

Introducing 2022 GIFCT Working Group Outputs

GIFCT WORKING GROUPS OUTPUT 2022



GIFCT
Global Internet Forum
to Counter Terrorism

Dr. Erin Saltman
Director of Programming,
GIFCT

In July 2020, GIFCT launched a series of Working Groups to bring together experts from across sectors, geographies, and disciplines to offer advice in specific thematic areas and deliver on targeted, substantive projects to enhance and evolve counterterrorism and counter-extremism efforts online. Participation in Working Groups is voluntary and individuals or NGOs leading Working Group projects and outputs receive funding from GIFCT to help further their group's aims. Participants work with GIFCT to prepare strategic work plans, outline objectives, set goals, identify strategies, produce deliverables, and meet timelines. Working Group outputs are made public on the GIFCT website to benefit the widest community. Each year, after GIFCT's Annual Summit in July, groups are refreshed to update themes, focus areas, and participants.

From August 2021 to July 2022, GIFCT Working Groups focused on the following themes:

- Crisis Response & Incident Protocols
- Positive Interventions & Strategic Communications
- Technical Approaches: Tooling, Algorithms & Artificial Intelligence
- Transparency: Best Practices & Implementation
- Legal Frameworks

A total of 178 participants from 35 countries across six continents were picked to participate in this year's Working Groups. Applications to join groups are open to the public and participants are chosen based on ensuring each group is populated with subject matter experts from across different sectors and geographies, with a range of perspectives to address the topic. Working Group participants in 2021–2022 came from civil society (57%), national and international government bodies (26%), and technology companies (17%).

Participant diversity does not mean that everyone always agrees on approaches. In many cases, the aim is not to force group unanimity, but to find value in highlighting differences of opinion and develop empathy and greater understanding about the various ways that each sector identifies problems and looks to build solutions. At the end of the day, everyone involved in addressing violent extremist exploitation of digital platforms is working toward the same goal: countering terrorism while respecting human rights. The projects presented from this year's Working Groups highlight the many perspectives and approaches necessary to understand and effectively address the ever-evolving counterterrorism and violent extremism efforts in the online space. The following summarizes the thirteen outputs produced by the five Working Groups.

Crisis Response Working Group (CRWG):

The GIFCT Working Group on Crisis Response feeds directly into improving and refining GIFCT's own [Incident Response Framework](#), 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. 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.

The second output from the CRWG is a paper on the Human Rights Lifecycle of a Terrorist Incident, led by Dr. Farzaneh Badii. This paper discusses how best GIFCT and relevant stakeholders can apply human rights indicators and parameters into crisis response work based on the 2021 GIFCT Human Rights Impact Assessment 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.

The final CRWG output is 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 and overlaps of protocols, and provides a set of recommendations for moving forward.

Positive Interventions & Strategic Communications (PIWG):

The Positive Interventions and Strategic Communications Working Group developed two outputs to focus on advancing the prevention and counter-extremism activist space. The first is a paper led by Munir Zamir 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.

The second paper, led by Kesa White, is on Good Practices, Tools, and Safety Measures for Researchers. This 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 (TAWG):

As the dialogue on algorithms and the nexus with violent extremism has increased in recent years, the Technical Approaches Working Group worked to produce a longer report on Methodologies to Evaluate Content Sharing Algorithms & Processes led by GIFCT's Director of Technology Tom Thorley in collaboration with Emma Llanso and Dr. Chris Meserole. While Year 1 of Working Groups produced a paper identifying the types of algorithms that pose major concerns to the CVE and counterterrorism sector, Year 2 output explores research questions at the intersection of algorithms, users and TVEC, the feasibility of various methodologies and the challenges and debates facing research in this area.

To further this technical work into Year 3, TAWG has worked with GIFCT to release a Research Call

for Proposals funded by GIFCT. This Call for Proposals is on Machine Translation. Specifically, it will allow third parties to develop tooling based on the [gap analysis](#) from last year's TAWG Gap Analysis. Specifically, it seeks to develop a multilingual machine learning system addressing violent extremist contexts.

Transparency Working Group (TWG):

The Transparency Working Group produced two outputs to guide and evolve the conversation about transparency in relation to practitioners, governments, and tech companies. The first output, led by Dr. Joe Whittaker, focuses on researcher transparency in analyzing algorithmic systems. The paper on 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.

