learn more about GIFCT's governance [here](#).

The past two years have been formative for an independent GIFCT, during which we established a roadmap for how to carry out our mission guided by our values and achieved significant progress toward those goals. In 2022, GIFCT strengthened and matured the work we do to support our

member companies with greater resources and engagement with our community. GIFCT launched an annual review process with our partner, Tech Against Terrorism, to better understand how members' current efforts continue to fulfill GIFCT's membership criteria. This is an important system to have in place as membership in the organization continues to grow, so that should companies face challenges in continuing their commitments, GIFCT and Tech Against Terrorism are positioned to provide additional support.

This year GIFCT began adding hashes of PDFs of attacker manifestos to [GIFCT's hash-sharing database](#) to help members identify if they are shared on their services. GIFCT also completed the technical work to add hashes from Tech Against Terrorism of URLs collected and alerted from the [Terrorist Content Analytics Platform \(TCAP\)](#). This work prepares us to begin adding hashes of URLs tied to entities on the United Nations Security Council's Consolidated Sanctions list and perpetrator-produced content that activates GIFCT's Content Incident and CIP next year. Adding these hashes to GIFCT's hash-sharing database enables us and our members to strengthen efforts to address some of the latest adversarial shifts in terrorist and violent extremist attempts to exploit platforms.

This year also saw the successful conclusion of Year 2 of GIFCT's Working Groups, which convened global stakeholders on the challenges at the nexus of technology and terrorist and violent extremist activity, and launched Year 3 of GIFCT's Working Groups that are currently ongoing.

Enhancing transparency of GIFCT's work remains a key objective. GIFCT delayed the release of the 2022 Transparency Report from our normal publication date in July until the end of the year in conjunction with our Annual Report to enable us to invest more time and effort in its production. In this year's Transparency Report, GIFCT sought to provide new metrics, greater insights, and more context about the work we do to support our members and convene our global multi-stakeholder community. As GIFCT's Annual Report continues to provide both longstanding and new stakeholders information about GIFCT as an organization, our Transparency Report provides information so others can see how GIFCT is doing in our efforts to advance our mission. Operating with transparency as a core value, GIFCT has the same commitment to annual transparent reporting that we require of our members, which allows us to inform about our efforts and remain accountable to our mission and values.

This report will elaborate on each substantive element of GIFCT's work in 2022, sharing both our latest progress and next steps for the coming year. To read GIFCT's 2022 Transparency Report, please see [here](#).

## **Global Engagements**

Over the last year, GIFCT hosted milestone events with its community and participated in a number of other forums and convenings as an expert on the threats and dynamics at the nexus of terrorism and technology. GIFCT was honored to participate at these events, where we engaged with a range of global stakeholders on the pressing issues of the day. Below are some of the more significant convenings GIFCT had the pleasure of contributing to.

**GIFCT-Hosted Events:**

- GIFCT's 2022 Global Summit
- GIFCT and Tech Against Terrorism West Africa Workshop
- Embedding Human Rights at GIFCT - virtual events to provide updates six-months after publishing GIFCT's Human Right Impact Assessment
- GIFCT hosted monthly E-Learning virtual events with Tech Against Terrorism

**Events Hosted by Governments and Intergovernmental Organizations:**

- Christchurch Call to Action Leaders Summit hosted by New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron
- Aqaba Process Global Counter Terrorism Conferences hosted by his Royal Highness the King of Jordan - GIFCT participated in the 2022 series of events focused on East Africa, South-East Asia, and Latin America
- G7 Meeting of the Autumn Roma-Lyon Group Conference in Berlin
- 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"
- United Nations Security Council's Counter Terrorism Committee Special Meeting on the Use of New and Emerging Technologies to Counter Terrorism (culminating in the signing of the [Delhi Declaration](#))
- European Union Internet Forum convenings throughout 2022
- United States House of Representatives Committee on Homeland Security Hearing on "The Dynamic Terrorism Landscape and What It Means for America"

**Events Hosted by Academic Institutions and Non-Governmental Organizations (NGOs):**

- RightsCon 2022
- Organization for Security and Co-operation in Europe (OSCE) Security Committee Meeting on Transnational Violent Extremism and Radicalisation Leading to Terrorism Including in the Digital Space
- Eradicate Hate Global Summit
- Future of Online Trust & Safety Conference with Trust & Safety Professional Association (TSPA) and the Digital Trust & Safety Partnership (DTSP)
- Unfinished Live - All Tech Is Human live recorded podcast

- Hedayah's Annual International Countering Violent Extremism (CVE) Research Conference
- Global Counterterrorism Forum UNGA Convening
- Global Network on Extremism and Technology's Annual Conference
- The Raisina Dialogue 2022, hosted by the Observer Research Foundation
- Swansea Terrorism and Social Media Conference (TASM) and Wales Technology Week

GIFCT also provided training to civil society organizations focused on preventing and countering violent extremism (including Meta's Redirect Practitioner Network).



# GIFCT 2022 Membership Updates

## Newest Members to Join GIFCT

With a clear-eyed understanding that the online threat of terrorism and violent extremism is cross-platform in nature, each member that joins GIFCT enables us to expand and strengthen our collective capacity by bringing new technology and expertise to the table and supporting our efforts to develop further cross-platform technical solutions. Expanding GIFCT's membership also supports our commitment to upholding human rights and follows the HRIA on GIFCT published in July 2021 that recommends GIFCT should take a "big-tent" approach to membership across the technology stack.

This year, GIFCT was pleased to welcome **four tech companies** as the newest members to GIFCT, growing the diversity and expertise of digital platforms committed to our mission. In 2022, we've welcomed **Clubhouse, GIPHY, Google and Niantic**. New members bring new opportunities to learn how different companies approach their efforts to prevent terrorists and violent extremists from exploiting their platforms and services, what they have achieved to date, and how together members can collectively strengthen their capacity to counter terrorism and violent extremism online.

To learn more about how GIFCT approaches and engages tech companies to join, see the explainer video we provide on our website [here](#).

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 supports the tech industry tackle terrorist exploitation of the internet, whilst respecting human rights. It is an independent public-private partnership backed by the United Nations Counter-Terrorism Executive Directorate.

## Mentorship with Tech Against Terrorism

In its mentorship program, Tech Against Terrorism supports tech companies in meeting GIFCT's membership criteria through a comprehensive capacity-building program. This program includes elements of policy and practical support for strengthening counterterrorism efforts and knowledge sharing regarding the state of the threat. Human rights, transparency, and accountability are also at the core of the mentorship program in supporting tech companies' online counterterrorism response. To advance those goals, Tech Against Terrorism supports mentee platforms with transparency reporting as well as understanding how to embed human rights considerations with online counterterrorism efforts.

## Assessment Criteria

Tech Against Terrorism conducts in-depth policy reviews and directly engages with mentee platforms to help assess whether companies meet GIFCT membership criteria.

## 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

In 2022, the following companies underwent mentorship with Tech Against Terrorism, were assessed by GIFCT, and accepted as GIFCT members:

