GIFCT
Global Internet Forum to Counter Terrorism

Annual Report

December 2021

GIFCT
Global Internet Forum to Counter Terrorism

Table of Contents	Page

Letter from GIFCT Executive Director, **Nicholas J. Rasmussen**

Dear GIFCT Members, Colleagues, Partners and Stakeholders,

I am enormously pleased and proud to share with you this first ever Annual Report of the Global Internet Forum to Counter Terrorism (GIFCT). 2021 was a milestone year for GIFCT as it marked the first full year for the organization in its new form as an independent entity with a full-time professional staff. Thank you to all who have participated in, collaborated on, and contributed to our work during this year.

2021 has been a year of significant progress for GIFCT, but the dynamic terrorism and violent extremism landscape that surrounds us is a daily reminder that much more work lies ahead. The important growth that we have made during 2021 can be counted in both organizational and substantive terms:

- We hired a professional staff of six, with presence in London, Washington D.C., and Los Angeles. We remain committed to expanding staff capacity as we work to become an even more global, inclusive, and diverse organization.
- We achieved status as a registered 501(c)(3) organization under U.S. law and have successfully completed our first tax filing and audit process.
- We commissioned an independent and forward-looking human rights impact assessment (HRIA) of GIFCT. Our hope was that this report would serve as a catalyst for GIFCT's organizational development as a newly independent entity, informing our work from the outset and allowing us to take early and decisive action to position human rights at the center of our strategic planning and programmatic activities.
- We delivered on our commitment in our first year to expand the taxonomy framework governing GIFCT's hash-sharing database. This effort represented an important first step for GIFCT as we seek to develop effective approaches to managing the "gray space" challenges that sit at the nexus of terrorism and technology.
- We brought the first year of GIFCT Working Group activity to a successful conclusion, with concrete output resulting from each of these Working Groups. More importantly, we refreshed the substantive agenda and membership for Working Group activity going forward into 2022, which resulted in a wider, more diverse set of expert stakeholders joining that important effort.
- We grew GIFCT's membership significantly, with the organization now including 18 companies, twice the number that were part of GIFCT at the time it began the transition to independent status at the end of 2019. We are delighted to welcome Zoom as our most recent GIFCT member, and we look forward during 2022 to welcoming even more new platforms and companies to GIFCT.

The next three years promise to be even more successful as we seek to expand both our reach and our

impact with an ambitious set of strategic objectives focused on concrete progress and output:

1. GIFCT will serve as the key convener, facilitator, and driver to bring together leaders from all stakeholding sectors to discuss the most important and complex issues at the intersection of terrorism and technology. We will demonstrate with concrete output that multistakeholderism can solve real-world problems and deliver genuine progress. We will continue to engage in this important work with human rights concerns and considerations embedded in our processes and our approach.
2. GIFCT will grow its membership even further, looking to bring a diverse set of new companies into the sector-wide effort to address online terrorism and violent extremism. The evolving threat landscape will guide our efforts to engage with an even more global array of such companies.
3. GIFCT will continue to provide critical support for efforts to build the collective capacity and capability of industry to address terrorism and violent extremism. We will do that by offering cross-platform technology solutions, enhanced information sharing, and practical research to support the work of GIFCT members.

A key part of GIFCT's organizational progress during 2022 will be the implementation of a membership tiering structure that will pave the way for companies beyond the founding members to more directly participate in, and to contribute resources to support, GIFCT's work. Broadening our base of support aligns with recommendations shared in the human rights impact assessment. The critically important partnerships that GIFCT maintains with Tech Against Terrorism to support our membership process and with the Global Network on Extremism and Technology (GNET) to drive practical academic research will continue to be essential to our success in 2022. I am proud of our continued association with the expert teams at both Tech Against Terrorism and GNET and look forward to many years of productive work together.

As we enter 2022, I am more encouraged and excited than ever at the promise and the potential of GIFCT. Our team looks forward to working closely with each of you in the multi-stakeholder effort to one day achieve our ultimate vision of rendering terrorists and violent extremists ineffective in the online environment.

Best,

Nicholas J. Rasmussen

Letter from GIFCT 2021 Operating Board Chair, **Monique Meche from Twitter**

As GIFCT's first full year with an Executive Director and staff in place, our focus for Twitter's term as Chair of GIFCT's Operating Board has been to position the organization on a strong strategic and programmatic path for the future, with robust governance and solid financial structures in place. This year, GIFCT has made substantial progress in a number of areas, celebrated many successes, and continued to grow as an organization.

Upon assuming the role of Operating Board Chair, we set out five key priorities:

I. Foundational Principles
Twitter's vision for the Operating Board was to set a strategic and operational plan for GIFCT to ensure its long-term success. We approved GIFCT's three-year strategic plan, 2022 budget, and strategic objectives guided by a renewed Mission, Vision, Values Statement.

GIFCT also conducted its first human rights impact assessment, an important landmark that has already led to change and will be a foundational resource going forward.

II. Membership Diversity
Broadening GIFCT's membership is a key way to increase GIFCT's impact, while ensuring that all members contribute to the work of GIFCT and disrupt terrorist use of the internet. To date, GIFCT is on track to double its December 2019 membership and has increased its membership from 9 to 18 companies. And, it's also encouraging that there are more than 10 companies currently in the Tech Against Terrorism mentorship process. The GIFCT Member Resource Guide, an expansive online compendium that includes 100+ open-source safety, transparency, counterspeech, and digital literacy resources from across all GIFCT member platforms, is now live and being used by members.

III. Crisis Response
One of our priorities was to ensure that GIFCT has a robust Incident Response Framework in place, particularly where there is no live-stream element to an attack, but the harm from other content is potentially severe. GIFCT announced a broadened Crisis Response framework that now includes a framework for sharing situational awareness in a broader range of incidents, including those that do not include livestream or video content. This enables GIFCT's membership to respond to a wider range of incidents and content types.

Operating Board members and GIFCT staff participated in the Christchurch Call To Action's Crisis Response Working Group. Their efforts developed a working plan that provides guidance to strengthen the coordination between GIFCT's and other existing crisis response protocols, bridges identified gaps, and increases information sharing. We also focused on aligning GIFCT's crisis response efforts with other protocols to address gaps in existing structures.

IV. Evolving Threat Landscape

Throughout 2021, GIFCT began the important work of the ever evolving threat landscape, particularly the rise of violent far-right extremism globally. In its early days, GIFCT's and the Internet Forum's focus was on ISIS and Al-Qaeda. Through expanding the hash-sharing database's taxonomy and hosting multiple e-learning webinars on violent far-right and conspiracy theory extremists, GIFCT has equipped its members with the tools needed to remove this content from their platforms.

Collaboration

Finally, GIFCT plays an important role in convening, educating, and informing the broader stakeholder community about the actions that members have taken to disrupt TVEC. From July 2020-2021, GIFCT convened more than 600 participants from tech, government, civil society, and academic partners around the world through monthly e-learnings with our partner Tech Against Terrorism. Although GIFCT's traditional in-person workshops have been paused through the pandemic, GIFCT most recently held a successful virtual workshop in partnership with the Ghanian Government focused on West African trends in terrorism and counterterrorism.

We are grateful for the collaboration and support provided by the GIFCT team, Independent Advisory Committee (IAC) members, Operating Board members, and other GIFCT stakeholders during our term as Chair. While there remains much work to do, we are pleased with GIFCT's success and expansion during 2021 and are excited about the continuation of both during YouTube's tenure as Operating Board Chair in 2022.

Best,

Monique Meche

Letter from GIFCT Independent Advisory Comittee Chair, **Bjørn Ihler**

The Global Internet Forum to Counter Terrorism (GIFCT) was, as the name indicates, intended to be a forum; a meeting space, and a place for conversation among a wide range of stakeholders to tackle the challenging topic of protecting our shared online spaces from the harmful abuse of those with terroristic intent. The Independent Advisory Committee (IAC) is one of the avenues through which the GIFCT embodies this - by bringing together, and listening to the voices of stakeholders beyond the corporate members of the organization.

By convening voices from government and civil society the IAC provides an outside perspective, insights and expertise to guide the GIFCT as an organization with an impact that reaches beyond the bounds of the member companies, the technology sector and indeed the realm of the internet. The IAC supports the GIFCT, the Operating Board, the Executive Director and other staff in navigating the complex CT/CVE landscape, striving to ensure that GIFCT fits into the larger field in a way that is meaningful and impactful and without replicating the work of other bodies and while remaining conscious of the evolving landscape both of terrorist activity and of global legislation, policy and technology efforts to counter the terrorist misuse of the internet.

I am excited to see GIFCT increasing engagement with the broader community of stakeholders from around the globe, reaching beyond, and building upon the existing networks of members of the IAC and the Working Group community. Ensuring that the diverse voices of human rights groups, rightsholders, and communities impacted by the work of GIFCT around the globe are heard at every level of decision making processes is key to cement the legitimacy, and added value of GIFCT as a body.

Providing insights, knowledge, and healthy resistance, the IAC and the wider multistakeholder community should be serving as a conscience in the processes of making decisions for an organization that through its members has the potential of affecting more users than any government in the history of the planet has governed. In this I am happy to see an increased focus on meaningful transparency and community engagement from the GIFCT. Extending the standards to which GIFCT is holding member companies with respect to transparency, and respect for human dignity and rights is one key area for further development in the year to come as the membership structure is further fleshed out.

As a novel construct, and as a new organization setting up the triangular structure including the IAC, the Operating Board and the GIFCT and Executive Director has come with some challenges. While much has been accomplished, we are still working to make this structure as effective, transparent and impactful as possible for all involved. Throughout the last few months of 2021 the IAC and Operating Board have worked to review existing documentation and establish new practices to ensure that the IAC is utilized in the best possible way going forwards, and that channels of communication and collaboration, while avoiding duplication of work are as streamlined as possible while maintaining the independence of the IAC.