The second output, led by Dr. Courtney Radsch, reports on Transparency Reporting: Good Practices and Lessons from Global Assessment Frameworks. The paper highlights broader framing for the questions around transparency reporting, the needs of various sectors for transparency, and questions around what meaningful transparency looks like.

The Legal Frameworks Working Group (LFWG):

The Legal Frameworks Working Group produced two complementary outputs.

The first LFWG output is about Privacy and Data Protection/Access led by Dia Kayyali. 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.

The second LFWG output focuses on terrorist definitions and compliments GIFCT's wider Definitional Frameworks and Principles work. This output, led by Dr. Katy Vaughan, is on The Interoperability of Terrorism Definitions. This 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.

Research on Algorithmic Amplification:

Finally, due to the increased concern from governments and human rights networks about the potential link 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 relation 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, she also looks at the potential agency played by algorithms, governments, users, and platforms more broadly to better understand causality.

We at GIFCT hope that these fourteen outputs are of utility to the widest range of international stakeholders possible. While we are an organization that was founded by technology companies to aid the wider tech landscape in preventing terrorist and violent extremist exploitation online, we believe it is only through this multistakeholder approach that we can yield meaningful and long-lasting progress against a constantly evolving adversarial threat.

We look forward to the refreshed Working Groups commencing in September 2022 and remain grateful for all the time and energy given to these efforts by our Working Group participants.

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)	ModusIzad - 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 (I267 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	

Crisis Response Protocols: Mapping & Gap Analysis

GIFCT Crisis Response Working Group

GIFCT WORKING GROUPS OUTPUT 2022



GIFCT
Global Internet Forum
to Counter Terrorism

New Zealand Government Representative

About this project

The Global Internet Forum to Counter Terrorism (GIFCT) has a multi-stakeholder working group dedicated to crisis response and incident protocols. The purpose of the Crisis Response Working Group (CRWG) is to improve members' collective ability to respond to online content incidents arising from real-world terrorist and violent extremist attacks in a manner that respects and protects human rights and a free, open, and secure internet.

In 2021–2022, CRWG has built on its level-setting exercise work in 2020-2021¹ by conducting a more detailed survey and mapping of the crisis response landscape. The aim of this exercise was to ensure that CRWG members' awareness was comprehensive and up-to-date and to inform CRWG's analytical and practical work in strengthening the multi-stakeholder response. This CRWG project also contributes to the Christchurch Call Community's Second Anniversary shared work plan for crisis response,² which called for a comprehensive mapping of all protocols that (a) defines the role of each, (b) describes individual thresholds for activation and stakeholder responsibilities, and (c) identifies where there are overlaps and gaps.

The project began with a survey of governments to check whether any had protocols in place or under development of which CRWG was not already aware. The next step was to develop and send a detailed questionnaire to the known protocol owners – the European Commission, GIFCT, the Christchurch Call, Australia, New Zealand, and the United Kingdom. The responses were collated in a detailed mapping and a gap analysis was conducted. CRWG has considered the views of protocol owners and stakeholders and has approached the exercise from both conceptual and thematic angles as well as operational ones, drawing on lessons learned from real-world experiences as well as tabletop exercises.³

Mapping the Protocols

CRWG's survey of the crisis response landscape as it exists in 2022 has not brought to light any unidentified protocols among governments in GIFCT Incident Response Directory or the larger set of Christchurch Call-supporting governments.

The United Kingdom's domestic protocol is the oldest. It was developed in 2017 after several terrorist incidents that year with an online dimension, including the Manchester Arena bombing in May. All the other multi-party and domestic protocols were developed in separate processes (but in view of each other) during the second half of 2019 following the launch of the Christchurch Call. All protocol owners (including the United Kingdom) support the Call and have committed to developing processes allowing governments and online service providers to respond rapidly, effectively, and in a

.....
 1 "GIFCT Crisis Response Working Group Annual Output," Global Internet Forum to Counter Terrorism, July 2021, <https://gifct.org/wp-content/uploads/2021/07/GIFCT-CrisisWorkingGroup21-AnnualOutput.pdf>.