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

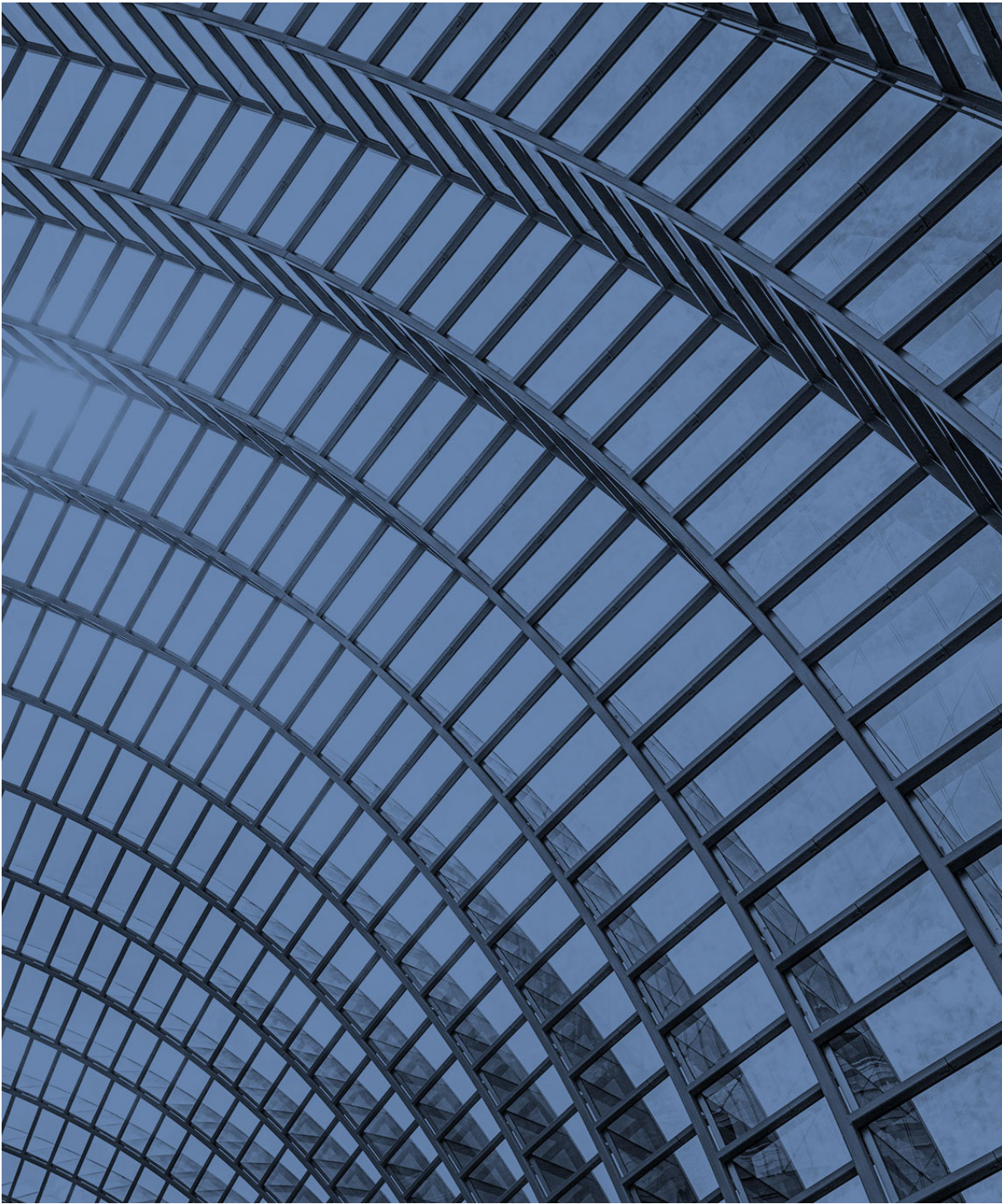
For a detailed overview of how the mentorship program works, please see the Tech Against Terrorism mentorship guide [here](#).

## Introducing the Annual Membership Criteria Review

In 2022, GIFCT and Tech Against Terrorism expanded and enhanced support to existing members and introduced a yearly review process of current GIFCT member companies to ensure they were continuing to uphold and fulfill the membership criteria. As tech companies' counterterrorism frameworks continuously evolve in response to the fast-changing threat landscape, this annual review process focused on policy updates introduced by member platforms since they joined GIFCT to ensure counterterrorism policies remain aligned with GIFCT membership criteria - in particular with regard to transparency and human rights commitments. The addition of an annual review is in line with recommendations made in GIFCT's HRIA in 2021.

For this first year of implementing this review, the Tech Against Terrorism team reviewed and assessed the publicly available policies of all 18 GIFCT members that had joined prior to 2022, including the

founding members. Platforms that joined GIFCT in 2022 will be included in the annual review process beginning in 2023. In addition to assessing baseline compliance with GIFCT's membership criteria, the compliance review also allowed Tech Against Terrorism to support member companies in further strengthening their transparency and human rights commitments with bespoke recommendations. These recommendations are voluntary and meant to inform tech companies' understanding of best practices about transparency reporting and operationalization of their human rights commitment.





## GIFCT's Commitment to Human Rights

Respect for universal and fundamental human rights is central to how GIFCT works to fulfill its mission to prevent terrorist and violent extremist exploitation of digital platforms. That is why in 2020, during the first year operating as an independent organization, GIFCT's leadership team took early and decisive action to build respect for human rights into the blueprint of GIFCT's ethos and operations.

### Progress on the Human Rights Impact Assessment

In the fall of 2020, GIFCT sought advice from a diverse and global range of stakeholders - including member companies, members of our IAC, and participants in our Transparency Working Group, about how best to proactively incorporate human rights considerations in GIFCT's workstreams.

Based on early consultations and recommendations, in December 2020, GIFCT commissioned the nonprofit Business for Social Responsibility (BSR) to conduct a [Human Rights Impact Assessment \(HRIA\) of GIFCT](#). The assessment was designed to be forward-looking, to act as a useful tool for thinking proactively about human rights at the nexus of terrorism and technology. The scope of this assessment was focused on GIFCT and not the actions or policies of individual GIFCT member companies (member companies are held to baseline criteria of public commitment to human rights for GIFCT membership; however, GIFCT respects that companies maintain their own policies and practices depending on the form and function of their platforms).

GIFCT published the HRIA in July 2021, making transparent a set of recommendations based on the UN Guiding Principles on Business and Human Rights to ground GIFCT's work. GIFCT's Executive Director at the time gave [a formal response](#) to the publication and BSR published a [blog post](#) on the effort.

The HRIA identified 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 assessment noted 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 develops and enables cross-platform tools and communications with its members, the HRIA recommended that GIFCT maintain a system for human rights due diligence - embedding human rights across its activities and engaging with affected stakeholders.

GIFCT continues to track its progress along the 47 concrete recommendations made in the HRIA, which contains suggestions spanning our membership processes, organizational governance, programs, and tooling. In 2021 and 2022, GIFCT embedded additional human rights due diligence in its membership process, transparency, and programmatic priorities. Detailed progress across specific recommendations is tracked in GIFCT's 2022 Transparency Report.

The HRIA has demonstrated its utility as a roadmap of recommendations to work toward. Embedding

human rights into policies and practices will always be a work in progress and consultations with GIFCT's global multi-stakeholder community have been key to continue soliciting feedback regarding particular aspects of our progress in this area. In February 2022, GIFCT held a meeting coordinated with BSR and our multi-stakeholder community to discuss our progress on the assessment's recommendations to date. Feedback has continued throughout the year, feeding into a formal GIFCT Human Rights Policy.

### **GIFCT Human Rights Policy**

GIFCT has now implemented a key HRIA recommendation for GIFCT by establishing a public [Human Rights Policy](#). This policy expresses GIFCT's commitment to human rights, describes our intention to embed respect for human rights across GIFCT processes, programming, and operations, and acknowledges our responsibility to address potential adverse human rights impacts that may arise from our work. This policy articulates how GIFCT will respect human rights as an independent organization and applies to all our activities, including how we aim to support the counterterrorism practices of our member companies, stakeholders, and the broader field.

GIFCT's approach to human rights is based on the UNGPs. This policy makes clear that the participation of both governments and companies in GIFCT means that both the state duty to protect human rights and the corporate responsibility to respect human rights have direct relevance for our work. This Human Rights Policy exists alongside baseline public human rights commitments that GIFCT requires all member companies to make. GIFCT's membership criteria constitute a key point of human rights guidance that GIFCT provides to members, and human rights considerations are embedded within the mentorship process carried out by our partners at Tech Against Terrorism that GIFCT sponsors.

Consistent with best practices and the expectations of the UNGPs, this policy was approved by GIFCT's Operating Board, was informed by consultation with stakeholders, and has been made publicly available.

### **Human Rights Progress Across GIFCT**

While the Transparency Report tracks specific progress across the HRIA's 47 recommendations, GIFCT includes broad updates within our Annual Report that have specific impacts on our commitment to human rights.

### **GIFCT Mentorship and Membership**

In 2022, GIFCT worked with our partners at Tech Against Terrorism to develop a proactive and reactive annual review process for members so that each company receives support to ensure there is no backsliding with respect to GIFCT membership criteria. A reactive review process is now in place so that an analysis can be carried out if stakeholders or partners flag a potential concern that a member has backslid against its commitments (including potential violation of human rights). In a related vein, to facilitate GIFCT's review and recommendation of a company for membership, GIFCT has piloted an extra layer of human rights review with BSR for prospective member companies.

## The Hash-Sharing Database

At the beginning of 2021, GIFCT [launched an effort](#) to engage a wide range of experts on how best GIFCT could expand the taxonomy that determines what hashed content qualifies for inclusion in our hash-sharing database beyond the United Nations Security Council's Consolidated Sanctions list and live-stream footage from mass violent attacks that have activated GIFCT's [CIP](#). Expanding the taxonomy of terrorist content means GIFCT can address the Islamist extremist bias that exists in the larger counterterrorism field and requires us to continue to remain diligent in reviewing potential impacts on human rights, ranging from other potential biases to over-censorship.