With the restructuring of the Working Groups and a growing focus on wider, and more diverse community engagement it is my hope that the engagement both with the IAC and the wider multistakeholder community will prove both meaningful and impactful in new ways as we advance the work of the organization.

The Human Rights Impact Assessment was a key product resulting, among others, from engaged contributions of the IAC this year. By inviting a broad range of representatives, both from IAC members and from external groups, the assessment contributed both to ensure the protection of rights, and to advance the relationship and level of trust between GIFCT and the wider stakeholder community. This early focus on human rights served to cement human rights as a key focus area and fundamental value of GIFCT as an organization, further informing the course of the organization in subsequent endeavours. The assessment will continue to serve as a guiding document as we advance the work of both the IAC and the organization, deliver on recommended actions, and continuously take into account rightsholders and impacted communities as key stakeholders in the work.

The IAC played a key role in advancing the expansion of the taxonomies and definitions framework of GIFCT. Not only did the group highlight the need for an expansion on the existing framework, but we also established a working group that produced a new practical taxonomy framework to empower GIFCT and member companies to better enforce policies, allocate resources, improve the GIFCT hash sharing database and the tools available to prevent the terrorist misuse of online services. Through this work we also welcomed the inclusion of PDF files and URLs in the GIFCT hash-sharing database, and firmly believe that will have a significant impact, while urging the continuous growth of this important tool to also include emerging types of content while remaining vigilant in protecting both fundamental freedoms and human dignity and lives.

Beyond contributing to these larger efforts the IAC continues to work closely with GIFCT both through active participation in operating board meetings, through regularly scheduled meetings with board members, and through the continuous bilateral dialogue between IAC members, the chair of the Operating Board, the Executive Director and GIFCT staff who regularly reach out to individual members of the committee for feedback and advise both on strategy, operations, activities and efforts.

In the world of counterterrorism it is easy to fall into the trappings of the day-to-day newscycle, of being reactive to the latest incident rather than being proactive in meeting evolving challenges. It is easy to look back at previous incidents, and to plan for how to meet replications of those, but as technology and terrorist tactics constantly evolve so must our measures to proactively combat the terrorist abuse of our shared online spaces both for purposes of recruitment, coordination, fundraising and spread of propaganda.

The member companies of GIFCT are on the cutting edge of developing technology - we know that malicious users with terroristic intent will be among the early adopters of new and evolving technology in the future, as they have been in the past. As the organization grows in membership, and as the

existing member, and founding companies launch new products, services and ventures that may fall outside of the landscape of content dissemination through centralized platforms that conventionally has been the focus of the field it is key that GIFCT is proactive, and holistic in its understanding of the relationship between technology, policy, society and the individual. In this it is key that the IAC continues to be a resource to the GIFCT, a body of immense knowledge and experience, bridging the gap between policy makers, technologists, academics, and activists, supporting the work of the GIFCT while through its independence maintaining its role as a voice of reason, a conscience, as we face the challenges of the internet of tomorrow.

Best,

Bjørn Ihler

Overview of the Global Internet Forum to Counter Terrorism: **2017 - 2021**

This month, we mark a year and a half since the Global Internet Forum to Counter Terrorism (GIFCT) became an independent entity with an inaugural exective director, Nicholas J. Rasmussen and an Independent Advisory Committee (IAC) to advise the organization's Operating Board. Since then, we have grown to a team of six full-time staff of counterterrorism and technology experts working with the now 18 technology companies we support 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 as a consortium of tech companies that recognized the need for combating terrorist and violent extremist activity online and the immense impact working together could have towards that end. Primarily driven by the urgent imperative to respond to the growing use of social media platforms by groups such as the Islamic State, in-house teams at GIFCT's member companies initially focused on developing cross-platform tools such as the hash-sharing database to share "digital fingerprints'' of identified terrorist content and establishing a forum where tech companies, governments, academia, and civil society could discuss the state of the 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, when the perpetrator livestreamed his horrific violence designed for virality as part of his attack, 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, committing 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 companies announced in September 2019 at the United Nations General Assembly that GIFCT would evolve from a consortium of tech companies to an independent non-profit organization with its own team of professionals working with our member tech companies towards our mission to prevent terrorist and violent extremist exploitation of digital platforms. Since then, GIFCT has continued collaborating with the Christchurch Call leadership on our shared goals while GIFCT's Working Groups -- both in substance and objectives -- closely align with those of the Christchurch Call's multi-stakeholder workstreams.

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

At GIFCT today, we work to fulfill our mission and achieve our vision guided by our values and organized by our 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, we aim to be **transparent**, **inclusive**, and **respectful of the fundamental and universal human rights** that terrorists and violent extremists seek to undermine. We approach and define 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 our 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 we are always seeking to expand and diversify our stakeholder community.
- **Respect for Human Rights:** We believe 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.

GIFCT Today

Executive Director Nicholas Rasmussen and the team of experts leading GIFCT's programming, technological, and strategic initiatives manage the day-to-day operations as an independent non-profit organization. An Operating Board made up of senior executives from the Forum's founding companies - Facebook, Microsoft, Twitter, and YouTube - governs the organization. The Operating Board is advised by an Independent Advisory Committee composed of representatives from civil society, government, and intergovernmental organizations and is currently chaired by Bjørn Ihler, co-founder of the Khalifa-Ihler Institute, which works to promote peace, human rights, and thriving communities. Learn more about GIFCT governance here.

2020 and 2021 have been formative years for the independent GIFCT, during which we established a roadmap for how we carry out our mission guided by our values. Under Nicholas Rasmussen's leadership, the team at GIFCT has incorporated cutting-edge research and input from a range of experts and practitioners to set a strategy for enhancing the collective capacity of member technology companies to combat terrorist and violent extremist activity online.

Over the course of 2021, GIFCT commissioned an independent human rights impact assessment from the firm Business for Social Responsibility (BSR) and charted a course for pursuing the forward-looking report's recommendations to ensure that we are embedding respect for human rights into every aspect of our work. This year, we also launched an effort to address the larger anti-Islamist bias in the counterterrorism field and to build upon the United Nations Security Council's Consolidated Sanctions List and our Content Incident Protocol for what qualifies for inclusion in the GIFCT hash-sharing database as terrorist and violent extremist content. 2021 also saw the successful conclusion the first year of the GIFCT Working Groups, which convened global stakeholders on the challenges at the nexus of technology and terrorist and violent extremist activity and saw a significant increase in interest to join the second year of GIFCT Working Groups that are currently ongoing.

This report will elaborate on each substantive element of our work in 2021 to share our latest progress and next steps for the coming year.

Global Engagements

Over the last year, GIFCT was invited to participate in a number of forums and convenings as an expert on the threats and dynamics at the nexus of terrorism and technology. We were 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 global and significant convenings we had the pleasure of contributing to.

Events Hosted by Governments and Intergovernmental Organizations:

- Christchurch Call to Action Second Anniversary Summit hosted by New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron
- G7 Meeting of Security Ministers hosted by the United Kingdom Home Secretary
- Multiple events convened by the United Nations Development Program
- European Union Internet Forum
- The 16th Annual Internet Governance Forum Meeting
- UN Office of Counter-Terrorism Expert Roundtable on Video Games and Violent Extremism
- ASEAN Regional Forum Workshop on Preventing Terrorist Use of the Internet
- Aqaba Process Blue Sky Global Counter Terrorism Conference hosted by his Royal Highness the King of Jordan
- USCIB/BIAC/OECD Conference + Engagement in the OSCE Transparency Forum
- Annual CTC-DCTC Conference: Combating Terrorism Center at West Point (CTC) in partnership with the Defense Combating Terrorism Center (DCTC)
- Commonwealth Secretariat's Regional Workshop on Preventing Terrorist Use of the Internet in Africa
- Future Challenges in PTUI (Preventing Terrorist Use of the Internet), hosted by the United Kingdom and Australian Embassies in Brussels

Events Hosted by Civil Society and Non-Governmental Organizations (NGOs):

- RightsCon 2021
- Eradicate Hate Global Summit in Pittsburgh, PA USA
- Soufan Center's Global Security Forum
- Future of Online Trust & Safety Conference with TSPA and DTSP (Trust & Safety Professional Association and the Digital Trust & Safety Partnership)
- International Institute for Counter-Terrorism's 20th World Summit on Counter-Terrorism
- IEEE Mitigating Societal Harms in a Social Media World Tech Forum to Explore Critical Societal Issues
- Atlantic Council's Digital Forensic Research Lab's 2021 360 Open Summit
- i2Coaltion Speaker Series
- Counter Extremism Project event in partnership with the German Foreign Ministry
- Goundswell Project Mother's Training on Digital Literacy and Safety to Mothers and Daughters hosted at the Azhar Academy for Girls in London

Events Hosted by Academic Institutions:

- Global Network on Extremism and Technology's First Annual Conference
- 22 July 2011 at Ten: Commemoration and Commitment Conference in Bergen
- Swansea Terrorism and Social Media Conference (TASM) and Wales Technology Week Panel
- Cambridge University Counterspeech Workshop
- Stanford University Program on Democracy and the Internet's Content and Policy Lab Workshop
- Deakin University's AVERT Research Network Online Conference on Violent Extremism
- Columbia University Lecture for John Jay College of Criminal Justice, CUNY

GIFCT also provided training to the following civil society organizations focused on preventing and countering violent extremism:

- The Nordic Safe Cities Training Camp for Practitioners
- Alliance for Peacebuilders
- Radicalization Awareness Network - Strategic Communication Workshop
- Kofi Annan Foundation - Envision Together Workshop
- Commonwealth Youth Peace Ambassadors Network

GIFCT Executive Director Nicholas Rasmussen participated in the May 2021 Christchurch Call to Action Second Anniversary Event, joining heads of states and leaders from tech and civil society.

Human Rights Impact Assessment

Respect for universal and fundamental human rights is central to how we work to fulfill our mission to prevent terrorist and violent extremist exploitation of digital platforms. That's why it was critical in the first year operating as an independent organization that we took early and decisive action to build respect for human rights into the blueprint of GIFCT's ethos and operations.