2 See Second Anniversary of the Christchurch Call Summit, Joint Statement by Prime Minister Rt Hon Jacinda Ardern and His Excellency President Emmanuel Macron, co-founders of the Christchurch Call, May 2021, <https://www.christchurchcall.com/supporters.html>.

3 Note that this report predates the formal debrief on GIFCT's response to the Buffalo shooting and will need to be updated in light of those findings and recommendations.

coordinated manner to the dissemination of terrorist or violent extremist content arising from a real-world attack.

The earliest and key line of effort to fulfill that commitment was the development of the Call's Crisis Response Protocol (CRP), out of which GIFCT's own Content Incident Protocol (CIP) was built and into which it docked. Google hosted a workshop in Wellington in December 2019, facilitated by the Atlantic Council and involving GIFCT, its member companies, its Independent Advisory Committee members, Call-supporter governments, and civil society experts to test these arrangements and generate recommendations to improve them.

Almost three years have passed, and all the protocols remain – appropriately – works in progress. They are dynamic instruments that are tested, iterated, expanded, and refined based on experience and as real-world threats, technical capabilities, and policy contexts change.

Since 2019, the protocols have been tested on multiple occasions, including in response to shocking and tragic real-world attacks, and as a result have been updated and expanded in different ways. For example, GIFCT has used its experience responding to incidents since 2019 to develop the CIP into a more comprehensive, three-tiered Incident Response Framework (IRF) of which the CIP is the highest level. The Christchurch Call implemented an update to its CRP in 2021. Europol hosted a tabletop exercise involving all multi-party and domestic protocol owners in November 2021. The European Commission, as Chair of the EU Internet Forum, is currently leading work to develop guidance on crisis communications for inclusion in its protocol.

Reflecting their shared origins, the protocols are similar in nature, purpose, aim, scope, and usage. These similarities are useful for interoperability. There are, however, some important differences too.

Nature

All the protocols are voluntary in nature but grounded in robust legal frameworks that ensure due process and protection or respect for human rights. The protocols do not in any way override those legal frameworks at the international, national, or regional level.

Purpose and aims

All the protocols are designed to enable a rapid, coordinated, and effective response to an online content incident or crisis. The government-led protocols do so by enhancing communications among the participants, especially in relation to online service providers. Whether communications are enhanced at the operational or executive level depends on the jurisdiction. The government-led protocols aim to prevent and reduce harm to individuals, communities, and the public, while denying perpetrator(s) the opportunity to amplify their messages, gain notoriety and incite others, and further their cause.

As an industry-led arrangement, the purpose of the GIFCT IRF is necessarily different but

complementary. The focus of the GIFCT IRF is facilitating rapid information sharing with and among its member companies. The purpose is to improve situational awareness and, should the CIP be activated, to enable hash sharing so that those of its member companies that allow user-generated content can find and remove content quickly in accordance with their respective policies and procedures.

Scope: Harmfulness of content

All the protocols focus on extreme violent content. They require that the material depict or call for imminent serious harm to life.

The EU and Christchurch Call protocols require the content to be linked to a suspected real-world terrorist or violent extremist attack. The GIFCT protocol also allows for coverage of “mass violence,” acknowledging that it can be difficult to establish the link to terrorism in the early stages of an online incident and limitations around its current approach to defining terrorism. The Australian protocol covers terrorist material as well as material that depicts abhorrent and extreme violent conduct⁴. The New Zealand domestic protocol also covers other kinds of significantly harmful material⁵.

Scope: Who produced the content?

GIFCT requires that terrorist or mass violent content be perpetrator- or accomplice-produced but excludes bystander footage. Other protocols also tend to focus on perpetrator- or accomplice-produced content, but take a more case-by-case approach to bystander footage. For example, the UK protocol has bystander footage in scope where it exceeds a threshold and breaches online providers’ terms of service. The judgment often depends on inferring the purpose of the person in producing and sharing the content; where they are acting in support of the attacker and their cause, the content would be in scope.

Scope: Is it a crisis?