The result of this effort was a [Taxonomy Report](#) with recommendations from global experts. It led GIFCT to propose new categories of hashes to be added to the database that more effectively address the latest types of terrorist and violent extremist content spreading online while ensuring an accountable approach that was globally informed, proportionate, and manageable by GIFCT. These included hashes from attacker manifestos, terrorist and violent extremist publications, and URLs of terrorist content identified through a partnership with Tech Against Terrorism's TCAP. This year began the implementation of these expansions.

Paramount in GIFCT's work to enhance the hash-sharing database is also the effort to ensure the quality of the database and that hashes included follow the refined parameters of our taxonomy. Significantly, this year GIFCT worked with member companies to ensure GIFCT gained better visibility into how members use the database as well as measuring and analyzing its composition as part of its management and oversight. GIFCT also introduced a robust but simple human rights assessment tool for all new technical initiatives and developments to ensure they respect human rights by design. Having institutionalized proactive check points to ask specific questions about human rights considerations while reviewing partnerships and projects will allow us to grow programs consciously

More about GIFCT's hash-sharing database can be found in this report's section on GIFCT's Strategic Pillar: Prevent. Further information about GIFCT's CIP can be found in the section on GIFCT's Strategic Pillar: Respond.

## Working Groups

Based on detailed formal feedback from its IAC about Working Groups and detailed further in the section on GIFCT Working Groups, GIFCT incorporated a series of human rights recommendations when kicking off Year 3 of GIFCT Working Groups this fall. In line with this feedback, GIFCT worked to improve and enhance transparency within the Working Group selection processes and communication pathways for participants, and launched a [Principles and Guidelines document](#) for Working Group participants to ensure better oversight and equity in voice. GIFCT has also proactively looked to increase the diversity of participants and consciously include advocacy-focused participants in each group, including consulting with the Christchurch Call Advisory Network (CCAN) for strategic participant inclusion from their network.<sup>1</sup>

In addition to IAC feedback, Working Groups continue to produce outputs and recommendations

.....  
<sup>1</sup> GIFCT held two positions in each Working Group for CCAN participants.

specific to human rights. Outputs from Year 2 Working Groups, produced in the Summer of 2022, tackled specific human rights questions related to crisis response, transparency, and data preservation.

- Crisis Response Working Group Year 2 Outputs:
  - › Mapping the lifecycle of an Incident and embedding a human rights approach
  - › Engaging civil society participants in GIFCT's crisis response tabletop exercise (this work also guided GIFCT in developing multi-stakeholder debrief sessions in the aftermath of activating the CIP)
  - › Enhancing transparency around advances in GIFCT's IRF
- Transparency Working Group Year 2 Outputs:
  - › Compiling cross-sector transparency reporting best practices
  - › Collating and comparing government legislation on transparency reporting requirements for tech companies
  - › Reviewing empirical evidence on how researchers have attempted to analyze content-sharing algorithms
- Technical Approaches Working Group Year 2 Outputs:
  - › Examining reporting, removal processes, and vaulting content in moderation practices alongside human rights considerations
  - › Probing underlying questions at the intersection of recommender algorithms and terrorist and violent extremist content

Over the next three to five years, GIFCT will remain committed to pursuing the recommendations given in the HRIA. Like our work to counter terrorism and violent extremism, GIFCT views the advancement of human rights approaches and practices as something requiring continual iteration and evolution. This will include approaches to enhance the transparency of the hash-sharing database as well as reviewing GIFCT practices and governance structures.



## GIFCT Working Groups

GIFCT's Working Groups aim to further GIFCT's mission of preventing terrorists and violent extremists from exploiting digital platforms. Each year, Working Group themes function across GIFCT's Prevent, Respond, and Learn pillars to contribute to GIFCT's objective of providing a space for understanding and expertise on salient issues related to countering terrorism and violent extremism online. In particular, Working Group Outputs aim to evolve GIFCT policies and practices, as well as contribute to growing GIFCT's capacities to deliver guidance and solutions to technology companies and counterterrorism and counter-extremism practitioners.

In 2020, GIFCT began convening a series of Working Groups to focus on critical themes related to countering terrorism and violent extremism online. GIFCT Working Groups bring together experts from diverse stakeholder groups, geographies, and disciplines to offer advice on specific thematic areas and deliver on targeted substantive projects. Each year GIFCT presents Working Groups' output, updates their themes and focus areas, and allows new participants to join. Working Group participants collaborate with GIFCT to prepare strategic work plans and outline objectives, goals, strategies, deliverables, and timelines.

### Conclusion of Year 2 GIFCT Working Groups: 2021 - 2022

From August 2021 to July 2022, GIFCT convened five Working Groups comprised of 180 experts and practitioners from across the world, holding around 60 meetings with representatives from tech companies (17%), governments and international governing bodies (26%), and civil society organizations (57%). The five Working Groups (1) refined crisis response protocols, (2) pursued innovations in positive interventions and strategic communications, (3) explored new technical solutions related to algorithms and artificial intelligence, (4) examined how to enhance transparency implementation, and (5) studied legal frameworks addressing data privacy and terrorist definitions.

At GIFCT's Global Summit in July 2022, each Working Group presented their year-long efforts, providing authoritative information on the current dynamics of each issue area and next steps in identifying and deploying solutions. Output from each Working Group is outlined and linked below.

#### Crisis Response Working Group

GIFCT's Crisis Response Working Group (CRWG) fed directly into improving and refining GIFCT's own [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 Tabletops 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 counterterrorism 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 CVE and counterterrorism 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, 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 Call 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.

### 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 legislation 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.

Outputs from Working Groups are made public on [GIFCT's website](#).

### Launch of Year 3 GIFCT Working Groups: 2022 - 2023

This fall, GIFCT ran an open and public application process for Year 3 Working Groups (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 worked closely with the Independent Advisory Committee to include their feedback in restructuring the overall Working Group themes and format ranging from re-aligning this year's themes with current cross-sector priorities as well as GIFCT's larger mission, along with developing better internal structures to guide Working Group participants. 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 (14%), academia (20.8%) or practitioners (24.2%), 18.4% representing governments, and 22.7% in tech.

Beginning in November 2022, five new GIFCT Working Groups have sharpened their focus to address the following themes respectively:

- 1. Refining Incident Response: Building Nuance and Evaluation Frameworks** - Previous years of GIFCT's Crisis Response Working Groups found that further refinement is needed for government, tech, and GIFCT efforts to identify and define (1) what constitutes a terrorist or violent extremist attack (specifically regarding edge cases) and (2) what "Terrorist and Violent Extremist Content" means in these contexts. This Working Group will continue questioning transparency, evaluation metrics, and data preservation protocols within wider crisis response efforts.
- 2. Blue Teaming Alternative Platforms for Positive Intervention** - A gap in the online intervention space is that PVE/CVE practitioners tend to use only three to four larger platforms for all counter-extremism efforts and practitioner work. To counter the cross-platform threat and provide solutions for real change across a wider number of platforms, this GIFCT Working Group will focus on highlighting alternative platforms to discuss how their platform operates and Blue Team where positive interventions, risk mitigation tactics, and friction-building strategies could be implemented. The output will be a tailored playbook of approaches to further PVE/CVE efforts on a wider diversity of platforms. It will help activists in their own efforts to challenge hate and extremism online and foster wider civil society-tech company partnerships.
- 3. Red Teaming: Assessing Threat and Safety by Design** - Looking at how the tech landscape is evolving in the next two to five years, this GIFCT Working Group aims to identify, understand, and scrutinize risk mitigation aspects of newer parts of the tech stack. Possible areas of focus include Decentralized-Web, Dating Services, E-Pay, storage, 3D printing, and E2EE. The Red Teaming format will allow the Working Group to identify what expected threats in terrorism and violent extremism might look like and what solutions and mitigations could or should be put in place (with human rights as a primary consideration). The outputs will aim to identify design principles for key components of trust and safety systems that seek to prevent terrorist and violent extremists from exploiting platforms when developing new technology. The Working Group will explore questions around technical safeguards, oversight, and best practices that are needed to ensure safety by design and protection of human rights while member companies carry out tools-based internal operations.
- 4. Frameworks for Meaningful Transparency** - Building off of the previous Transparency Working Group output on [global assessment frameworks](#) funded by GIFCT and produced by Dr. Courtney Radsch, this wider piece of multi-stakeholder work aims to establish a framework for transparency reporting. This includes a mapping of what meaningful transparency means to different key stakeholders on the topic of terrorism and violent extremism and what third-party oversight models might look like.