After seeking the advice from a diverse, global range of civil society stakeholders — members of our Independent Advisory Committee, participants in our Working Groups, and other individuals following and invested in GIFCT — we decided in the fall of 2020 to commission an independent assessment of the actual and potential human rights impacts of GIFCT's work. The Operating Board's support for this decision reaffirmed its commitment to situating civil society expertise, human rights, and free expression at the center of the newly independent GIFCT.

In December 2020, we formally commissioned the non-profit Business for Social Responsibility (BSR) to conduct the assessment. Recommended to us by numerous stakeholders, BSR is an industry leader in the arena of evaluating the human rights impacts of technology company policies and operations. The scope of this assessment was focused on GIFCT and not the actions or policies of individual GIFCT member companies, and was designed to be forward-looking - ideally making it a useful tool for organizations and individuals thinking proactively about human rights at the nexus of terrorism and technology.

Over the course of the six-month assessment, GIFCT worked closely with BSR on the development of rights-respecting positions and policies in real time, allowing us to situate universal and fundamental human rights at the center of our strategic planning and programmatic activities. Throughout this process, we were committed to remembering and prioritizing the individuals most vulnerable in this context: the victims of both terrorism and violent extremism and of efforts to address terrorism and violent extremism.

GIFCT's human rights impact assessment was informed by the UN Guiding Principles on Business and Human Rights. Drawing from these principles, the BSR team operated on the following key methodological assumptions:

- All human rights are potentially relevant for GIFCT
- Human rights are interconnected
- A stakeholder-inclusive process is essential
- Vulnerability must be prioritized

Guided by these standards, BSR held conversations with over 40 individuals and organizations across our stakeholder community. From these discussions, BSR offered 47 concrete recommendations to GIFCT that spanned nine themes and 35 questions, to include membership, organizational governance, content removal and preservation, and consideration of terrorist and violent extremist content, among others.

GIFCT has already taken action in line with the recommendations from the Human Rights Impact Assessment.

To date, we have implemented recommendations including the following:

- Refined our membership criteria to bring greater transparency to the membership process and to set clear expectations and standards for aspiring member companies to meet as a condition of joining GIFCT;
- Launched a multi-stakeholder effort to expand the taxonomy of terrorist content that qualifies for inclusion in the GIFCT hash-sharing database to address biases in our current taxonomy and help our members identify a broader range of terrorist content that may exist on their platforms;
- Participated in efforts to pursue counterterrorism and violent extremism priorities from a holistic and strategic perspective;
- Conducted a stakeholder mapping to identify organizations and experts that would increase the diversity of rights holders whose voices are heard in GIFCT activities;

Over the next six-12 months, we are working to make concrete progress against additional recommendations set forth in the Human Rights Impact Assessment, to include:

GIFCT Membership:

- Establishing a tiered membership structure for GIFCT
- Broadening the diversity of stakeholders we work with and expanding GIFCT membership to a broader range of tech companies based on size, geographic location, and platform service
- Providing assistance to smaller member companies to address human rights risks when working to prevent terrorist and violent extremist exploitation of their platforms

Content Moderation:

- Introducing and expanding transparency and oversight mechanisms alongside the extension of content in the hash-sharing database
- Using a GIFCT "common understanding" of terrorist and violent extremist content to determine inclusion in the hash-sharing database in the medium to long term

Theory of Change and Programmatic Priorities:

- Developing position statements on the rights-based laws, policies, regulations, and strategies needed to more effectively address the exploitation of digital platforms by terrorists and violent extremists

Over the next three to five years, we are committed to exploring the feasibililty and advisability of further recommendations from the Human Rights Impact Assessment, to include:

Content Moderation:

- Investigate how to enable third-party reviews of the hash-sharing database to assess whether hashes are consistent with the GIFCT taxonomy

Organizational Matters:

- Establish a mechanism to provide stipends for non-company / non-government participants in GIFCT

Governance, accountability, and transparency:

- Review the merits of transitioning to a multi-stakeholder Operating Board

BSR's forward-looking assessment offers enduring strategic and tactical value not only to GIFCT but also to our constituent stakeholders committed to the project of promoting and protecting universal and fundamental human rights. From BSR's pioneering methodological framework to its careful consideration of cross-sector challenges, this assessment serves as a vital component of how we work to move the tech industry forward in combating terrorist and violent extremist exploitation online while respecting fundamental human rights and freedoms.

GIFCT's human rights impact assessment marks only the beginning of our journey to embed human rights across all our work and remain diligent to potential adverse human rights impacts as we progress. We look forward to continuing this work together.

You can read Executive Director Nicholas Rasmussen's response to the publication of the human rights impact assessment here and the assessment in its entirety here. BSR's blog post on this effort is available here, and more information about their broader work on human rights and organization can be found here and here.

GIFCT Working Groups

Successful Conclusion of Year 1 and Renewing our Focus in Year 2

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 at the GIFCT Global Summit, we present Working Groups' output, update their themes and focus areas, and allow new participants to join. Working Group participants collaborate with GIFCT to prepare strategic work plans and outline objectives, goals, strategies, deliverables, and timelines.

GIFCT Working Groups Year 1: 2020 - 2021

From July 2020 to July 2021, GIFCT's six Working Groups convened more than 200 experts and practitioners from across the world, holding more than 55 meetings with representatives from 10 tech companies, 13 governments and international governing bodies, 26 civil society organizations, and 41 research and academic institutions. The six groups (1) explored new technical solutions, (2) refined crisis response protocols, (3) studied legal frameworks addressing terrorist and violent extremist content, (4) pursued innovations in algorithmic amplification and positive interventions, (5) examined how to enhance transparency, (6) and looked at new ways to include researchers and academics.

At the Global Summit in July 2021, each Working Group published their efforts - providing authoritative information on the current dynamics of each issue area and next steps in identifying and deploying solutions. Output from each Group is outlined and linked to below:

Technical Approaches

Gap Analysis Report, led by Tech Against Terrorism, summarizing technical gaps, solutions, and recommendations for how cross-platform technical collaborations can be strengthened. The report was directed particularly at smaller tech platforms and focused specifically on content. The report was accompanied by an Executive Summary written by the co-leads of the group.

Crisis Response

The Crisis Response Working Group produced two internal directories created for cross-sector crisis communication, linking relevant government authorities to the right contacts at GIFCT member companies and made the directories available to those specific points of contact. The group also produced a briefing paper discussing how various crisis protocols are initiated and how to debrief relevant stakeholders and review protocols in the aftermath of a crisis.

Legal Frameworks

The Legal Frameworks Working Group produced a Gap Analysis Report focused on what constitutes "data" and identifies a number of policy questions and challenges that arise from the operational use of information by various actors.

Content-Sharing Algorithms, Processes, and Positive Interventions

The CAPPI Working Group produced a research brief focused on Content-Sharing Algorithms and Processes, which mapped the type of algorithmic processes that could be exploited by violent extremists and terrorists. They also produced a paper analyzing Positive Interventions online with a range of international case studies.

Transparency

The Transparency Working Group produced a briefing paper that breaks down various aspects of what meaningful transparency means to different sectors and identified explicit recommendations for GIFCT in their own transparency reporting.

Academic and Practical Research

The Academic and Practical Research Working Group developed a paper assessing the knowledge gaps and barriers that affect stakeholders within the field of preventing and countering violent extremism as they begin moving toward holistic and coordinated solutions. They also produced a White Paper on emergent issues that are understudied and (consequently) misunderstood.

Outputs from Working Groups are made public on the GIFCT website and the annual summit sessions on Working Groups can be found here:

GIFCT Working Groups Year 2: 2021 - 2022

Through August 2021, public and open applications were received for participants to join refreshed Working Groups addressing an updated set of thematic topics. There was a total of 273 applications, 76.2% of which were new applicants who had never participated in a GIFCT Working Group before. In the final formation of Working Groups. A total of 178 participants were assigned to five reorganized Working Groups and were chosen based on their subject matter expertise, sector diversity, geography, and perspective. Working Group participants come from 35 countries across six continents, with 57% drawn from civil society, academia or practitioners, 26% representing governments, and 17% in tech.

Beginning in August 2021, five GIFCT Working Groups have sharpened their focus to address the following themes:

Technical Approaches: Tooling, Algorithms & Artificial Intelligence

- What technical solutions can be used to prevent/mitigate unintended consequences of

algorithms and AI?

- How can tooling and tactics be implemented for smaller platforms?
- What technical approaches beyond photo/video hashing can be used to prevent terrorists and violent extremists from exploiting digital platforms (including within recommendation features)?
- 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?

Transparency: Best Practices & Implementation

- What other sectors can we look to for best practices on transparency reporting and communication to key stakeholders?
- What are frameworks and examples of algorithmic transparency that can help guide the tech community?
- What are the key barriers for tech companies in sharing API access or meaningful data with researchers?
- What further support can be given to platforms approaching their first transparency report?

Crisis Response & Incident Protocols

- What are best practices to ensure refinement and readiness of different global protocols (e.g., Christchurch Call, GIFCT, European Union) and other domestic law enforcement protocols?
- What is the role of each sector and network within the different incident response protocols?
- Where can GIFCT further facilitate crisis response and where is it up to individual companies and law enforcement entities?
- What is the impact of these protocols on human rights and how can we ensure that they are appropriately balanced and protected?

Positive Interventions & Strategic Communications

- How best can we turn passive counter-narrative exposure into active strategic communications in order to facilitate disengagement?
- What newer and smaller platforms are available to launch positive interventions in order to reach target audiences?
- How do we upscale and optimize global public-private partnerships between platforms and NGOs developing intervention campaigns?
- Where can positive interventions become more automated or proactively surfaced across platforms based on user behavior or signals?

Legal Frameworks

- What barriers are tech companies facing in increasing API access to data for researchers?