Each protocol has activation criteria related to the nature of the content. Most also have criteria or thresholds for determining whether the situation is a crisis, and they are reasonably well aligned across the protocols. Decision-makers are typically required to assess how fast and widely the content is spreading (or likely to spread), and how many countries and online service providers may be impacted. For example, the EU Crisis Protocol contains a risk matrix which has also been incorporated into the Christchurch Call CRP. Fundamentally, these assessments are about determining whether usual governmental or business processes are adequate to find and refer/remove or otherwise act on the content, or whether enhanced communications and cooperation are necessary.

.....

4 See the [Subdivision H of Division 474 of the Australian Criminal Code](#) and the [Online Safety Act 2021](#) for a more detailed definition of ‘abhorrent violent conduct’.

5 This includes content that is or is likely to be ‘objectionable’ in New Zealand’s [Films, Videos, and Publications Classification Act 1993](#), and/or content that should not be visible and viewed by vulnerable members of society due to the level of harm it can cause.

Usage

As was observed by CRWG in 2021–2022, these protocols are for extraordinary situations. Business for Social Responsibility (BSR) has noted that crisis response entails making decisions at speed and therefore mistakes may be made, impacting human rights or internet freedoms.⁶ It is therefore important that activation criteria and thresholds are reasonably robust, especially when activating a protocol engages additional powers or tools.

It is good that activations therefore remain rare; for example, GIFCT has only activated a CIP on three occasions, and in general the protocols have not been used to initiate many coordinated content takedowns. Nevertheless, the protocols have been successful in connecting and strengthening the relationships between the relevant players across sectors, increasing situational awareness of online bad actors and violating content, and improving monitoring, coordination, and communications.

Strengthening crisis response

CRWG considered the desired outcomes for crisis response – i.e., what success would look like – as well as the elements that must be in place to achieve that and potential gaps. It is worth noting that none of the gaps were previously unknown to CRWG or the wider crisis response community, although recent events (e.g., in Ukraine and Buffalo) have thrown some into starker relief. The good news is that there is already considerable work underway within GIFCT and elsewhere to address known weaknesses.

The value of the crisis response mapping exercise has been in systematically thinking through and comprehensively laying out the known issues as a basis for CRWG to prioritize its own work, for the Independent Advisory Committee to advise GIFCT on priorities for organizational development, and for the broader crisis response community to move forward together. On that basis, CRWG makes the following recommendations:

Scope

- GIFCT should continue work in 2022 towards a **comprehensive, behavior-based definitional framework** for its work, including the IRF. This is critical in addressing the trend away from attacks by proscribed groups and towards attacks by individuals inspired and motivated by disparate ideologies in online extremist communities. This work may also assist other industry bodies like Tech Against Terrorism and companies inside and outside GIFCT in developing their own more comprehensive definitional frameworks.
- CRWG should convene an expert discussion on **legitimate exclusions and the treatment of bystander footage** in the IRF, other protocols, and GIFCT member companies' terms of service. CRWG's tabletop exercise in April 2022 highlighted the challenges of differentiating content

.....
⁶ Business for Social Responsibility, "Human Rights Assessment: Global Internet Forum to Counter Terrorism," Global Internet Forum to Counter Terrorism, July, 2021, https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf.

captured from different vantage points (perpetrator, CCTV, bystander) and/or shared for different purposes (e.g., in condemnation or support of the attack, as an eyewitness account, as a safety message, or as part of journalist reporting). A deep dive on this subject would help clarify the boundaries between violative and legitimate uses of content in crisis situations.

- CRWG may also wish to consider the treatment of content related to acts of **state-sponsored terrorism and violent extremism** across the different crisis response protocols, in light of recent events in Afghanistan and Ukraine.

