

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
Automatic	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	

Human Rights Lifecycle of a Terrorist Incident Online

GIFCT Crisis Response Working Group

GIFCT WORKING GROUPS OUTPUT 2022



GIFCT
Global Internet Forum
to Counter Terrorism

Dr. Farzaneh Badii
Digital Medusa

Executive Summary

From January 15 to May 31, 2022, the Working Group on Crisis Response Protocols (CRWG) – a subgroup of the Global Internet Forum to Counter Terrorism (GIFCT) – met with stakeholders across civil society organizations, governments, academics and companies (through a series of individual and group meetings in addition to tabletop exercises). The output of this effort is the present report that aims to:

1. Outline the lifecycle of a terrorist incident on the Internet and its human rights impact;
2. Propose a framework for crisis protocol operators and GIFCT to use for explicating the lifecycle of incidents and to consider human rights implications in crisis response; and
3. Clarify the relationship between human rights and GIFCT's mission through explaining the human rights impact at each stage of the crisis lifecycle.

Broadly speaking, the output of the report is centered on an analysis of the lifecycle of a terrorist attack online, mapped against nine actual case studies (from Halle to Christchurch), and brings together the stages of the crisis protocol with their implications for human rights.

Crisis Protocol Stages: This section outlines the different stages of a terrorist incident on the Internet, from Horizon (before an attack takes place) to the Conclusion (which includes actions from standing down a response through to conducting debriefs). Definitions of each stage and particular categories of mapping, such as the type of attack or the virality of the attack, are available throughout the report.

Human Rights Principles: At each stage of a crisis, a number of potential human rights are potentially impacted. These human rights, which may include privacy, nondiscrimination and equality before the law, and access to effective remedy are mapped against not only the Crisis Protocol Stage but also the rightsholders based on a 2021 Human Rights Assessment undertaken by Business for Social Responsibility for GIFCT. Rightsholders include but are not limited to victims of terrorism and violent extremism, victims of efforts to counter terrorism and violent extremism, human rights defenders, the accused, and particularly groups spanning women, girls, and families as well as men and boys.

Using actual case studies coupled with a series of tabletop exercises enabled us to refine the proposed framework for crisis protocol operators in the event of a terrorist incident on the Internet. However, this framework should be considered a starting point for future discussions and investigations on how terrorism manifests online, appropriate and effective methods for crisis response across relevant groups, and the human rights potentially impacted at each stage of response. In collaboration with civil society, government, academic and industry partners, we look forward to continuing to grow and refine this framework in the future.

Background

The Working Group on Crisis Response Protocols (CRWG), a subgroup of Global Internet Forum to Counter Terrorism (GIFCT), drafted this report to:

1. Outline the lifecycle of a terrorist incident on the Internet and its human rights impact;
2. Propose a framework for crisis protocol operators and GIFCT to use for explicating the lifecycle of incidents and to consider human rights implications in crisis response; and
3. Clarify the relationship between human rights and GIFCT's mission through explaining the human rights impact at each stage of the crisis lifecycle.

This report also contributes to the Christchurch Call work plan for crisis response, which includes establishing due process and human rights protections, to ensure all protocols are developed and implemented in a robust way.

Method

We have used a mixed method approach to draft this report, but mainly employed an iterative process by interviewing several stakeholders involved with tackling online crises. These include civil society organizations, academics, tech-corporations and law enforcement agencies. We have also made use of the table-top exercises that were held by GIFCT to develop the indicators of human rights impact.

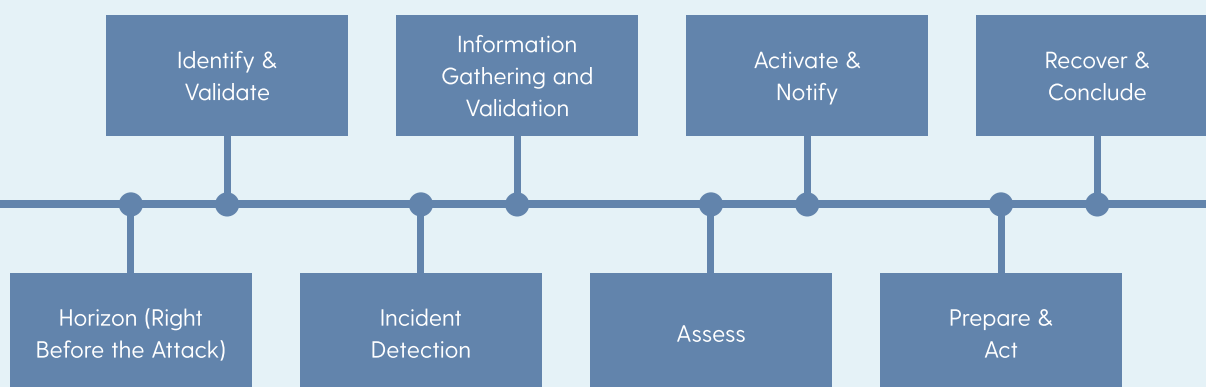
This report provides categorical tables about various terrorist and violent extremist incidents with an online impact. Through case studies it then describes each stage of the crisis protocol and its human rights impact and provides a framework for understanding the possible level of human rights impact at each stage of the crisis protocol.