- What are the intellectual property barriers in considerations for "algorithmic transparency"?
- Where do we see legal regulations and policies in different parts of the world that are posing challenges for tech companies in solving for privacy versus security?
- Where can we provide better guidance for smaller companies looking to innovate while also complying with increasing regulation?

GIFCT is also funding an overarching piece of research to bring together the algorithmic questions embedded within technical approaches, legal frameworks and transparency. This output will be added to the wider output of the Working Groups.

Participant Affiliations in the August 2021 - July 2022 Working Groups:

Tech Sector	Government Sector	Civil Society / Academia / Practitioners	Civil Society / Academia / Practitioners
ActiveFence	Aqaba Process	Access Now	Lowy Institute
Amazon	Association Rwandaise de Défense des Droits de l'Homme	Anti-Defamation League (ADL)	M&C Saatchi World Services Partner
Automattic	Australian Government - Department of Home Affairs	American University	Mnemonic
Checkstep Ltd.	BMI Germany	ARTICLE 19	Moonshot
Dailymotion	Canadian Government	Australian Muslim Advocacy Network (AMAN)	Moduslzad - Centre for applied research on deradicalisation
Discord	Classification Office, New Zealand	Biodiversity Hub International	New America's Open Technology Institute
Dropbox, Inc.	Commonwealth Secretariat	Bonding Beyond Borders	Oxford Internet Institute
ExTrac	Council of Europe, Committee on Counter-Terrorism	Brookings Institution	Partnership for Countering Influence Operations, Carnegie Endowment for International Peace
Facebook	Department of Justice - Ireland	Business for Social Responsibility	Peace Research Institute Frankfurt (PRIF); Germany
JustPaste.it	Department of State - Ireland	Centre for Analysis of the Radical Right (CARR)	PeaceGeeks
Mailchimp	Department of State - USA	Center for Democracy & Technology	Point72.com
MEGA	Department of the Prime Minister and Cabinet (DPMC), New Zealand Government	Center for Media, Data and Society	Polarization and Extremism Research and Innovation Lab (PERIL)
Microsoft	DHS Center for Prevention Programs and Partnerships (CP3)	Centre for Human Rights	Policy Center for the New South (senior fellow)
Pex	European Commission	Centre for International Governance Innovation	Public Safety Canada & Carleton University
Snap Inc.	Europol/EU IRU	Centre for Youth and Criminal Justice (CYCJ) at the University of Strathclyde, Scotland.	Queen's University
Tik Tok	Federal Bureau of Investigation (FBI)	Cognitive Security Information Sharing & Analysis Center	Sada Award, Athar NGO, International Youth Foundation
Tremau	HRH Prince Ghazi Bin Muhammad's Office	Cornell University	Shout Out UK
Twitter	Ministry of Culture, DGMIC - France	CyberPeace Institute	Strategic News Global
You Tube	Ministry of Foreign Affairs - France	Dare to be Grey	S. Rajaratnam School of International Studies, Singapore (RSIS)
	Ministry of Home Affairs (MHA) - Indian Government	Dept of Computer Science, University of Otago	Swansea University
	Ministry of Justice and Security, the Netherlands	Digital Medusa	Tech Against Terrorism
	National Counter Terrorism Authority (NACTA) Pakistan	Edinburgh Law School, The University of Edinburgh	The Alan Turing Institute

	Organisation for Economic Co-operation and Development (OECD)	European Center for Not-for-Profit Law (ECNL)	The Electronic Frontier Foundation
	Office of the Australian eSafety Commissioner (eSafety)	Gillberg Neuropsychiatry Centre, Gothenburg University, Sweden,	The National Consortium for the Study of Terrorism and Responses to Terrorism (START) / University of Maryland
	Organization for Security and Co-operation in Europe (OSCE RFoM)	George Washington University, Program on Extremism	Unity is Strength
	Pôle d'Expertise de la Régulation Numérique (French Government)	Georgetown University	Université de Bretagne occidentale (France)
	North Atlantic Treaty Organization, also called the North Atlantic Alliance (NATO)	Georgia State University	University of Auckland
	Secrétaire général du Comité Interministériel de prévention de la délinquance et de la radicalisation	Global Network on Extremism and Technology (GNET)	University of Groningen
	State Security Service of Georgia	Global Disinformation Index	University of Massachusetts Lowell
	The Royal Hashemite Court/ Jordanian Government	Global Network Initiative (GNI)	University of Oxford
	The Office of Communications (Ofcom), UK	Global Partners Digital	University of Queensland
	UK Home Office	Global Project Against Hate and Extremism	University of Salford, Manchester, England,
	United Nations Counter-terrorism Committee Executive Directorate (CTED)	Groundscout/Resonant Voices Initiative	University of South Wales
	UN, Analytical Support and Sanctions Monitoring Team (1267 Monitoring Team)	Hedayah	University of the West of Scotland
	United Nations Major Group for Children and Youth (UNMGCY)	Human Cognition	Violence Prevention Network
	United States Agency for International Development (USAID)	Institute for Strategic Dialogue	WeCan Africa Initiative & Inspire Africa For Global Impact
		International Centre for Counter-Terrorism	Wikimedia Foundation
		Internet Governance Project, Georgia Institute of Technology	World Jewish Congress
		Islamic Women's Council of New Zealand	XCyber Group
		JOS Project	Yale University, Jackson Institute
		JustPeace Labs	Zinc Network
		Khalifa Ihler Institute	
		KizBasina (Just-a-Girl)	
		Love Frankie	

GIFCT Strategic Pillar: Prevent

Updates to Expanding the Taxonomy of the GIFCT Hash-Sharing Database for Terrorist and Violent Extremist Content and CVE Training

As GIFCT develops a foundation for expanding its taxonomy for hash-sharing, there are fundamentally two approaches that we can build on top of the existing system in order to complement its current strengths and weaknesses; list based approaches and behavioral, content-specific approaches.

Taxonomy for the GIFCT Hash-Sharing Database before the 2021 Expansions

GIFCT originally established the hash-sharing database taxonomy in 2016 with a list-based approach addressing content produced by individuals and entities on the United Nations Security Council's Consolidated Sanctions List. This also allowed the consortium at the time to find common ground amongst tech company members who often use slightly different operational definitions of "terrorism" and "terrorist content". Following the terrorist attacks in Christchurch, New Zealand in March 2019 in which the perpetrator livestreamed his attack, GIFCT expanded the taxonomy in order to enable hash-sharing of content from such attacks where violent propaganda is produced. This initial expansion took a behaviorial-based approach, and as a result GIFCT began addressing producers of terrorist content that are not included on the United Nations Security Council's Consolidated Sanctions List.

Based on these two initial approaches, hashes of terrorist content that qualified to be put in the hash-sharing database had to meet the following taxonomy that recognized the **producers** of the content as well as the **type** of content:

Content produced by individuals and entities on the United Nations Security Council's Consolidated Sanctions List when the content depicts or includes:

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

Video or livestream content depicting murder or attempted muder produced during a terrorist or mass violent attack by the perpetrators or accomplices that results in GIFCT activating the Content Incident Protocol (CIP). When this content is hashed and shared in the database, it includes a label corresponding to the specified activated CIP. Activated CIPs and corresponding labels in the database currently include:

- Christchurch, New Zealand Perpetrator Hashes: On March 15, 2019, the need for a separate hash label was declared after an attacker live-streamed his attacks on two mosques.
- Halle, Germany, Perpetrator Hashes: On October 9, 2019, the CIP was activated following an attacker livestreaming his attack on a synagogue.
- Glendale, Arizona, U.S., Perpetrator Hashes: On May 20, 2020, the CIP was activated following an attacker livestreaming his attack on the Westgate Entertainment District.

How We Approach Further Expansions

GIFCT will develop and publish a definitions and principles framework. This exercise will explore options based on behavioral and list-based approaches - for example, how best to reference established lists maintained by government and intergovernmental organizations such as the United Nations. It will build on the existing categories of hashes by creating a definitional framework for assessing terrorist and violent extremist organizations that addresses an evolving threat landscape with the aim of offering additional resources to a wider range of tech companies as they apply their own terms of service.

The recent GIFCT Human Rights Impact Assessment recommends that GIFCT "accompany the expansion of the hash-sharing database to include violent extremist content, adequate transparency and oversight mechanisms." To that end, in our 2021 Transparency Report we published initial data detailing the feedback we received from members on hashes in the database. In addition, we have published an explainer video to clarify how the hash-sharing database operates and solidified the functionality that enables hashes to be removed from the database when they are included there in error.

What's Coming in 2022: Implementing Expansions and Enhancing Transparency

Over the coming months, we will work to implement a holistic approach to assessing the use of the hash-sharing database by GIFCT members to develop recommended best practices for future use and to enhance transparency of the database.

Feedback from GIFCT member companies (published in our July 2021 Taxonomy Report) clearly showed a pressing need to improve the breadth of capabilities that GIFCT provides to support its members in preventing terrorists and violent extremists from exploiting their platforms. To meet this need, we committed to include three new categories of hashed content that reflect how terrorist and

violent extremist activity manifests online. These three additional categories further reflect feedback from our Independent Advisory Committee, GIFCT Working Group output, and a global consultation process which led to a public Taxonomy Report. This feedback focused on specific ways GIFCT could look to go beyond some of the Islamist extremist biases within government lists, while staying limited and proportionate in scope, in line with GIFCT's mission.