Participation

- GIFCT and the Christchurch Call should extend the Incident Response Directory and Crisis Response Protocol to more **governments** (subject to appropriate criteria and safeguards). This is a particular priority for the Christchurch Call, as it is the only mechanism available to most non-EU governments to initiate a collective response. CRWG may also convene a discussion for all protocol owners and participants on how best to engage with **third countries** (currently outside the protocol), especially where legal frameworks and human rights protections are less developed.
- CRWG should identify the **different kinds of online services** that may be exploited by terrorists, violent extremists, and supporters during and immediately after an attack and think about how to achieve broader engagement and effective coverage of this online ecosystem. The crisis response community should support **GIFCT's** efforts to identify companies aligned with its mission and to bring them on board as members, using the mentoring services provided by Tech Against Terrorism. We should also support **Tech Against Terrorism** in developing its Terrorist Content Analytics Platform (TCAP) to deal with a broader range of content types and extend its alerting function. Working with GIFCT and Tech Against Terrorism, we should survey a range of **smaller platforms** to understand any barriers they face to mounting effective crisis responses, and what additional shared tooling and other practical supports would be useful. Finally, we should discuss how to deal with those online service providers that resist self-regulation and voluntary cooperation, including through **legislative and enforcement action**.
- CRWG should continue to develop the **role of civil society and researchers** in crisis response. As recognized in the Christchurch Call and the Bergen Plan of Action, there is potential to better utilize the expertise and skills of a global network of individuals and organizations committed to combatting terrorist and violent extremist content online and realizing a vision of the internet as a force for good. For example, they could assist GIFCT companies and governments in finding violative content across the internet and address it quickly in a rights-respecting way.

Operational Issues

- To meet the expectations of stakeholders, GIFCT should maintain its current **capacity to monitor and respond to incidents 24/7** and work with its member companies to build the resiliency of that posture.
- GIFCT should build on successful technical tools such as hashing and matching videos/images and early-stage solutions for text and PDFs to explore solutions to hash **audio content**. GIFCT

should also work with member companies to fully operationalize the hashing of **URLs** in the TCAP as a powerful way of disrupting out linking from GIFCT members' platforms to off-platform repositories of CIP-related content.

Data Preservation and Access

- Building on CRWG's report in 2020–21 and Europol's November 2021 tabletop exercise, the crisis response community should find appropriate ways to advance the discussion of the principles guiding proactive information sharing in threat-to-life situations, and proactive data preservation for domestic and cross-border law enforcement purposes, with a view to making concrete progress in these areas.
- Both the Christchurch Call and EU protocols point to the desirability of preserving data so it can also be accessed for other legitimate purposes, including journalism, research, international investigations, and judicial processes. This is key to operationalizing victims' right to access effective remedies. GIFCT and the wider crisis response community should continue to explore and further develop solutions like Tech Against Terrorism's TCAP archive and integrate them into a coordinated and comprehensive crisis response system.

Crisis Communications

- According to the EU's Radicalisation Awareness Network (RAN) Policy Support, good crisis communications can reduce the opportunity for terrorists and violent extremists to draw strategic benefits in the aftermath of an attack. The Christchurch Call and other protocol owners should therefore consider developing strategic communications frameworks, building on the principles in the EU Crisis Protocol and the work being done by RAN-PS on practical guidance for implementing the principles.

Cross-Cutting Issues

- GIFCT and other protocol owners should apply the human rights matrix developed in CRWG in 2021–22. The purpose of the matrix is to help practitioners identify the individuals and groups whose rights may be at risk at different points in the "lifecycle" of a response with a view to preventing or mitigating negative impacts. The matrix is a work in progress, and in the future CRWG could focus on refining the human rights indicators in the matrix and developing a framework for assessing the impacts of actions at each stage of response. Protocol owners may wish to tailor the matrix and indicators to their process and practice using them in exercises. Stakeholders may also use this work to structure a human rights impact assessment as part of any debrief and review.