## 5. Legal Frameworks: Animated Explainers on Definitions of Terrorism and Violent Extremism

- This Working Group has committed to developing a series of short explanatory animations to support the [research on applying terrorist definitions](#) led by Dr. Katy Vaughn in Year 2's LFWG and the recently launched GIFCT [Definitions and Principles Framework Site](#). This will provide other mediums for understanding the pros, cons, and risks around definitions and government lists.

GIFCT is also funding an overarching piece of research to address the question of user journeys through our academic research arm, GNET. The research aims to shed light on the process by which individuals find and join online communities, engage with content and individuals, and take actions motivated by their experience in the online community. The aggregate report will offer a novel and holistic picture of online radicalization processes, with a particular focus on the presence (or lack there of) of algorithmic amplification of terrorist and violent extremist content.



## GIFCT Strategic Pillar: Prevent

GIFCT's mission is to prevent terrorists and violent extremists from exploiting digital platforms and help GIFCT members protect users of the internet.

Our team of technical experts is the focal point for GIFCT's Strategic Prevent Pillar - the aim of which is to equip digital platforms and civil society groups with awareness, knowledge, and technical tools to develop sustainable programs to disrupt terrorist and violent extremist activity online. The threat of terrorism and violent extremism continues to evolve dynamically. Similarly, the technology landscape is evolving rapidly as new technology emerges and existing technologies are repurposed and reused in novel ways. The technical solutions GIFCT develops must do more than address the status quo, they must evolve to keep pace with the changing landscape.

GIFCT continues to develop cross-platform technical solutions that strengthen how our members can combat attempts to exploit their platforms and improve the health of the broader online ecosystem. Online, terrorism and violent extremism are cross-platform in nature with terrorist exploitation of the internet often involving multiple platforms and types of online services. GIFCT's technical solutions are designed to be cross-platform to address this reality. These technical solutions strengthen GIFCT member's individual efforts while further tackling how bad actors often migrate across platforms (even in single attempts to exploit the internet). With this guiding objective, GIFCT's technology team develops technical products that are designed to multiply the impact of our collective efforts.

Significantly, how GIFCT develops these capabilities is just as important as what GIFCT develops. A human rights-based approach is at the core of GIFCT's mission, and as such, we design, test and build considering the rights that the systems we develop will impact as well as whose rights will be impacted at every phase of development. Ultimately, the aim is to contribute to building a stronger, safer, and more secure open internet for all users.

### GIFCT's Hash-Sharing Database

GIFCT's hash-sharing database is currently our leading cross-platform technical solution that allows members to identify if and where terrorists or violent extremists are attempting to exploit their respective platforms. The hash-sharing database is a shared, safe, and secure industry database of hashes of known content produced by terrorist entities. Hashes are numerical representations or digital fingerprints of content, such as images, videos or PDFs, that cannot be reverse-engineered to recreate the content itself. Hashes can be either "cryptographic" or "locality sensitive." Cryptographic hashes are for "exact matching," so if one pixel in an image is changed, the hash will be completely different. Locality-sensitive hashes help us match visually similar images. To learn more about how the hash-sharing database works, visit GIFCT's website [here](#).

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. For nuanced metrics on the amount of hashed content corresponding to the taxonomy of the Hash-Sharing Database please see our Transparency Report.



To ensure that GIFCT keeps pace with the evolving terrorist threat and adds value to each member, we continually evolve the hash-sharing database so that a greater range of different digital platforms can exchange signal on known terrorist and violent extremist content. This ensures that the database provides a high-quality signal to identify where terrorist and violent extremist activity may be taking place on member platforms that violate their policies and terms of service.

### **Governance of GIFCT's Hash-Sharing Database**

As part of establishing GIFCT as an independent nonprofit organization, this year we completed the process to assume management of the legal agreements and access to the hash-sharing database with its members, which was formerly managed by Facebook. As a result, GIFCT members have now signed up for an updated information-sharing agreement that ensures data is appropriately protected and secured at all phases of its life cycle and in line with the latest regulations and industry-standard best practices.

As part of our management practices, GIFCT has developed a [code of conduct](#) providing members with guidelines for use of the hash-sharing database. This code of conduct was developed to proactively establish best practices and clear parameters in the event that misuse took place. While such misuse has not taken place to date, it is important GIFCT has a code and remedies for misuse established to safeguard the important efforts the organization and its members have put into practice. With this in mind, GIFCT has laid out a series of consequences for misuse which range from formal requests for corrections of an error made in the database to revocation of GIFCT membership and further penalties to hold those accountable (should this unlikely scenario take place). These documents along with GIFCT's regular transparency reports are key elements of our strategy to ensure that the database is operating in accordance with the highest ethical standards and the [United Nations Guiding Principles on Business and Human Rights \(UNGPs\)](#).

### **Taxonomy Expansions for GIFCT's Hash-Sharing Database**

The hash-sharing database began by gathering hashes from GIFCT members relating to content produced by terrorist entities on the UN Security Council's Consolidated Sanctions List. In 2019, that expanded to include perpetrator-produced content relating to mass violence attacks, in coordination with our Content Incident Protocol. In 2021, GIFCT published a [Taxonomy Report](#) with recommendations from global experts and GIFCT member companies on how best to expand the taxonomy further and effectively address current trends in terrorist and violent extremist content spreading online.

In line with this report, in 2022, GIFCT enabled and added hashes of violent extremist and terrorist attacker manifestos compiled in coordination with global expert academics. GIFCT also completed the technical work to add hashes from Tech Against Terrorism of URLs from the [TCAP](#) tied to entities on the United Nations Security Council's Consolidated Sanctions list as well as perpetrator-produced content shared as part of an offline attack that activates GIFCT's Content Incident and CIP. Hashing URLs from TCAP is an important first step towards being able to address [outlinking](#) from GIFCT member platforms to terrorist content hosted elsewhere online. In this case, TCAP provides GIFCT

with the hashes that GIFCT then adds to the database.

As part of this taxonomy expansion work, GIFCT has also built new technical capabilities to enable the hashing of 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, beyond those hosting recorded image and video content, to harness GIFCT's collective capacity in line with their respective policies and enforcement practices. Hashing attacker manifestos enables GIFCT and our members to address risks associated with critical terrorist incidents more completely and responsively, while also better countering the long tail of inspiration and incitement to violence that these manifestos create.

## Transparency

This year, in line with our core values and commitment to transparency, GIFCT sought to meaningfully enhance the information and insights we can share about our work, particularly for the hash-sharing database. GIFCT delayed the release of the [2022 Transparency Report](#) from our normal publication date in July until the end of year in conjunction with our Annual Report to enable us to invest more time and effort to accomplish this. In this year's Transparency Report, in addition to standard metrics GIFCT has previously provided about the current volume and composition of the database, we have further provided:

- 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 that has now been concluded);
- 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; and
- Delivery of findings from GIFCT's first sampling and review exercise of hashes to ensure the quality and reliability of the hash-sharing database for members.

## New Technology

### Developing Terrorist and Violent Extremist Classifiers

In 2021, following consultation with GIFCT members, GIFCT's Tech Approaches Working Group identified a range of capability gaps facing smaller platforms. One of these gaps was a system to classify multimedia content as terrorist or violent extremist in a way that is contextualized and explainable, and provides a degree of confidence to content moderators. After an open request for proposals process, GIFCT has now commissioned a project with Faculty.AI to develop tools that can be used to inform human content moderators' decisions about terrorist and violent extremist content in line with a respective platform's policies and help prioritize this content's review. This project will build on Faculty's existing expertise and technology in this area - expanding existing capabilities to

address the full range of violent extremist threats in a way that protects user privacy and is conscious of the cost of running these large models for small companies. The project has begun the initial phase of development and is due for delivery in 2023.

Developing systems like this responsibly is fundamental to GIFCT's mission. GIFCT and Faculty.AI have committed to developing this technology following internationally recognized human rights and standards, in line with GIFCT's newly established human rights assessment for all new technical initiatives and developments to ensure they respect human rights by design. This commitment is established through a range of internal policies and practices including:

- Undertaking GIFCT's work in adherence with the UNGPs, in accordance with our values and international law;
- Seeking to avoid contributing to or causing negative human rights impacts through GIFCT's business or activities;
- Seeking to prevent negative human rights impacts that relate to GIFCT's work, services, and products (or their implementation);
- Proactively and continually monitoring GIFCT's business, activities, and programs for human rights impacts and taking appropriate, timely action in response to any risks identified; and
- Continuing to actively support the promotion of human rights within GIFCT's business and professional networks.