As we announced in July 2021 during the annual GIFCT Global Summit, we are expanding the taxonomy of the hash-sharing database to include:

1. **Attacker Manifestos:** Hashed PDFs and images of violent extremist and terrorist attacker manifestos in coordination with global expert academics;
2. **Branded Publications:** Hashed PDFs and images of branded terrorist and violent extremist publications in coordination with global academics; and
3. **TCAP URLs:** Hashed URLs corresponding with terrorist content links flagged to companies through Tech Against Terrorism's Terrorist Content Analytics Platform (TCAP). TCAP automates the collection, verification and analysis of terrorist content across technology platforms. Tech Against Terrorism will hash TCAP URLs to feed to GIFCT in an effort to support the hash sharing consortium. TCAP includes URLs from Islamic State, al-Qaeda, affiliates of these two organizations, Taliban entities, white supremacist and neo-Nazi groups that have been designated by the United Nations, European Union, Australia, Canada, United Kingdom, Canada, and United States (Departments of State and Treasury). The first step will be to import hashes that fit with GIFCT's existing taxonomy (the United Nations Security Council's Consolidated Sanctions List), with the potential to broaden this in line with the planned definitions and principles framework.

Following the announcement of these three new categories in July 2021, GIFCT began implementation and has now incorporated initial capabilities into the hash-sharing database that enables the creation of hashes related to PDFs and URLs. This capability expansion includes integrating the TLSH algorithm into our systems for hashing text from PDFs and developing a new convention for the hashing of URLs. We have also produced an Alpha release of a portal to enable sharing of data from Tech Against Terrorism to GIFCT without providing access to hash data shared by members to ensure compliance with relevant data sharing regulations. Over the next few months, we will be incorporating this into our end-to-end capabilities and will begin ingesting hashes under each of the three categories.

Why are we shifting from URL sharing to TCAP hashing?

Starting in 2020, GIFCT had a URL sharing pilot to test the utility to our members of a service gathering and alerting members to URLs on their platform that potentially were terrorist related. At the end of the trial period, we found that although some URLs were identified for some members and these were actioned according to those member's policies, the value to our full set of members was limited. At the same time, Tech Against Terrorism had developed the Terrorist Content Analytics Platform (TCAP) and

begun alerting tech companies (including GIFCT members) to URLs relating to their platforms that Tech Against Terrorism had identified as terrorist content. TCAP alerting effectively filled the gap that the GIFCT URL sharing pilot was attempting to fill. To ensure that we were focusing on interventions that could most effectively deliver on GIFCT's mission, we pivoted our URL sharing work to focus on hashing URLs that TCAP identified, complimenting TCAP's sharing of URLs with individual companies by sharing those same URLs in hashed form with all GIFCT members so that they can use the hashed URLs as a signal to identify outlinking from their platforms to terrorist content.

Prevention Through CVE Training

Ensuring that GIFCT's prevention efforts continue to aid practitioners and civil society, GIFCT and Hedayah have launched a partnership to ensure greater access to appropriate training and tools to counter violent extremist propaganda online. Building off of the initial resources of the GIFCT Campaign Toolkit and Member Resource Guide, GIFCT and Hedayah will be providing practitioner-focused training on digital platforms to interested governments, policymakers, civil society practitioners, and wider civil society organizations to better prevent the spread of violent extremist propaganda and to amplify counter-and alternative narratives to propaganda on digital platforms. This initiative aims to enhance cooperation and understanding of relevant online tools used by civil society organizations in their efforts to counter terrorism and violent extremism online.

GIFCT Strategic Pillar: Respond

Development of the Incident Response Framework

Following the attacks in Christchurch, New Zealand in March of 2019, GIFCT members established a centralized communications mechanism to share news and information about ongoing violent events that might result in the spread of violent content online produced as part of the specific offline event unfolding.

This year, we matured our Incident Response Framework, establishing three levels of response to offline terrorist events with an online aspect to guide how GIFCT and our members respond to events with different levels of online implications beyond the CIP that was developed in 2019:

Content Incident Protocol (CIP):

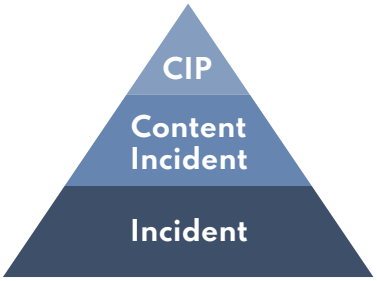
- An ongoing terrorist or mass violence event;
- Live-streamed or recorded video by perpetrator or accomplice;
- Depicting murder or attempted murder;
- On a member platform (or so broadly available online its spread is inevitable).

Content Incident (CI):

- An ongoing terrorist or mass violence event;
- Other content (ex. photo, audio, or text) by perpetrator or accomplice;
- Depicting murder, attempted murder, or violence from the attack;
- On a member platform (or so broadly available online it is inevitable).

Incident (I):

- An ongoing terrorist or mass violence event, threat, or attempt; *and*
  - » Content related to the terrorist attack but unclear whether depicting murder, attempted murder, violence, or bystander footage[1] from a terrorist attack **OR**
  - » Gaining international media attention or appearing to have a significant online element.



These communications allow for widespread situational awareness and a more agile response among member companies. Since establishing our Incident Response Framework, member companies have initiated communications in response to over **193** offline terrorist or mass violence events* in as close to real-time as possible, sharing situational awareness and information in real-time in an effort to identify any online dimension to the offline event.

1 Bystander footage is not considered terrorist or violent extremist content and so is not cause for activation of the incident response framework for the purpose of removing that content

Fig 1. The above map indicates the locations across six continents of offline terrorist or mass violence events between April 21, 2019 and October 31, 2021, that have resulted in communications as part of GIFCT's Incident Response Framework.

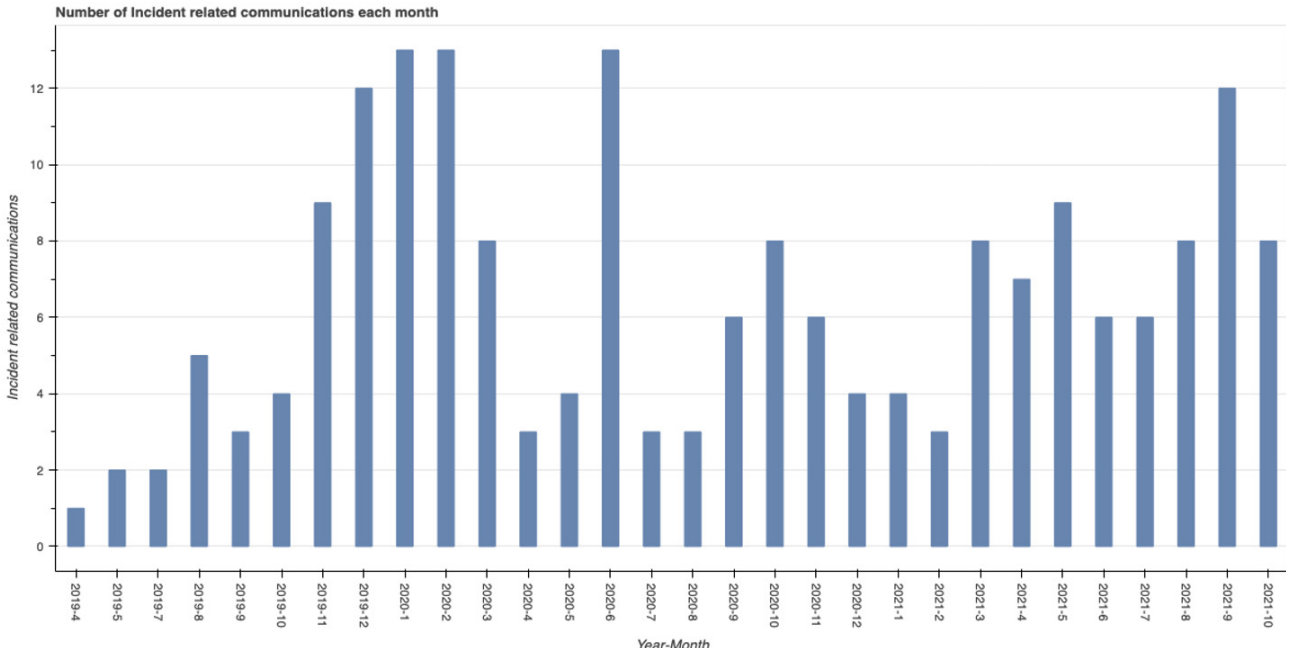


Fig 2. The above chart shows by month the number of offline terrorist or mass violence events between April 21, 2019 and October 31, 2021, that have resulted in communications as part of GIFCT's Incident Response Framework.

GIFCT Strategic Pillar: Learn

Knowledge Sharing and Expanding Access to Nuanced Information

Action-oriented learning is the third strategic pillar of GIFCT's work. As an independent NGO, GIFCT's goals include enabling multi-stakeholder engagement around terrorist and violent extremist misuse of the internet to meet key commitments consistent with its mission, as well as advancing a broader understanding of terrorist and violent extremist operations and their evolution, including the intersection of online and offline activities. GIFCT advances learning through (1) our Working Groups (discussed on page 18), (2) GIFCT's academic arm - the Global Network on Extremism and Technology (GNET) - and (3) our collaborative events with Tech Against Terrorism.

E-Learnings and Workshops

GIFCT partners with Tech Against Terrorism for monthly e-learning workshops that are open to global participants across sectors. While in-person workshops have temporarily been put on hold during the COVID-19 pandemic, in March 2021 Tech Against Terrorism and GIFCT launched monthly e-learning events in order to continue multi-sector knowledge-sharing by bringing global experts on key topics of interest to tech companies to the virtual stage. GIFCT works with Tech Against Terrorism to try to ensure that sessions span a diversity of topics, feature representation from different sectors, and include voices from around the world.