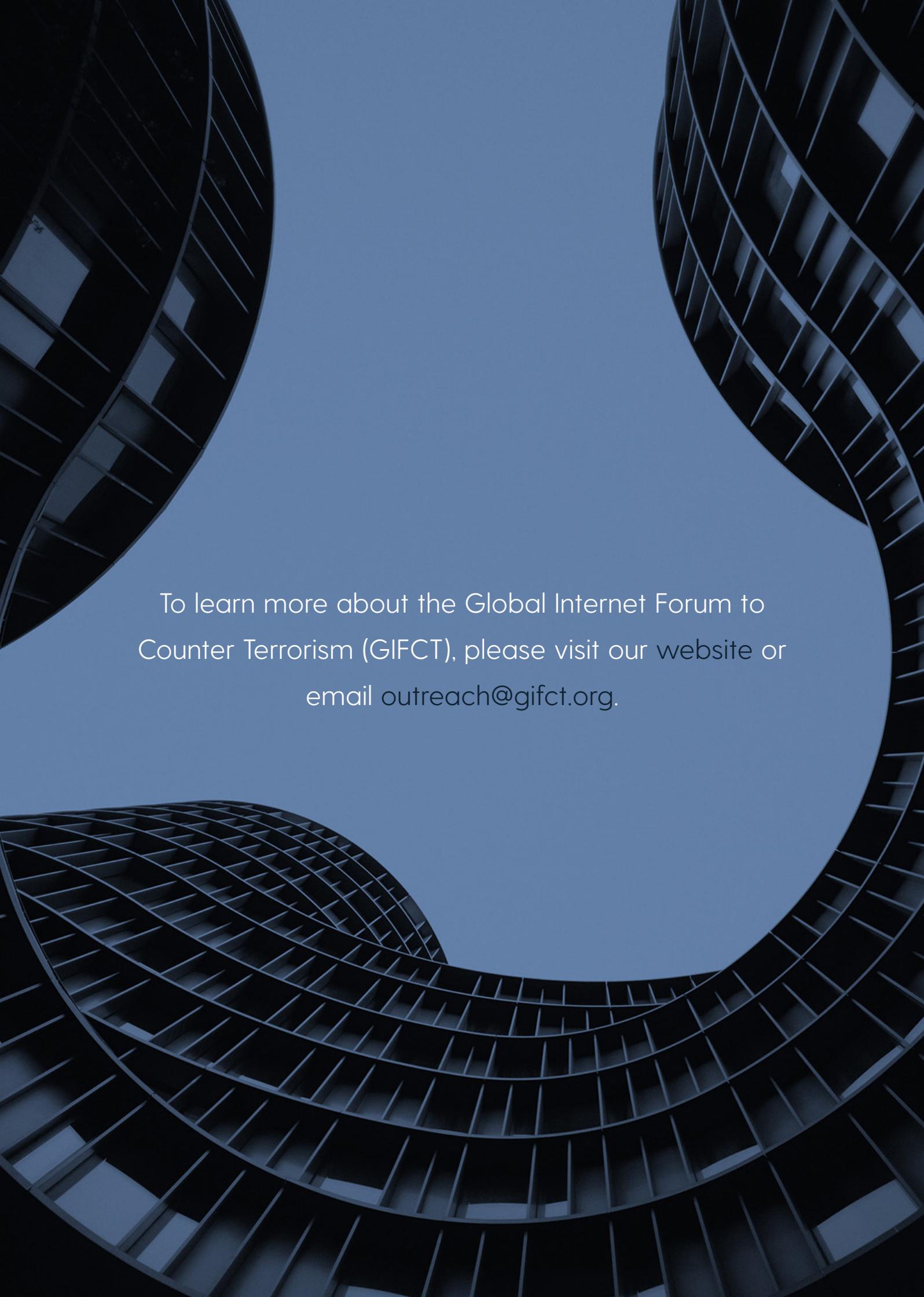
Immediate next steps

- GIFCT will provide a formal debrief of the Buffalo incident in accordance with the framework

developed by CRWG last year.⁷ That will be an opportunity for the organization, its member companies, and government and civil society stakeholders to reflect on the incident and the response, and to identify ways to improve again on our collective response networks, tools, and processes. As a contribution to future debriefs, and as part of ongoing work to develop good practices for transparency around the different stages of crisis response, CRWG could do work in 2022–23 on the best **metrics for evaluation**, so we can better assess our progress and demonstrate it to others.

- CRWG will use this mapping and gap analysis, complemented by the Buffalo debrief findings and recommendations, as a basis for identifying and prioritizing its work in 2022–23 and beyond. CRWG will ask protocol owners to update the information in the mapping each year to ensure members' knowledge of the crisis response landscape remains up-to-date and as a basis for more detailed investigations in specific areas.

.....
⁷ "GIFCT Crisis Response Working Group Annual Output," Global Internet Forum to Counter Terrorism, July 2021, <https://gifct.org/wp-content/uploads/2021/07/GIFCT-CrisisWorkingGroup21-AnnualOutput.pdf>.



To learn more about the Global Internet Forum to Counter Terrorism (GIFCT), please visit our website or email outreach@gifct.org.