Crisis Protocol Stages

The stages of crisis protocol described here are a combination of common practices of various crisis protocols and the sub-group's ideas. The horizon stage was specifically added by the sub-group. The stages are as follows:

1. Horizon (right before the attack)
2. Identify and validate (Stages 2 through 6 may involve contact/cooperation with third party governments and OSPs and industry bodies like Tech Against Terrorism (TAT)).
3. Incident detection (through internal monitoring, or a tip received from a partner organization, or media reporting).
4. Information gathering and validation/part of pre-activation (seeking information to understand what has happened or is happening and ensure that understanding is valid, i.e. corresponds to reality).
5. Assess/also part of pre-activation (whether the incident meets criteria/thresholds for activation, such as murder or mass violence, has a terrorist or violent extremist motivation,

- content was produced by perpetrator, accomplice or supporter, has potential to go viral).
6. Activate and notify (activate the protocol, notify the members, inform them of the level of action needed (monitoring or doing more), maybe also notify civil society organizations and the public).
 7. Prepare and Act/active response and information sharing (look at Open Source Intelligence (OSINT) materials, share hashes and awareness about where the content is, take action to find/moderate/remove content, preserve data, share actions and outcomes, ongoing strategic communications).
 8. Conclude (assessment against threshold, stand down response, notify members/stakeholders/public, may continue to monitor, documenting decisions/actions, organizing debrief/multistakeholder review, sharing findings with stakeholders and public).



Human Rights Principles

The human rights principles referred to above are based on the Business for Social Responsibility (BSR) human rights impact assessment of GIFCT.¹ They include:

1. Life, liberty, and security of person (UDHR 3; ICCPR 6, 9)
2. Nondiscrimination and equality before the law (UDHR 1, 2, 7; ICCPR 2, 3, 26; ICESCR 2, 3; CEDAW 2; CERD 2)
3. Access to effective remedy (UDHR 8; ICCPR 2)
4. Freedom of opinion, thought, conscience, and religion (UDHR 18, 19; ICCPR 18, 19)
5. Freedom of assembly and association (UDHR 20; ICCPR 21, 21)
6. Privacy (UDHR 12; ICCPR 17)
7. Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence

.....
¹ Dunstan Allison Hope, Lindsey Andersen, and Susan Morgan, "Human Rights Assessment, Global Internet Forum to Counter Terrorism," Business for Social Responsibility, July, 20, 2021, <https://www.bsr.org/en/our-insights/report-view/human-rights-impact-assessment-global-internet-forum-to-counter-terrorism>

before being proven guilty (UDHR 9, 10, 11; ICCPR 14; CERD 5)

Whose Human Rights

In order to draw a human rights lifecycle, it is also important to mention whose rights (as well as what rights are affected). Most of the following are taken from the BSR Human Rights Impact assessment report (we added “the accused” to the group of people whose rights might be affected).² We decided that economic and social groups might be impacted in the longer term and do not squarely fit the crisis protocol framework, so we might not include formal, societal, practical discrimination and hidden groups in the lifecycle.

1. Victims of terrorism and violent extremism

These rightsholders are the direct victims of terrorist activities that have an online angle. They are usually the ones that are the targeted group or the casualty.

2. Victims of efforts to counter terrorism and violent extremism

The victims of efforts to counter terrorism include groups that are adversely impacted by efforts to counter terrorism and violent extremism online. These groups are usually subject to overbroad or wrongful content removal or other actions. Another group is those who do the counterterrorism activities such as law enforcement, tech company security research departments, and those who undertake OSINT. Exposure to terrorist materials and undertaking research about these issues can affect the rights of these groups.

3. Human rights defenders

Human rights defenders include professional and citizen journalists, civil society organizations, nonviolent political activities, and members of vulnerable groups advocating for their rights.