The following ten e-learning events in 2021 had **860** total participants join from across the globe and from a variety of sectors:

- The Nexus Between Violent Extremism and Conspiracy Theory Networks Online: Understanding and Challenging groups like QAnon, Oath Keepers and The Boogaloo Movement (March 17, 2021)
- Technical approaches to countering terrorist use of the internet: URL sharing and collaborative tech sector efforts (March 31, 2021)
- Countering Terrorist Use of Emerging Technologies: Assessing Risks of Terrorist Use of End-to-End-Encryption and Related Mitigation Strategies (April 29, 2021)
- The Nuts and Bolts of Counter Narratives: What Works and Why? (May 27, 2021)
- Mapping the threat: The T/VE online landscape in APAC and regional platforms' response (June 24, 2021)
- Supporting platforms' content moderation and transparency efforts: Existing resources and tools (July 22, 2021)

- United Nations' Efforts in Counterterrorism and CVE: Resolutions, Mandates and Partnerships (August 26, 2021)
- Online terrorist financing: assessing the risks and mitigation strategies (October 28, 2021)
- Countering terrorist use of the internet, moderating online content and safeguarding human rights (November 23, 2021)
- Future Forecasting post pandemic (December 14, 2021)

First Sub-Saharan Africa Virtual Workshop:

Terrorism & Violent Extremism in West Africa: Threat Mapping & Solution Building Online

While GIFCT in-person workshops have been put on pause due to the ongoing COVID-19 pandemic, GIFCT worked with the National Cyber Security Center in Ghana to convene our first Sub-Saharan Africa workshop virtually in October of this year. Sub-Saharan Africa had been highlighted as an under-engaged region for GIFCT, and the GIFCT Programming Team prioritized engagement to ensure better connection in the region and proactive outreach to regional partners across government, tech, and academia.

This virtual workshop convened West African stakeholders, focused on the regional terrorist and violent extremist threat landscape and its online dimensions, and laid the groundwork for in-person regional engagements in 2022. This session brought together a panel of experts and practitioners to share their assessments on how the threat manifests online and discuss new and emerging solutions to such challenges.

Representatives from Facebook, the Institute for Security Studies in the Regional Office for West Africa, the Sahel, and the Lake Chad Basin joined the panel alongside GIFCT's parters at Tech Against Terrorism and the National Cyber Security Centre (NCSC) of Ghana. These tech, government, and NGO experts discussed ways that terrorists use the internet, both regionally and globally, and examined specific risks of their use and exploitation of digital platforms to the region. This expert panel and participating audience further explored positive and sensible measures that can be taken to reduce the proliferation of violent extremist materials online and how tech companies operating globally and locally can adapt their counterterrorism responses.

This GIFCT Workshop, while virtual, marked the first GIFCT-hosted event on the African continent, as well as the first regional engagement organized since the start of the COVID-19 pandemic. The virtual event saw 176 participants from a range of West African sectors and countries.

GIFCT looks forward to continuing monthly e-learnings and in-person regional workshops when it is safe and appropriate to do so.

Trainings on Developing, Launching and Evaluating Online PVE & CVE Campaigns

GIFCT will continue to offer training and support to civil society organizations in their efforts to prevent and counter violent extremism online, through government and non-governmental networks. In 2021, GIFCT provided training to a range of international peacebuilders and activists in coordination with the following networks:

- Alliance for Peacebuilding (AfP)
- Commonwealth Youth Peace Ambassadors Network (CYPAN)
- Nordic Safe Cities
- Radicalization Awareness Network (RAN)
- Kofi Annan Foundation, Envision Together

Training sessions provide guidance on general online safety practices, understanding counterspeech in the online context, and practical information related to deploying online campaigns, measurement and evaluation. This training helps guide the audience through a range of GIFCT tech company resources within our Member Resource Guide and the Campaign Tool Kit materials for practical use. GIFCT looks forward to furthering these engagements and trainings in 2021.

Conducting & Funding Research with GNET

In January 2020, GIFCT began Phase Two of support for its academic research network, the Global Network on Extremism and Technology (GNET). GNET is led by the International Centre for the Study of Radicalisation (ICSR), based at King's College London.[2] GNET brings together an international consortium of leading academic institutions and experts with core institutional partnerships from the Australia, Germany, Singapore, the United Kingdom, and the United States, to study and share findings on terrorist and violent extremist use of digital platforms.

GNET Insights, Reports and Workshop Metrics

In 2021, GNET published 145 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 22 different countries: Australia, Austria, Belgium, Canada, France, Germany, India, Ireland, Italy, Malaysia, Morocco, Netherlands, Norway, Pakistan, Poland, Scotland, Singapore, Spain, Sri Lanka, Sweden, the United Kingdom and the United States. GNET's longer research papers are focused on terrorist and violent extremist use of technology, and offer actionable findings and practical solutions

2 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 in 2019 from GRNTT and can be found here.

to the tech industry. In 2021, GNET produced six reports from authors based in five different countries. Reports are available in English, French, German, and Arabic:

- Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities by Manjana Sold and Julian Junk (The Peace Research Institute Frankfurt)
- Conspiracy Theories, Radicalisation and Digital Media by Daniel Allington (King's College London)
- Polarising Narratives and Deepening Fault Lines: Social Media, Intolerance and Extremism in Four Asian Nations by Jordan Newton, Yasmira Moner, Kyaw Nyi, and Hari Prasad (The Centre of Excellence and National Security (CENS))
- Bringing Women, Peace and Security Online: Mainstreaming Gender in Responses to Online Extremism by Alexis Henshaw (Troy University)
- GNET Survey on the Role of Technology in Violent Extremism and the State of Research Community-Tech Industry Engagement by Lydia Khalil (The Lowy Institute)
- 'Fogging' and 'Flooding': Countering Extremist Mis/Disinformation After Terror Attacks by Martin Innes (Cardiff University)

To further facilitate multi-sector knowledge-sharing opportunities and to provide expertise to a range of stakeholders, GNET and GIFCT team with institutional partners in different parts of the world to curate 16 workshops focusing on the nexus between terrorism and technology. The workshops were held virtually from their home institutes in Australia, France, Germany, India, Netherlands, Singapore, the United Kingdom, and the United States. Topics included:

- The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021 (SLAID)
- The Digital Billion: South Asia, expanding online, and expanding extremism
- Under-researched topics in domestic violent extremism
- Online governance and right-wing extremism: Addressing challenges in proscription and Taxonomy
- Terrorist financing
- Content preservation and legal carve-outs for evidentiary content
- "The Fake as Virus: Towards an Epidemiology of Extremism"
- Extremism in 2021, January 6 and beyond
- Online intervention programs addressing right wing extremism
- "Right-Wing Extremism: East and West"
- Studying online radical Islamism in France after the Fall of IS

- Challenges faced by women researchers in the violent extremism and tech field
- Extremism in Australia – the nexus between terrorism and technology
- "The Gamification of Extremism"
- Far-right responses to the U.S. Capitol attack
- "Big Data, Counter-Terrorism and Transparency"

In May 2021, GNET launched its First Annual Conference which encouraged and facilitated discussions and dialogue between the tech sector and expert academics, civil society representatives, and government. The five different panels brought together a range of diverse topics and saw 350 to 400 unique visitors logging into the various sessions throughout the day.

Over the next year, GIFCT is looking forward to supporting GNET in facilitating mental health resources for researchers working in the terrorism and violent extremism space online. GNET is commissioning a project focused on secondary trauma suffered by academics and practitioners who are frequently exposed to disturbing material.

GIFCT looks forward to continuing its partnerships with Tech Against Terrorism and GNET in order to foster global knowledge-sharing and learning in 2022.

GIFCT 2021 Membership Updates

Newest Members to Join GIFCT

To date, we have achieved important progress towards our mission to prevent terrorist and violent extremist exploitation of digital platforms and our vision of a world in which the technology sector marshals its collective creativity and capacity to render terrorists and violent extremists ineffective online. A key milestone in our work to date has been the human rights impact assessment, which we commissioned in December 2020 and published this past July. That assessment recommended that GIFCT should take a "big-tent" approach to membership across the technology stack. At this point, we have been able to double the membership of the organization - from nine member companies at the end of 2019 when the process of establishing GIFCT as an independent organization began to **18 member companies today.**

This year, we were pleased to welcome five tech companies as the newest members to GIFCT, growing the diversity of digital platforms committed to our mission. Most recently, we've welcomed Zoom in addition to Airbnb, JustPasteIt, Wordpress, and Tumblr this past spring. New members bring new opportunities to learn how different companies approach their efforts to prevent terrorists and violent extremists from exploiting their platform or service, what they've achieved to date, and how we can collectively strengthen our capacity to counter terrorism and violent extremism online.

To learn more about how we approach and engage tech companies to join as members of GIFCT, see the new explainer video we provide on our website here.

Mentorship with Tech Against Terrorism

In its mentorship program supported by GIFCT, Tech Against Terrorism assesses and provides recommendations on platforms' overall transparency efforts and measurement against the GIFCT membership criteria.

GIFCT membership criteria

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

- Support for expanding the capacity of civil society organizations to challenge terrorism and violent extremism

Tech Against Terrorism's support model is based on a holistic approach to transparency reporting that recognizes that transparency is a process, in which transparency reporting is an outcome. To that effect, platforms need – and receive as part of the Mentorship Program – support in introducing and improving the policies and processes required to produce a transparency report. Tech Against Terrorism also works with GIFCT applicant companies to help assess whether companies meet the GIFCT membership critieria set forth above. The assessment is used to confirm a platform's capacity to receive reports of abuse on its services and that a platform has a desire to explore new technical solutions.

In 2021, the following companies have been assessed by Tech Against Terrorism to meet the GIFCT membership requirements and were accepted as GIFCT members:

- Zoom
- Airbnb
- JustPaste.it
- Tumblr
- WordPress.com

Assessment Criteria

Tech Against Terrorism uses the Tech Against Terrorism online assessment and the Tech Against Terrorism Pledge to help assess whether companies meet components the GIFCT membership criteria.

- The assessment is occasionally used to confirm a platform's capacity to receive law enforcement requests for information and content removal and that a platform has a desire to explore new technical solutions. Companies may also confirm meeting these two requirements in our update calls or via email.