## Future Plans

In 2023, to further our mission and the key objective of preventing terrorists and violent extremists from exploiting digital platforms, GIFCT aims to ensure our products and programs have wide reaching benefits for all our members. GIFCT members have an increasingly diverse range of products and services not only focused on user-generated content, but also digital marketplaces, entertainment, and gaming (among others). To address the future of an even further diversified membership and respond to a changing dynamic set of threats and opportunities, GIFCT must diversify the value we add to members and society. By building baseline capabilities at a trial or prototype level that respond directly to the needs of members and help identify new areas that we can positively impact members, we can improve efficiency and effectiveness across the tech sector.

Privacy Enhancing Technologies<sup>2</sup> will be important to GIFCT's future and this is one area we expect to develop and invest in, including trials of new systems that respond directly to member companies' needs.

As GIFCT seeks new avenues to build additional value, we must also strengthen and enhance the hash-sharing database. In 2023 this will focus on ensuring all members can take full advantage of

.....  
 2 Kent Seamons, "Privacy-Enhancing Technologies," in *Modern Socio-Technical Perspectives on Privacy*, eds. Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Cham: Springer, 2022), 149-170, [https://doi.org/10.1007/978-3-030-82786-1\\_8](https://doi.org/10.1007/978-3-030-82786-1_8).

all aspects of the system. This will include improving the ease of integration and looking to solutions such as Meta’s Hasher Matcher Actioner tool. This will also include testing tools in development to analyze their effectiveness with the Hash Sharing Database, such as Jigsaw and Tech Against Terrorism’s upcoming tool, being built in support of and with support from GIFCT. GIFCT looks to test and support a set of complementary and freely available tools to support member’s content moderation efforts that help prevent terrorists and violent extremists from exploiting a range of different types of digital platforms.

Finally, across all of these lines of effort, GIFCT must take an evidence-based data-driven approach to our work. By monitoring and measuring the impact of GIFCT’s cross-platform solutions and services, combined with evaluating the needs of our different stakeholders and further investment in transparency across all our systems, GIFCT can ensure the sustainable and robust delivery of our mission.

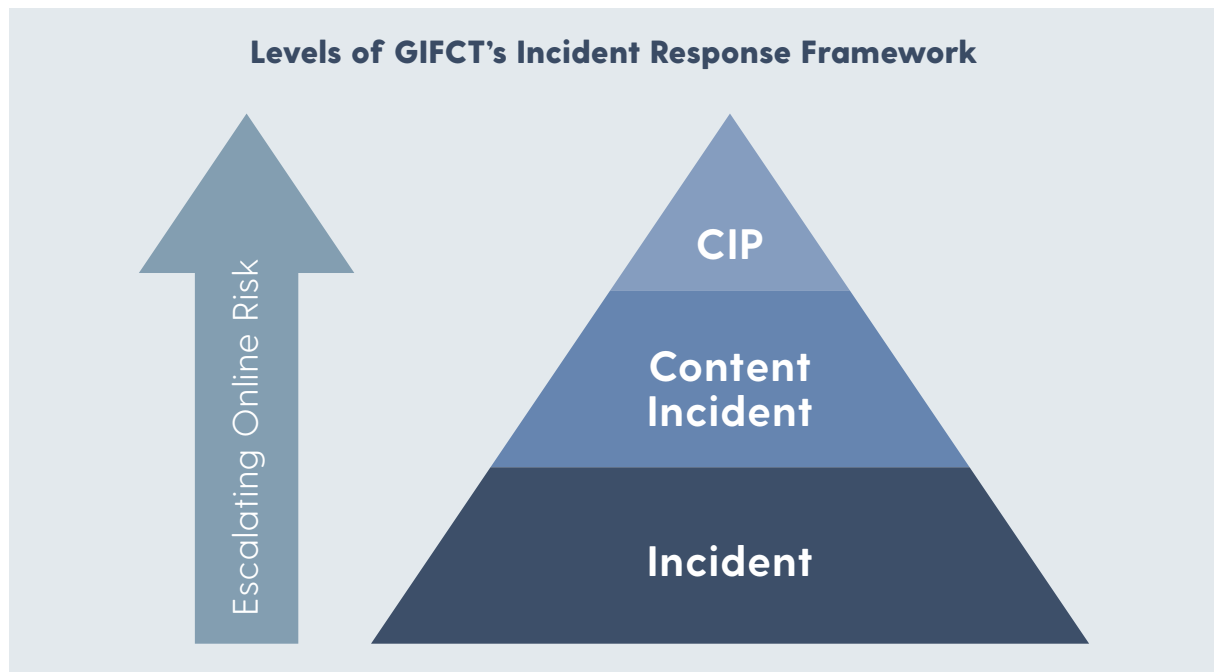


## GIFCT Strategic Pillar: Respond

### GIFCT's Incident Response Framework

GIFCT's Incident Response Framework (IRF) is the set of protocols and processes in place to guide how GIFCT and our members respond quickly, effectively and in a coordinated manner to terrorist and mass violence events with a significant online aspect.

GIFCT's IRF contains levels of response that reflect the severity of online exploitation related to the offline terrorist or violent extremist event and the response GIFCT and its members carry out. These Levels are Incident, Content Incident, and Content Incident Protocol (CIP).



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 overall goals for GIFCT's IRF are to increase the pace of industry awareness of and response to terrorist and violent extremist content circulating online that relates to an offline terrorist event, decrease terrorist and violent extremist content circulating on digital platforms, and enhance communications between industry, government, and civil society regarding the response to a terrorist or violent extremist event.

GIFCT's role is to ensure that member companies have the ability to respond in a coordinated manner to terrorist events with a significant online aspect, particularly where perpetrator-produced content is circulated as part of an event, while preserving their independence to act according to their respective policies and terms of service. GIFCT continues to identify ways to strengthen and expand our situational awareness capabilities in order to receive alerts about an unfolding event as quickly as possible within the operational parameters of our staffing and resourcing.

## IRF Activations in 2022

Since the initial development of the IRF in 2019, GIFCT and our members have initiated communications to share situational awareness and information in response to over **306** terrorist or mass violence events and significant online terrorist developments in **44** countries across **6** continents. **11** of these events activated various levels of the IRF because of their significant online dimensions.

In 2022, GIFCT activated the Incident level of the IRF three times, the Content Incident level of the IRF once (in response to the attack in Udaipur, India) and the CIP level of the IRF twice (in response to the attacks in Buffalo, New York and Memphis, Tennessee, United States).



## Implementing New Elements to GIFCT's Incident Response Framework in 2022

### Multi-Stakeholder Debriefs

In 2021, the Year 1 Crisis Response Working Group developed a recommended approach for cross-sector debriefs following the activation of the CIP. GIFCT adopted these recommendations and built into the IRF a multi-stakeholder debriefing process to ensure that our stakeholders are informed of the context and events that prompted the activation of the CIP as well as the actions carried out as a result. A key part of this process is receiving feedback from members, as well as civil society and governments, on parts of the IRF that are delivering well, those areas that face challenges, and possible solutions to consider.

During 2022 GIFCT conducted two debriefs following the two CIP activations in response to the attacks in Buffalo and Memphis. Through the debriefs, members highlighted the need for improved situational awareness and information flow among themselves and GIFCT - a priority capacity that GIFCT continues to work on to expand and enhance. Over the last year, GIFCT has developed and deployed new operational systems that help (in as close to real-time as possible) identify instances when an offline violent event is taking place in which the perpetrators or accomplices of the attack are attempting to exploit digital platforms as part of their violence. Going into 2023, GIFCT will continue to implement these systems into its framework and mechanisms for communicating with members.

### Expanding Capabilities

Stemming the spread of terrorist and violent extremist content online is GIFCT's northstar, and as our IRF illustrates, is critical in our efforts to respond to a terrorist or mass violence attack. Expansions to GIFCT's database enabling the hashing of attacker manifestos allow us to address a greater range of online threats such as the manifestos published by the attackers in Buffalo, New York and Bratislava, Slovakia. This year GIFCT also developed the initial capability to hash URLs identified by our partner Tech Against Terrorism where specific terrorist content exists. Although not yet fully populated with these hashes, this capability to hash URLs will enhance the ability of GIFCT and member companies to address attempts to spread perpetrator-produced live-streams when shared on a member platform as a URL (where the video is being hosted on a non-GIFCT member platform).

In addition to implementing and refining these additional categories of hashes to GIFCT's hash-sharing database and increasing our technical capacity for situational awareness that alerts us to developing attacks, GIFCT is committed to carrying out a range of efforts that will strengthen our response when the IRF is activated.