4. Women, girls, families, men, and boys

According to the BSR report women, girls, and families as well as men, boys and the LGBTQI+ community can be disproportionately hampered by terrorist and extremist content, for example arising from problematic use of gender stereotypes in efforts to counter terrorism and violent extremism.³

5. The accused

The accused is the potential perpetrator that might be identified as the person behind spreading terrorist and violent extremist content.

The list of impacted rightsholders is not exhaustive, as it is difficult to identify all the rightsholders which vary across geographies and context. We will however try as much as possible to discuss which rights of these rightsholders could be hampered during the crisis protocol.

.....
² Hope, Andersen, & Morgan, “Human Rights Assessment.”

³ Hope, Andersen, & Morgan, “Human Rights Assessment.”

Scope

The scope of the work and online activities are limited to online content incidents, involving livestream/video/audio/image/text that records or depicts a recent, ongoing or imminent real-world terrorist and violent extremist attack. It is also important to note that this document is concerned with the “crises” that have an online angle and do not include stages of radicalizations or other aspects.

Categories of Attacks

Based on a combination of the Global Terrorism Database and other categorizations at Council of Foreign Relations,⁴ we have included the following aspects for categorizing terrorist attacks with an online aspect:

1. Geographical scope

Whether the attack crossed international borders or if there were citizens of different countries affected by the attack.

2. Used online service providers and online materials

What platforms were used and what content was shared online.

3. Multiple platforms

As part of the attack whether attackers or supporters exploited multiple platforms to share terrorist content online.

4. Virality

Defined as achieving a large number of views in a short time period due to sharing.⁵

Virality is maximized to the extent that content viewed by one consumer is shared with others.⁶

5. Type of attack and weapon information

Whether the terrorist attacks included the use of weapons and what type was used.

6. Target type

Whether religious organizations, business institutions, government entities were the target.

7. Terrorist group name and kind

What kind of a terrorist group it was and whether it state sponsored or not.

.....

4 Cyber Operations Tracker, Council on Foreign Relations, n.d., <https://www.cfr.org/cyber-operations/>.

5 Alhabash and McAlister see virality as a combination of user-generated activities performed on social networks. They take a behavioral approach to defining virality by focusing on viral reach (i.e., access to and sharing of content), affective evaluation (i.e., likes and dislikes), and message deliberation (i.e., comments and status updates). See Saleem Alhabash and Anna R. McAlister, “Redefining virality in less broad strokes: Predicting viral behavioral intentions from motivations and uses of Facebook and Twitter,” *New Media & Society* 17, no. 8 (2015): 1317–1339.

6 Gerard Tellis et al., “What drives virality (sharing) of online digital content? The critical role of information, emotion, and brand prominence,” *Journal of Marketing* 83, no. 4 (2019): 1–20.

8. Number of perpetrators

How many perpetrators and accomplices undertook the attack.

9. Number of casualties

The number of people who were injured or killed.

10. Claims of responsibility

Whether a group claimed responsibility for the attack.

11. Timing

If the attack happened in the past, is ongoing or imminent.

12. Threats

Terrorist threats that did not materialize or were prevented/not undertaken.

13. Intention for mass violence

Whether the terrorist has a clear intention to undertake mass violence.

14. Shared by (perpetrator, accomplice, sympathizer, bystander)

Who shared the materials and how were they shared.

15. Used crisis protocols

Which crisis protocol was activated or is about to be activated.

16. Prior conviction

Whether the perpetrator(s) had a prior conviction or arrest on related issues.