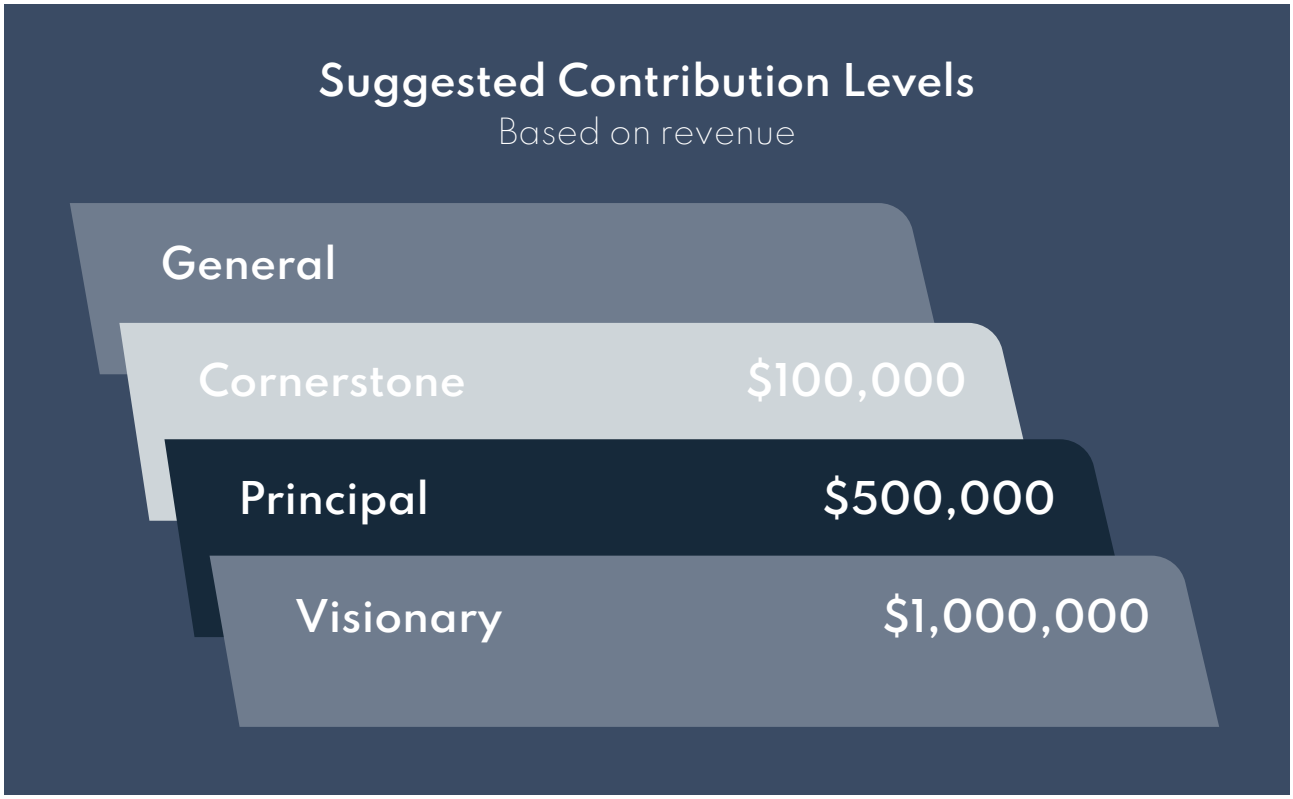
The Tech Against Terrorism Pledge – which all participating companies are asked to sign – is used to demonstrate a platform's "public commitment to respecting human rights, particularly free expression and privacy, when implementing content removal policies."

For a detailed overview of how the Mentorship Program works, please see the Tech Against Terrorism mentorship guide (shared separately).

Introducing the Membership Tiering Structure

GIFCT's mission and vision require us to continue expanding our membership to include more digital platforms committed to this work, further diversifying the range of platforms and digital services we support and where in the world they operate. The dynamic threat landscape we face and the migration of terrorist and violent extremist activity to different plaforms demand that GIFCT works to expand the circle of companies engaged in this important work. Growing our membership also means GIFCT learns how more platforms conduct their important work combatting terrorist activity and other bad actors on their services and allows us to provide more nuanced support and resources to our members (including the cross-platform tools that can be utilized by a broader range of companies). As this effort will increasingly require a broader and more sustainable resource framework, we have designed a framework for suggested contributions from members based on their respective revenue.

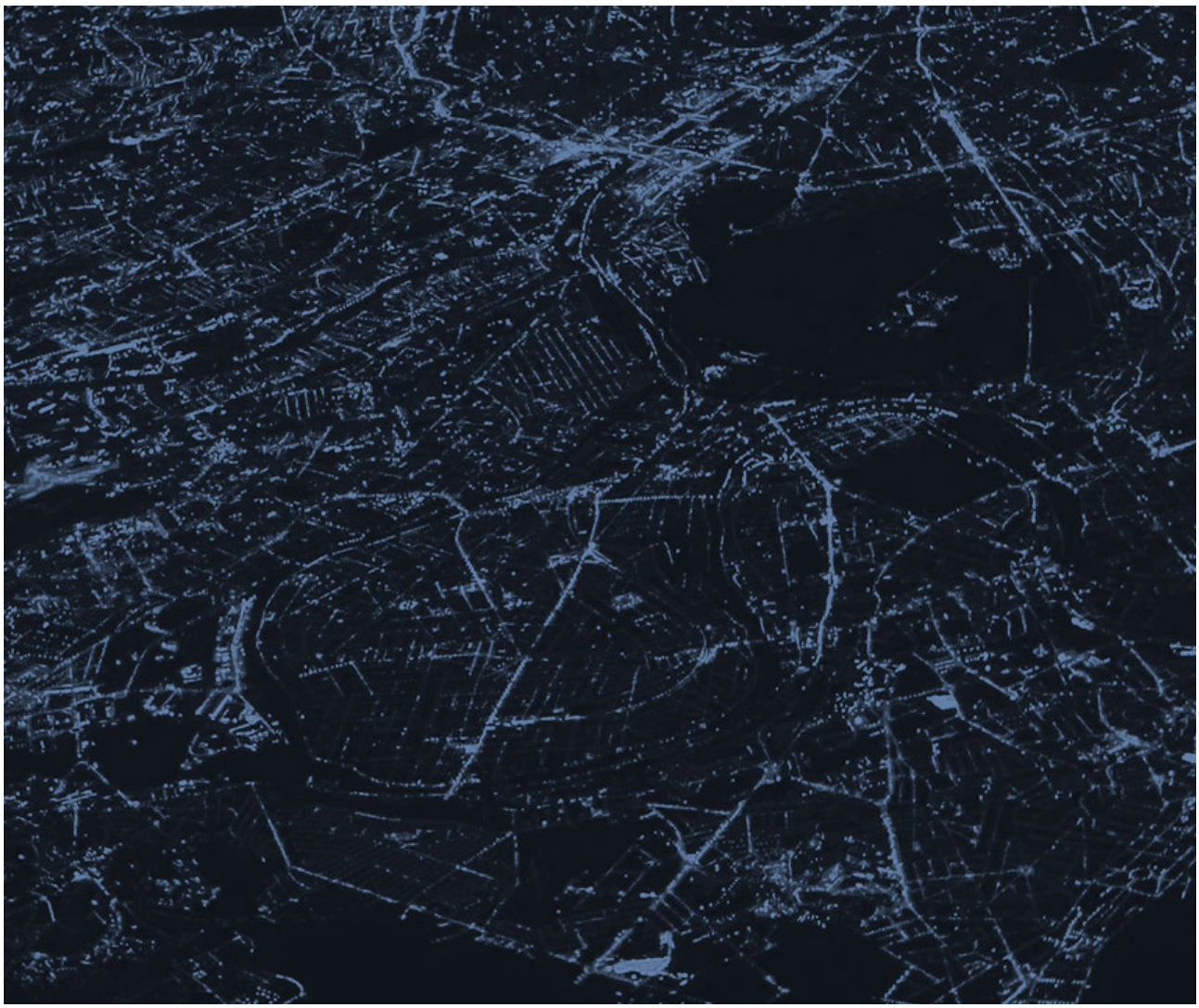
The GIFCT membership tiering structure we've initially designed establishes four levels of recommended contributions from member companies based on revenue while also ensuring that every member, including smaller companies with very limited resources, still have access to all of the operational benefits of GIFCT membership to strengthen their capacity to prevent terrorists and violent extremists from exploiting their platforms. We approached this work with the goal to provide a framework through which we can raise further contributions to GIFCT's operations while being transparent about our funding sources. While this membership tiering structure will guide our efforts to grow the resources of the organization, we will continue to be guided by our criteria for entry into GIFCT, not the prospect of a potential member's financial contribution, to determine new and ongoing membership.



This year, we are introducing the membership tiering structure and its framework in this report. Starting in 2022, this report will also include each company's level in the membership tiering structure based on their contributions to GIFCT that year.

Going forward, we will use this structure not only to help us grow our overall membership and the nuanced resources we provide to platforms, but also to diversify the leadership of our Operating Board of tech companies who help guide and advise on our strategic initiatives. Over the coming year, we will explore how best to have additional members who contribute at their suggested level join the Operating Board in either a permanent or rotating capacity.

We welcome the opportunity to have 2022 as a trial period where we work with our members to understand how we can best support them in navigating this structure and what further resources and cross-platform tools can produce the greatest impact towards our shared mission and vision. We look forward to ongoing discussions with our members regarding this framework and refining our approach in response to feedback.