### Testing GIFCT's Readiness and Response

Throughout the year, GIFCT works to test and finetune its protocols, readiness, and systems so that when responding to an attack, our member companies (and GIFCT itself) are positioned to respond quickly and effectively. Since 2019, GIFCT has convened and participated in exercises to test our

protocols in order to identify where gaps may exist, as well as to establish understandings and expectations for how GIFCT's IRF works in relationship to other international crisis response protocols, including the EU Crisis Protocol and the Christchurch Call Crisis Response Protocol.

In 2022, GIFCT conducted three tabletop exercises to test different aspects of the IRF. In the first, GIFCT worked to understand how an attack and our response can impact the human rights of online users, victims, and others. In the second test, GIFCT convened our member companies to evaluate the current state of our centralized communications mechanism. In the third assessment, GIFCT tested our internal protocols since updating based on responses to incidents and the exercises earlier in the year, improving our readiness to respond quickly and effectively.

Engaging with GIFCT's stakeholders from government, civil society, and tech is both a responsibility and an opportunity to learn and improve. GIFCT will continue to meet with stakeholders to understand how they are impacted by violent attacks that prompt GIFCT and its members to activate the IRF in order to gain greater knowledge on how we can share pertinent information that does not limit GIFCT's capabilities to maintain our priority of supporting members to respond to online dimensions of the attack. GIFCT will continue to convene our stakeholders and members to test our protocols through exercises and evaluate our systems through our Incident Response Working Group. This year the group will include a focus on how to evaluate the impact of the IRF and other incident response protocols as well as addressing other areas for improvement as identified in the Crisis Response Working Group's 2022 [Protocol Mapping](#).

GIFCT is grateful to our members for their commitment and determination in their response to the tragedies that we sadly had to respond to this year and our stakeholders for providing information and feedback through the first implementations of the debriefing process. In just over three years, GIFCT has made important progress in our collective efforts, and we are eager to continue to improve in this area.



## GIFCT Strategic Pillar: Learn

### Knowledge Sharing and Expanding Access to Nuanced Information

Action-oriented learning is the third strategic pillar of GIFCT's work. GIFCT's goal is to enable the exchange of information about terrorist and violent extremist exploitation of the internet across sectors while also advancing a broader understanding of the evolution of terrorist and violent extremist activity online. This includes ensuring more is understood about the intersection between online and offline activities, and the current adversarial threat landscape today. GIFCT advances learning through (1) GIFCT Working Groups, (2) GIFCT's academic arm - the [Global Network on Extremism and Technology \(GNET\)](#) - and (3) our collaborative knowledge-sharing events with [Tech Against Terrorism](#). GIFCT also develops resources based on feedback from these workstreams to ensure members and wider stakeholders can easily find the information they need to make informed decisions to better counter terrorism and violent extremism online.

### GIFCT Resources

#### Definitions and Principles Framework

Based on Operating Board and IAC feedback in August 2021, GIFCT began developing resources to help guide tech companies in better understanding formal definitions of terrorism and violent extremism as well as the government lists associated with these definitions. As a result, GIFCT's Programming Team developed the [Definitions and Principles Framework](#) microsite to assist tech companies in developing (or making more robust) their external and internal policies and practices for defining and taking action against terrorist and violent extremist content and activities.

The framework provides important resources across four categories:

1. **A global understanding of terrorism** by comparing governments' and international bodies' definitions of terrorism and violent extremism;
2. **A behavioral understanding of terrorism** by comparing the signals used to legally define and proscribe terrorist and violent extremist individuals, activities, and groups;
3. **Understanding context to apply definitions** by highlighting globally relevant themes on how terrorism and violent extremism manifests and how (via actionable research from GNET) it relates to technology;
4. **Risk Mitigating Designation Lists** by understanding the pros, cons, and risk mitigation strategies to consider when assessing how to apply government terrorist designation lists.

#### Core Partners

GIFCT has two core partners to advance the work under its Strategic Learn Pillar - GNET and Tech Against Terrorism. GIFCT's partnership with GNET in this regard connects GIFCT members to invaluable, action-oriented research by academics and experts from across the globe on some of the most significant issues affecting digital spaces. In parallel, GIFCT's work with Tech Against Terrorism centers on facilitating knowledge sharing among sectors and strengthening situational awareness

and analysis of terrorist and violent extremist activity online.

## GNET

### Conducting & Funding Research

In January 2022, GIFCT began Phase 3 of support to [GNET](#), its academic research network. GNET is 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 also encourages academic contributions from a wide global network of experts and practitioners to ensure insights about adversarial shifts at the nexus of terrorism and technology are more fully understood.

### Insights, Reports and Workshop

#### Insights

In 2022, GNET published 116 insights - short, concise papers that empower experts to probe and explore contentious issues as they relate to violent extremist behaviors and technology. Insight contributors spanned 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, UK, Uruguay, and the United States.*

To align with the UN's [16 Days of Activism Against Gendered Violence](#) (November 25 to December 10), GNET launched in partnership with Monash Gender, Peace and Security a special Insight series entitled, "Gender and Online Violent Extremism." Over the 16 days, contributors provided cutting-edge analysis on three core themes: 1) the perpetration and experience of gendered violence by extremist groups online, 2) the participation of women in online violent extremism, and 3) the experience of female and gender-diverse researchers working in the online extremism space.

### Research Papers & Reports

GNET's longer research papers are focused on terrorist and violent extremist use of technology, and offer actionable findings and practical solutions. In Phase 1 (2018 - 2019), GIFCT supported the Global Research Network on Terrorism and Technology (GRNTT), aimed at developing research and providing policy recommendations around the prevention of terrorist exploitation of technology. Thirteen papers were published by GRNTT in 2019 and can be found [here](#).

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:

- [Manipulating Access To Communication Technology: Government Repression or Counterterrorism?](#) by Fatima Mustafa (Lahore University of Management Sciences)
- [Offline Versus Online Radicalisation: Which is the Bigger Threat?](#) by Dr. Nafees Hamid (ICSR)

and Christina Ariza (King's College London)

- [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)
- [Radical Right Activities in Nusantara's Digital Landscape: A Snapshot](#) by Munira Mustaffa (The Chasseur Group)
- [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
- [Emergent Technologies and Extremists: The DWeb as a New Internet Reality?](#) by Inga Trauthing (International Center for the Study of Radicalisation) and Lorand Bodo

In 2023, GNET will publish reports on counterterrorism law enforcement and social media company engagement, the Islamic State's deplatforming in South Asia, critical dates for extremist groups, gamified copycat terrorist attacks, meme content analysis, feminist cyber security, typologies of extremism within Muslim gaming groups, the webification of Jihadism in Nigeria, and a guide to understanding accelerationism. Additionally, GIFCT is looking forward to supporting GNET in facilitating mental health resources for researchers working in the terrorism and violent extremism space online. GNET has commissioned a project focused on secondary trauma suffered by academics and practitioners who are frequently exposed to disturbing material that will be published in early 2023.

GIFCT is also collaborating with GNET in 2023 to produce a comprehensive report on user journeys. The project will cover a diverse range of terrorist and violent extremist ideologies and platforms. The research aims to shed light on the process by which individuals find and join online communities, engage with content and individuals, and take actions motivated by their experience in the online community. The aggregate report will offer a novel and holistic picture of online radicalization processes, with a particular focus on the presence (or lack there of) of algorithmic amplification of terrorist and violent extremist content.

## **Workshops & Annual Conference**

To further facilitate multi-sector knowledge sharing opportunities and provide expertise to a range of stakeholders, GIFCT supported GNET to work 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. These workshops allowed for robust conversations, tracking adversarial shifts and discussing policy and collaborative solution potentials with academics, tech companies, and government representatives attending various events internationally.

Topics included:

- Far right extremist financing online in Australia (The Lowy Institute)
- Online governance and right-wing extremism: Addressing challenges in proscription and taxonomy (The International Centre for Counter-Terrorism)
- Content Preservation: Exploring options to preserve and provide access for evidentiary social media content (Cyber Threats Research Centre)
- SLAID: Identifying and disrupting serious cyber-enabled crime and online extremism (Cyber Security Cooperative Research Centre)
- The digital billion: South Asia, expanding online, and expanding extremism (Observer Research Foundation)
- Understanding technological resilience of violent extremist networks (Policy Centre for the New South)
- Platform to platform: Online extremists' reactions to terms of service enforcement (Program on Extremism, George Washington University)
- The fusion of offline and online interventions against extremism in the Philippines (The Centre of Excellence for National Security)
- Between broadcasting and hide-and-seek: How extremists use alternative (social) media platforms (The Peace Research Institute Frankfurt)
- Researcher safety online (The International Centre for Counter-Terrorism)
- Assessing (and countering?) the threat of incel violence (Cyber Threats Research Centre)
- OSINT and counter-terrorism: Access to data and (AI) technologies in Africa (Policy Centre for the New South)
- Examining the Buffalo terrorist attack & response (ARC)

In May 2022, GNET launched its [Second Annual Conference](#), which encouraged and facilitated discussions and dialogue between the tech sector and expert academics, civil society representatives, and governments. The conference's five panels brought together a range of diverse topics and saw approximately 300 unique visitors both in person and virtually logging into the various sessions throughout the day.

