

GIFCT Crisis Response Working Group Annual Output

July 2021





Executive Summary

The Global Internet Forum to Counter Terrorism (GIFCT) Crisis Response Working Group (CRWG) was established in April 2020 as part of the GIFCT substantive Working Group structure. The CRWG's objective is to drive effective collaboration among industry, government, and law enforcement to minimize the spread of terrorist or violent extremist content online stemming from an offline event.

Since April 2020, the CRWG has been facilitated by Microsoft and co-led by five representatives from the European Union. The CRWG's membership consists of 19 individuals, accounting for representatives from all sectors. Additionally, the chair of the GIFCT Independent Advisory Committee (IAC) is invited to attend working group meetings in an observer capacity. While members of civil society are part of the overall working group, their involvement to-date has been limited.

Since its inception, the CRWG has met regularly in plenary sessions and on numerous occasions in smaller groups to advance the work of three subworking groups (WGs). These three sub-WGs focused on the following initiatives:

- Sub-Working Group #1: Creating and adopting a confidential Incident Response Directory for crisis response communications and informationexchange between and among participating governments and GIFCT member companies
- Sub-Working Group #2: Establishing a process for conducting Cross-Sector Debriefs (following the initiation of one or more protocols) to allow feedback for review and updates as needed
- Sub-Working Group #3: Identifying the Operational and Investigative Requirements of law enforcement agencies during a protocol-initiating event

This summary report – an abbreviated version of the CRWG's first Progress Report delivered in April 2021 – outlines work to-date with a particular focus on the deliverables of the three sub-WGs. These initial priorities were selected given their practical but essential nature in order to improve joint responses and to ensure the CRWG is continually integrating existing work and adapting to new information. In addition, the report suggests future priorities for the WGs for the remainder of 2021 and into 2022.

Early Formation and Focus + Sub-working Groups

Early Formation + Focus

At its earliest meetings, the CRWG established Operating Guidelines, reviewed the outcomes and outputs of previous crisis response tabletop exercises, and conducted a substantive "level-set" at which emergency response protocol owners completed a common template and shared the operational details of their individual protocols.

From this level-setting exercise, a summary document of existing protocols was compiled, setting out the key elements of the protocols, including their purpose, activation criteria, procedural steps and information about protocol-initiating events. The goal was to leverage this summary in targeted outreach to other geographies to encourage the creation (and joining up) of (potentially new) additional protocols to the WG process.

Sub-Working Groups

As part of the CRWG strategic plan, the WG formed three initial sub-working groups to deliver at least three separate and discrete work products, namely:

- A confidential Incident Response Directory for crisis response communications (as well as relationship-building and informationexchange);
- A process for conducting Cross-Sector Debriefs upon initiation of various emergency protocol(s); and
- A catalog of the Operational and Investigative Requirements for law enforcement agencies in cooperation with GIFCT member companies.

Below is a summary of the outputs from each of these sub-WGs.



Sub-working Group #1

Incident Response Directory

To enable prompt and effective communications during a crisis, this sub-WG developed a dynamic list of contacts (the "Incident Response Directory") that would enable notifications to be sent to each participating country and GIFCT member company. In addition to creating such a directory to receive crisis response notifications, the project provided an opportunity to build a broader GIFCT crisis response network and strengthen bilateral relationships. The creation of the database directory by the sub-WG therefore served a dual-purpose.

The directory includes primary contacts for each participating entity to receive notifications during a real-world event. These primary contacts include shared mailbox (or "alias") addresses to ensure any emergency communications are sent to multiple relevant contacts within a given organization.

To support the networking aspect of the directory, countries and companies can also provide additional contacts, allowing for broader situational awareness apart from specific content decisions.

The GIFCT organization is the custodian of the Incident Response Directory and continues to work with countries and companies to populate the database. When the GIFCT Content Incident Protocol or other crisis protocol is next initiated, the directory will be leveraged and all primary contacts will be notified, allowing those contacted to cascade information within their country or company, generating a more streamlined response.