GIFCT 2021 Financials

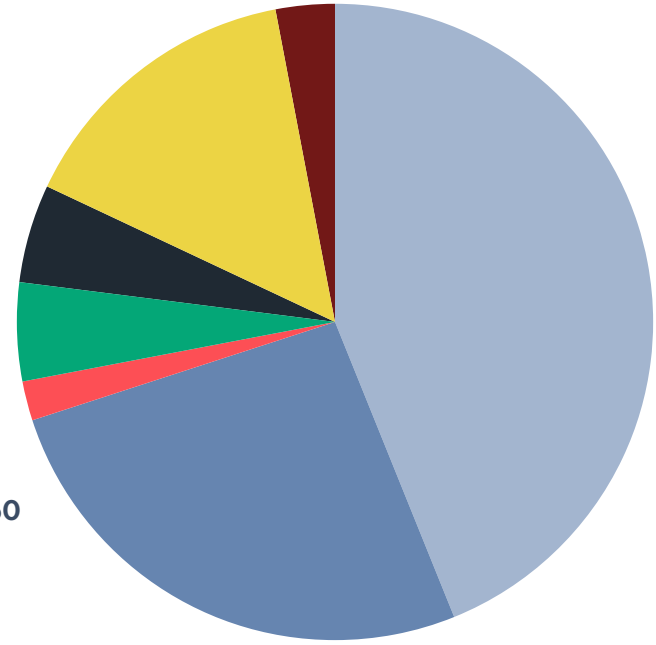
Support and Contributions

GIFCT's four founding member companies and Operating Board members - Facebook, Microsoft, Twitter and YouTube - currently fund GIFCT's operations. Since the initial founding of GIFCT in 2017, its four founding members have funded its operations, initiatives, and programs. In 2020, the four founding members provided additional contributions as start-up support for GIFCT as it began its own operations as an independent entity, providing a total of $7,114,350 that year, in addition to in-kind contributions to help support GIFCT operations and initiatives.

GIFCT intends to diversify and grow our resource framework in 2022 as we implement a new membership tiering structure (see page 37). As we move to implement this new framework, additional GIFCT member companies, including Amazon, Airbnb, and Discord have already stepped forward and signaled their willingness to contribute to GIFCT in 2021.

2021 Annual Contributions: **$3,200,000**

- Staff Salary/Employee Related Expenses + Contractor Services Fees: **$1,715,207**
- Partnerships: **$1,000,000**
- Programming: **$567,000**
- Vendor + Consulting Services: **$211,200**
- Tech Development: **$180,000**
- Administrative Expenses + Support: **$110,387.60**
- Independent Advisory Committee: **$90,000**

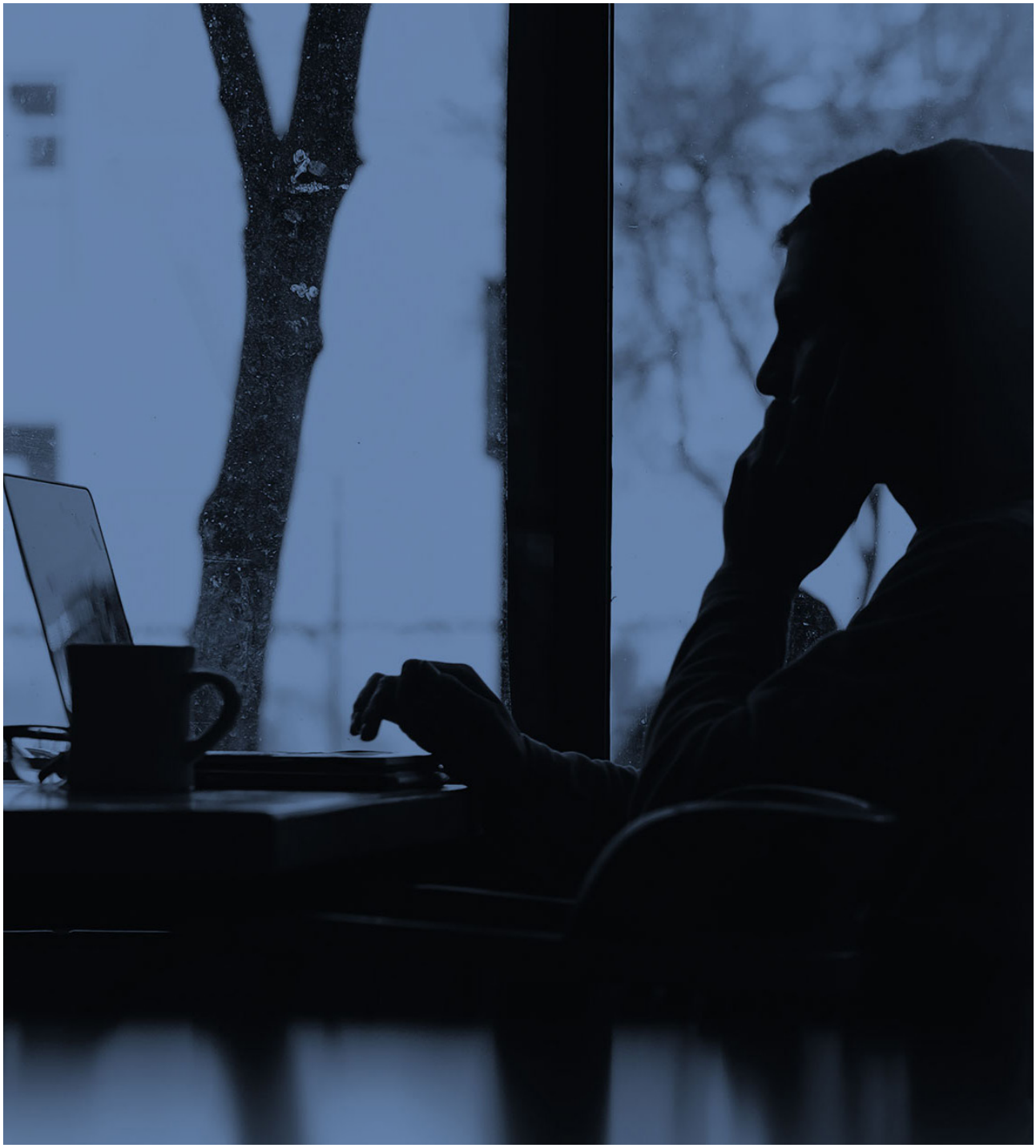


2021 Total Projected Expenses: **$3,874,294.60**

While this total for projected expenses is greater than total contributions for 2021, GIFCT is not operating at a deficit as a result of the additional contributions provided in 2020 as start-up support.

What to Expect in 2022

In 2022, we will implement our membership tiering structure to increase support for GIFCT's operations from additional members beyond the four founding companies. In turn, we will include the membership tiering structure in the GIFCT Financials section of the report and provide further information about the financial contributions we receive. We will also provide a further detailed report on our 2021 actual expenses when we file our IRS 990 form as a U.S.-based 501(c)(3) non-profit organization.



The Year Ahead: 2022

We look forward to the year ahead and to making concrete progress towards achieving a series of long-term objectives and goals.

As Executive Director Nicholas Rasmussen shared in his letter (see page 3), 2022 kicks off a multi-year initiative for GIFCT to achieve three strategic objectives during 2022 through 2024 that will guide our work:

1. Be a leading organization to convene, engage, and provide thought leadership on the most important and complex issues at the intersection of terrorism and technology, demonstrating with concrete output that multistakeholderism can deliver genuine progress.
2. Create a global, diverse, and expansive community of GIFCT member companies reflective of the ever-evolving threat landscape.
3. Build the collective capacity and capability of the industry by offering cross-platform technology solutions, information sharing, and practical research for GIFCT members.

More specifically in 2022, GIFCT will hold itself to account for efforts to achieve the following goals we believe are vital to reaching our longer-term strategic objectives and upholding our values:

Human Rights Impact Assessment
Early next year, we will publicly share a progress report on our work to respond to recommendations in BSR's human rights impact assessment of GIFCT. This was a commitment we made this past summer when BSR published the assessment and we laid out a roadmap for our plan to build its recommendations into our work across our initiatives and operations.

As we shared earlier in this report, we will continue to expand the diversity of the digital platforms and tech companies who join GIFCT as members, enhance the transparency of our hash-sharing database, and share GIFCT's approach to and understandings of terrorist content online and the effective strategies to combating terrorist and violent extremist exploitation of digital platforms.

Prevent
In line with our commitments to GIFCT's human rights impact assessment, we will focus on expanding the hash-sharing database's definitional framework for terrorist content to address anti-Islamist bias in the larger counterterrorism field in addition to enhancing the transparency of the database.

We will focus our expansion work on implementing the three additional categories of terrorist content we shared in July 2021 (see page 26) so that our member companies can utilize hashes of terrorist publications, terrorist manifestos, and URLs from Tech Against Terrorism's TCAP to detect potential activity and content on their platforms that violate their respective terms of service and policies. Additionally, GIFCT will strive to expand our hashing capabilities to include audio-hashing in addition

to image, video, text and PDF hashing.

As GIFCT expands our capabilities and taxonomy for the hash-sharing database, we know it is ever more crucial that we also enhance its transparency. Building on the additional information we began providing in the 2021 GIFCT Transparency Report, we will further seek to provide greater insights about the content currently hashed and the utility the database effectively provides to both large and small member platforms.

Respond

We will continue assessing and enhancing GIFCT's Incident Response Framework to identify gaps and strengthen our capacity to streamline cross-member communications and situational awareness during the critical period when an offline terrorism related event is unfolding and there is risk that it will become an event with a significant online dimension. We know that the dynamic threat landscape means that new risks and threats constantly emerge and so we must take every opportunity to enhance our collective ability to effectively respond to these attacks.

Learn

We are proud to continue our e-learning webinar programs in partnership with Tech Against Terrorism as well as our regionally specific workshops that enable experts, practitioners, tech, government, and civil society to share knowledge, lessons learned, and best practices on a wide range of topics at the nexus of terrorism and technology. We are also immensely grateful for the continued work and expertise of our partner the Global Network on Extremism and Technology as they embark on another year of research and analysis on current trends in the online terrorist threat landscape.

GIFCT
Global Internet Forum to Counter Terrorism

Thank You

We thank and applaud all of our member companies committed to our mission for the impact and progress we achieved this year, and we are grateful to the diverse array of participants in GIFCT Working Groups and to our vital community of global stakeholders for their hard work and important contributions. We look forward to 2022 and the opportunity it will provide to make meaningful progress towards our core mission of preventing terrorist and violent extremist exploitation of digital platforms.