GIFCT looks forward to continuing its partnership with GNET in order to foster global knowledge sharing and learning in 2023.

## **New Partners with GNET**

GIFCT and GNET feel strongly about collaborating and building solutions with existing networks. In order to ensure further collaboration with experts working on topics related to GIFCT's mission, GNET built formal partnerships with two new networks in 2022.

### **Extremism and Gaming Research Network**

The Extremism and Gaming Research Network (EGRN) 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. GIFCT is a partner organization of EGRN. Set up as a practitioner-led initiative in 2021 to counter new online harms and develop evidence-driven solutions, today EGRN convenes over 50 members, ranging from United Nations agencies to think tanks and private sector organizations. Through its partnerships, EGRN is at the center of emerging research and analysis while impacting policy and tech design. EGRN published four insights with GNET in 2022.

### **Accelerationism Research Consortium**

GIFCT is a partner organization of 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.

ARC is dedicated to the study of accelerationism, an understudied but urgent development in political violence and terrorism. Accelerationism presents a distinct global and transnational security threat to democratic societies that defies conventional counterterrorism mechanisms and programs. Many facets of accelerationist terrorism have been evaluated across various sectors, but until now no concerted effort to collectively address the threat has been conducted. To date, accelerationist terrorism has yet to be analyzed with methodological rigor, nor has its assessment received the necessary financial and institutional support.

ARC works to provide a forum for researchers to generate empirical, objective analysis and research on the topic of accelerationism. Much like GIFCT, this entity aims to bridge the divide among practitioners, researchers, and journalists by establishing cross-industry working groups that will collaboratively discuss, debate, and level-set approaches to understanding and addressing the threat of accelerationist actors and groups. ARC has published 6 insights with GNET in 2022.

## **GIFCT - Tech Against Terrorism Knowledge Sharing Partnerships**

### **E-Learnings**

GIFCT partners with Tech Against Terrorism for monthly e-learnings that are open to global participants across sectors under Chatham House Rules. Launched in March 2021, e-learning events aim to enable 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.

The following nine e-learning events in 2022 had a total of 446 participants join from a variety of sectors across the globe:

- [Global Challenges in Moderating Far-Right Violent Extremism Online](#) (February 24, 2022)
- [The Gamification of Extremism: Extremist Use of Gaming Platforms](#) (March 24, 2022)
- [Audio Content & Detection: Moderation Challenges and Opportunities with Existing Audio Detection Models](#) (April 28, 2022)
- [Moderation online: Beyond content](#) (May 24, 2022)
- [Live-streaming of Terrorist and Violent Extremist Content: Moderation and Crisis Response](#) (June 23, 2022)
- [Misogynist and Male Supremacist Violent Extremism: Evolving National Security Threats](#) (August 18, 2022)
- [Mental Health Tooling and Support for Researchers and Content Moderators](#) (September 29, 2022)
- [Moderation Online: Beyond Content](#) (November 10, 2022)
- [Year in review: Trends in Terrorist and Violent Extremist Use of the Internet and the Online Counterterrorism Response](#) (December 15, 2022)

## Global Workshops

Since its founding in 2017, GIFCT and its partner Tech Against Terrorism have hosted GIFCT Workshops around the world, providing a more formally structured opportunity for tech companies and committed stakeholders to share counterterrorism strategies and knowledge. GIFCT Workshops bring together tech platforms with policy makers, law enforcement, civil society, academic experts, and practitioners to share experiences, best practices, and models for cross-sector collaboration.

To date, these workshops have engaged more than 140 tech companies, 40 NGOs, and 20 government bodies taking place in locations across the globe including:

- Sydney, Australia
- Brussels, Belgium
- Paris, France
- Berlin, Germany
- Accra, Ghana
- Delhi, India



- Jakarta, Indonesia
- Tel Aviv, Israel
- Amman, Jordan
- Abu Dhabi, United Arab Emirates
- London, United Kingdom
- California, United States of America (x2)
- New York, United States of America

### **First Africa Workshop - Terrorism & Violent Extremism in West Africa: Threat Mapping & Solution Building Online**

After a pause on in-person GIFCT Workshops due to the COVID-19 pandemic, GIFCT and Tech Against Terrorism [convened their 14th Workshop on September 7, 2022 in Accra \(Ghana\)](#). Using a hybrid format (in person and virtually) and working in close partnership with the National Cyber Security Center (CSA) in Ghana, this convening focused on the current threat landscape in the West Africa region and its nexus to online activity. Working in partnership with Tech Against Terrorism and GIFCT, the workshop was hosted by the Kofi Annan Foundation in Accra and CSA. Building upon feedback from an [initial virtual workshop hosted last fall](#), West Africa had been highlighted as an under-engaged region for GIFCT. As a result, GIFCT's Programming Team prioritized in-person engagement in this region to ensure a better connection and proactive outreach to regional partners across government, tech, and academia.

The event brought together 97 experts and practitioners from tech, government and civil society in person, with a further 120 joining virtually to develop a multi-stakeholder assessment of the current threat landscape and identify where solutions and further partnerships can be fostered. In particular, representatives from Meta, Paradigm Initiative, Building Blocks for Peace Foundation, Search for Common Ground, and the Tony Blair Institute for Change joined panels alongside GIFCT, Tech Against Terrorism, and CSA. These tech, government, and NGO experts discussed current threat assessments, models for multi-stakeholder collaboration, and resiliency for programs and practitioners working to prevent and counter violent extremism.

This Workshop also marked the first in-person GIFCT-hosted Workshop since becoming an independent nonprofit organization in 2020. GIFCT looks forward to continuing monthly e-learnings and in-person regional workshops in 2023.

## GIFCT 2022 Financials

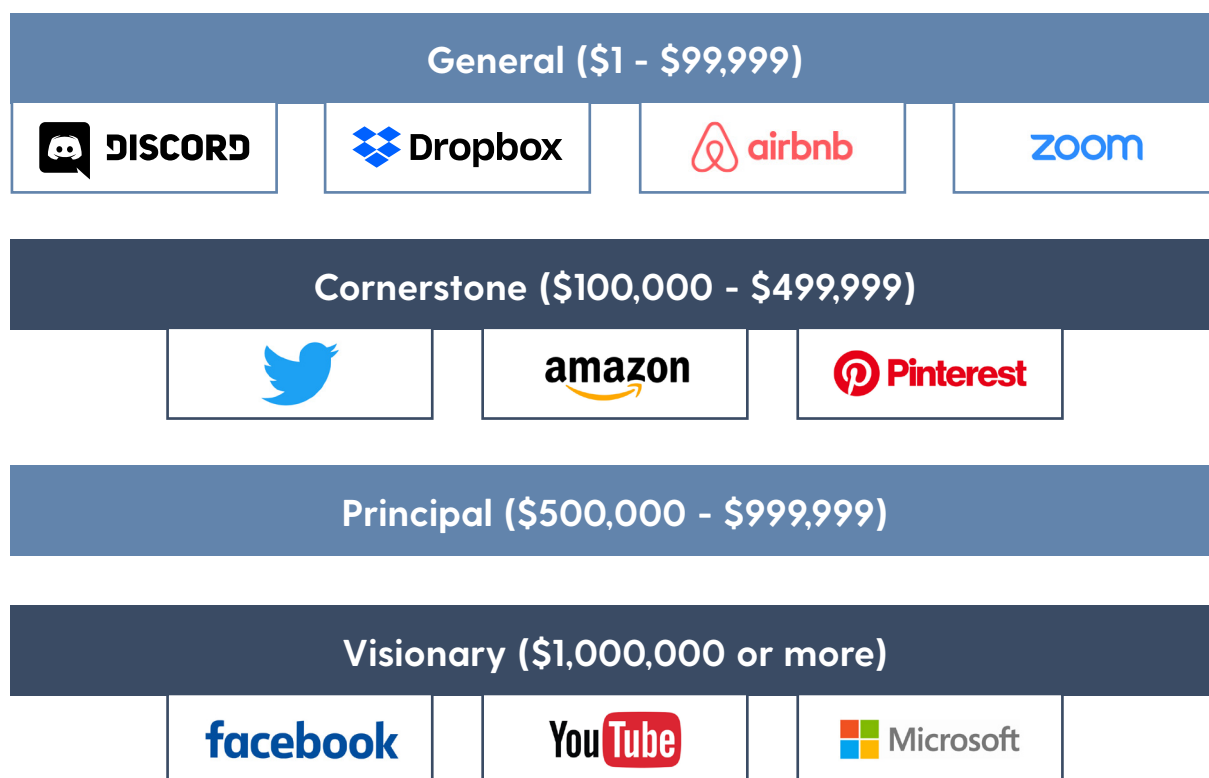
### Support and Contributions

At the end of last year, GIFCT introduced a suggested tiered membership donation framework to expand financial contributions beyond its four founding member companies (Facebook, Microsoft, Twitter and YouTube) that make up GIFCT's Operating Board. 2022 is the first year operationalizing this structured framework to guide how GIFCT grows and diversifies contributions from those member companies able to do so. This framework guides suggested contributions based on company revenue and can be used going forward as part of a broader process to diversify our Operating Board.