Sub-working Group #2

Cross-Sector Debriefs

With an eye toward continuous improvement to sufficiently respond to evolving threats, the goal of this sub-working group was to create a process by which representatives from all sectors could jointly review, analyze, and suggest improvements to protocol processes following a real-world terrorist or violent extremist event. The group recommended a two-tier process for mandatory (Tier 1) debriefs and elective/by-request (Tier 2) debriefs, depending on the number and type of protocols initiated.

Tier 1 Debriefs

A Tier 1 debrief is defined as a formal, cross-sector process (i.e., government, law enforcement, the GIFCT organization and its member companies, and civil society). A Tier 1 debrief is mandatory following the initiation of at least two crisis protocols (e.g., GIFCT CIP + domestic/ other) in response to a real-world terrorism or violent extremism event. Tier 1 debriefs will be organized and led by the impacted government(s) in conjunction with GIFCT, and held within a reasonable time period following the conclusion of the various protocols at issue. The targeted time frame is within six weeks of the real-world event, but Tier 1 debriefs will be planned and carried out on a case-by-case basis.

Tier 2 Debriefs

A Tier 2 debrief is defined as a formal, cross-sector process involving tobe-determined participants at the request of one or more stakeholders following the initiation of at least one crisis protocol (i.e., GIFCT CIP or other protocol) in response to a real-world terrorism or violent extremism event.

Upon completion of either a Tier 1 or a Tier 2 Debrief, the organizing entity is encouraged to submit a summary report to GIFCT, and a template was developed for this purpose.



Sub-working Group #3

LEA Operational and Investigative Requirements

The objective of this sub-working group is to identify the operational and investigative requirements of law enforcement agencies during a protocolinitiating event and examine the role of industry in safeguarding those requirements.

The sub-WG, initially consisting of law enforcement and government representatives, drafted a set of "Principles for Collaborative Action" to assist in cooperation during a protocol-initiating event.

These principles include:

- Acknowledging and committing to a collective response;
- Fostering the proactive sharing of information and disclosure of critical information (i.e., threat to life) connected to terrorist or violent extremist content; and
- Enabling proactive data-preservation.

In addition to these principles, the sub-working group has also documented law enforcement minimum investigative requirements during a protocolinitiating event. These investigative requirements include questions about the perpetrator and/or accomplice(s), what modified media is manifesting online, the tech companies impacted, and data that may be provided.

These outputs have helped to identify gaps for GIFCT to help address the operational needs of law enforcement during the active phase of a protocol. The initiatives of this group continue to develop, including work that might go beyond the scope of the CRWG. GIFCT and CRWG co-leads are currently exploring alternative fora to best address the requirements of law enforcement during (as well as beyond) a protocol-initiating event.



Next Set of Proposed Priorities

As the work of the three initial sub-WGs approaches completion, the GIFCT CRWG outlined its next set of proposed priorities:

- Building on the initial steps taken to ensure effective communication among industry, government, and first responders during a crisis response protocol-initiating real-world event. These might include scoping the creation of an automated alerting system, refining the types of information that might be shared among GIFCT stakeholders during an incident, and the transition from individual points of contact to shared mailbox or "alias" addresses;
- 2. Consulting and advising GIFCT as it builds its broader Incident Response Framework to address scenarios that do not meet the threshold of a CIP;
- 3. Defining and devising a plan for "operational excellence" across stakeholder groups when multiple protocols are initiated;
- 4. Scoping and organizing a tabletop exercise involving all stakeholders to test all known protocols (and involving civil society in such efforts); and
- 5. Ongoing engagement with the Christchurch Call to Action forum to support crisis response best practices being shared among a more diverse set of stakeholders.

Conclusion

In conclusion, the GIFCT CRWG has made substantial progress toward its initial priorities, including improved communications through an Incident Response Directory, structured protocol reviews through debrief processes, and enhanced understanding of the operational requirements of law enforcement. These achievements have helped the CRWG identify a next set of priorities centered around continuing to streamline GIFCT stakeholder responses in the event of an offline attack with online implications. Looking forward, the CRWG welcomes future participation from other governments as they consider and develop new crisis response protocols as well as increased participation of civil society organizations focused on safeguarding human rights.

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