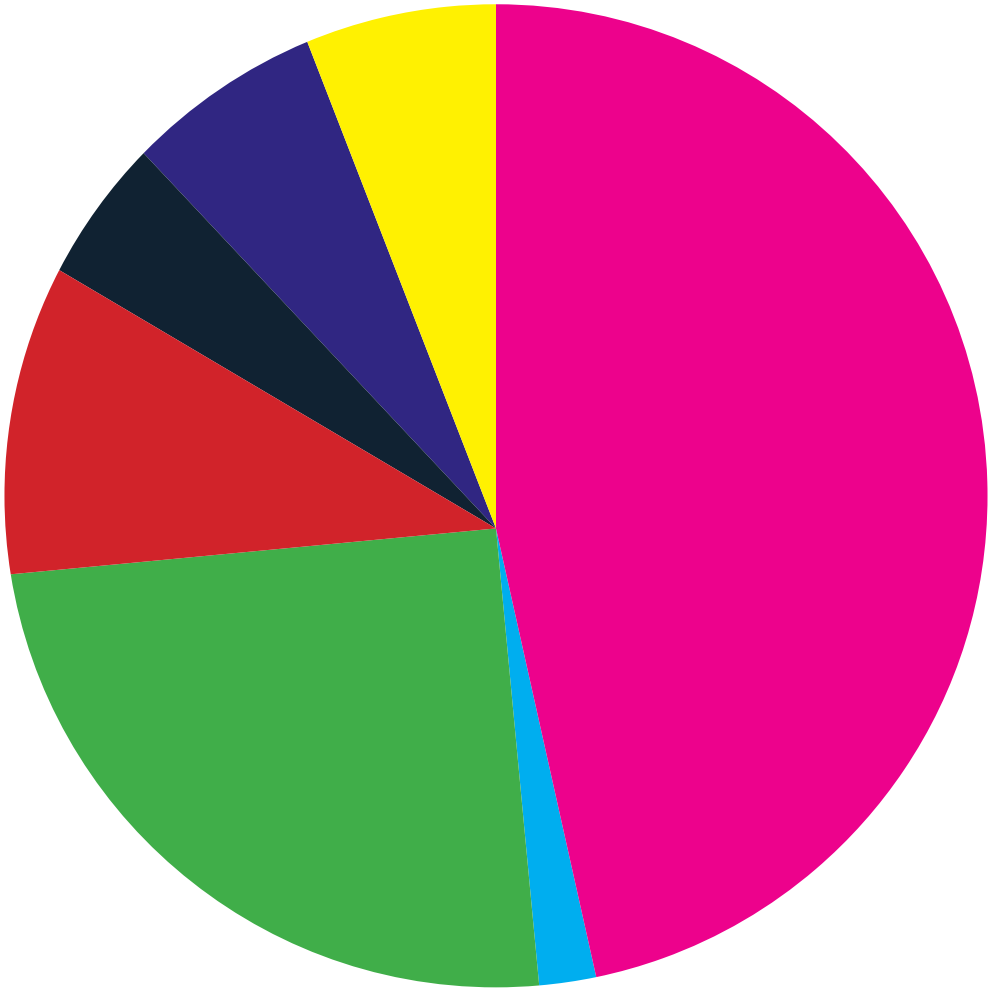
GIFCT is grateful to our members for their commitment to our mission and continued efforts and for their financial support where possible. These contributions allow GIFCT to grow, diversify and sustain the tools and resources we provide our members and the broader counter terrorism and violent extremism field.








### 2022 Annual Contributions: \$3,675,000

#### Contributions in 2022 by Suggested Level



**2022 Total Projected Expenses: \$4,269,524**



	<b>Staff Salary/Employee Related Expenses + Contractors</b>	<b>\$1,985,900</b>
	<b>Independent Advisory Council</b>	<b>\$85,462</b>
	<b>Partnerships</b>	<b>\$1,072,286</b>
	<b>Programming</b>	<b>\$440,917</b>
	<b>Tech Development</b>	<b>\$194,807</b>
	<b>Vendor + Consulting Services</b>	<b>\$258,894</b>
	<b>Administrative Expenses + Support</b>	<b>\$231,258</b>

While this total for projected expenses is greater than the total contributions for 2022, GIFCT is not operating at a deficit as a result of the contributions provided by the founding members in 2020 as start-up support.

GIFCT looks forward to continuing work with its members and diversifying its funding further in 2023.

## What to Expect in 2023

### The Year Ahead: 2023

In the coming year, GIFCT looks forward to strengthening and maturing its structures, protocols, and resources for its members and the wider counter terrorism and violent extremism community. As this report detailed, GIFCT will look to further its progress across its core work and strategic pillars.



### Membership

In 2023, GIFCT will seek to continue to grow our membership of tech companies operating a diverse range of digital platforms and services across the globe. This effort is vital to GIFCT's mission, vision, and ability to continue to develop cross-platform solutions that address the latest attempts by terrorists and violent extremists to exploit the internet.

### Human Rights Impact Assessment

Guided by the recommendations in the HRIA, GIFCT looks forward to continuing to identify concrete ways to embed due diligence regarding human rights across our work. In particular, GIFCT will seek to further develop a due diligence framework that guides how it follows and upholds our recently published [Human Rights Policy](#). This policy articulates how GIFCT will respect human rights as an independent organization and applies to all our activities, including how we aim to support the counterterrorism practices of our member companies, stakeholders, and the broader field.

### **Strategic Pillar: Prevent**

In 2023, GIFCT will remain steadfast in its core technical work to increase the ease, utility, and value of our cross-platform solutions for our members. This work will include completing the implementation of adding hashes of URLs provided by TCAP to the hash-sharing database and adding hashed PDFs of terrorist and violent extremist branded publications to the database. GIFCT will also be working with partners to provide GIFCT members with access to tooling that can make utilizing the database easier for smaller companies with limited resources.

Essential to this effort will be to continue enhancing the transparency of GIFCT's tools, including the hash-sharing database. It is through this transparency effort that GIFCT ensures ongoing measuring and analysis that grows our collective understanding about the effectiveness of our technical solutions and upholds our commitment to human rights.

### **Strategic Pillar: Respond**

In 2023, GIFCT will focus on three main areas to continue to strengthen our readiness and further improve our efforts to stem the spread of terrorist and violent extremist content produced as part of an offline violent attack. First, continuing to implement recommendations regarding due diligence with respect to human rights throughout GIFCT's IRF process and procedures will be paramount. GIFCT will also further the implementation of a robust technical system that enables greater real-time alerts and situational awareness regarding developing events. Third, in tandem with the Prevent work, hashed URLs will provide GIFCT and member companies with greater ability to address attempts to share perpetrator-produced live-stream content (i.e., when shared on a member platform as a URL where the content is hosted on a non-GIFCT member platform).

### **Strategic Pillar: Learn**

GIFCT looks forward to a year of enhanced partnerships with core partners, GNET and Tech Against Terrorism, as we further advance our resources to provide action-oriented research and opportunities for knowledge sharing. GIFCT is grateful for the research and focus areas GNET will partner with us to pursue in order to advance our collective understanding of critical topics at the intersection of extremism and technology. GIFCT is also excited to continue to partner with Tech Against Terrorism to host Workshops, convening stakeholders on the pressing challenges posed by terrorism and violent extremism in particular regions across the world while maintaining our globally accessible virtual e-learning series.





**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.