Categories	Halle	Glendale	Conflans	London Bridge	Vienna	Washington DC	Streatham	Reading	Christchurch
Geographical scope	Global	Global	Global	Local	Local	Local	Local	Local	Global
Used Online Service providers	Livestream on Twitch, Manifesto on Meguca	Live streamed, Snapchat	Twitter, footage	Videos and Pictures	Bystander videos and subsequent attacker manifesto release after the incident (video)	Parler, Twitter, Facebook, GAB	Bystander video of the police response	Bystander video of the aftermath shared	Initially, 8Chan with links to livestream on Facebook, and to manifesto on Mega, Solidfiles, Zippyshare, Mediafire
Multiple platforms	Yes	Yes	Yes	Unknown	No (manifesto was shared more widely)	Yes	Unknown	Yes (Instagram and Twitter)	Yes
Virality	5 livestream views; 2200 recorded views	No	Image posted on Twitter, liked by some	Unknown	Unknown	Yes	No	No	Yes
Type of attack	Armed Assault	Armed Assault	Armed Assault	Armed Assault	Armed Assault	Armed and Unarmed Assaults	Armed Assault	Armed Assault	Armed Assault
Weapon information	Handmade gun	Gun	30cm knife	Knife	Gun	Use of various weapons	Knife	Knife	Gun
Target type	Religious institution, Business	Business	Civilian, Educational institution	Civilians	Civilians	Government officials and buildings	Civilians	Civilians	Religious institution (mosques) and Muslim Civilians
Terrorist group name or kind	Anti-Semitic extremist	Incel	Radicalized individual (Jihadi inspired)	Jihadi Inspired Extremism	Alleged IS Supported attack	Anti Government/ Authority	Jihadi Inspired terrorism	ASL (AQ aligned group based in Libya)	White identity motivated violent extremism
Number of perpetrators	1	1	1	1	1	725 arrests	1	1	1
Number of casualties	1 killed	3 injured	1 killed	3 killed (including perpetrator)	5 killed, 23 injured	7 killed, many injured	3 injured	3 killed, 3 injured	51 killed, many injured
Claims of responsibility	N/A	N/A	No (however the perpetrator has featured in ISIL propaganda, was in contact with ISIL and his brother was a member of ISIL)	No	Yes (Amaq)	No (some individuals have accepted responsibility during their individual trials or plea agreements)	No (attacker had previously been convicted of offenses relating to disseminating AQ material)	As well as being a member of ASL, the attacker had ISIL material on his device	N/A
Timing	Past	Past	Past	Past	Past	Past	Past	Past	Past
Threats	No	No	No	No	No	No	No	No	No
Intention for mass violence	Yes (though did not fully materialize)	Yes	No	Yes	Yes	Unknown	Yes	Yes	Yes
Shared by	Perpetrator	Perpetrator	Perpetrator	Bystanders	Bystanders	Perpetrators, Accomplices, Sympathizers, Bystanders	Bystanders	Bystanders	Perpetrator
State responsibility	No	No	No	No	No	No	No	No	No
Used crisis protocols	GIFCT (CIP)	GIFCT (CIP)	EU	UK	New Zealand (not fully activated but the monitoring stage triggered)	None	UK	UK	No (was prior to (and reason for) development of all except UK protocols
Prior conviction	No	No	Unrelated charges	Yes	Yes	Yes for some perpetrators	Yes	Yes	No

Case Studies

We will briefly discuss the human rights implications of the following attacks at each stage since they resulted in monitoring the attack or activation of various Crisis Response Protocols:

- Halle, Germany, October 2019
- Christchurch, New Zealand, March 2019
- Glendale, AZ, USA, May 2020
- Conflans, France, October 2020
- Washington, D.C., USA, January 2021

As much as possible, the cases are studied by following the Crisis Protocol stages. However in some cases, some stages have been collapsed into one either because there was not much information about activities during that stage or the activities could not be analyzed based on each stage.

Halle

This incident was an armed attack on a synagogue. The perpetrator posted a manifesto (a platform called Meguca which is loosely affiliated with 4Chan) detailing the attack.⁷ During the horizon period, there was no monitoring or surveillance. The perpetrator recorded himself from the beginning of the attack in his car, streaming on Twitch for 35 minutes, with approximately five people viewing it live and 2200 people viewing the recording of it. After somebody reported the “recorded” video, it was taken down.⁸

In its transparency report on the incident GIFCT stated the following: “On Wednesday, October 9, 2019, the GIFCT activated its new Content Incident Protocol (CIP) for the first time after the protocol’s development following the terrorist attack in Christchurch, New Zealand the previous March. The CIP was declared following the tragic shooting in Halle, Germany and the perpetrator’s attack video circulating on multiple digital platforms.”⁹

Stages 1-4: Horizon, Identify and validate, Incident detection, and Information gathering and validation:

1. **Life, liberty, and security of person** – During the horizon stage, the act of live streaming had the potential to incite more violence. It was, however, not viral content. The rightsholders were actual and potential victims of terrorism and violent extremism as the video streaming could incite more violence. We are not aware of any other action that had an impact on other human rights and rights holders at this stage.
2. **Nondiscrimination and equality before the law** – No known violations.

.....
⁷ Daniel Koehler, “The Halle, Germany, Synagogue Attack and Evolution of the Far-Right Terror Threat,” CTC Sentinel 12, no. 11 (2019), <https://ctc.westpoint.edu/wp-content/uploads/2020/02/CTC-SENTINEL-112019.pdf>.

⁸ See Twitch’s Twitter thread on the 2019 Halle incident: <https://twitter.com/Twitch/status/1182036266344271873>.

⁹ Update to GIFCT Statement on Halle Shooting, GIFCT, October 17, 2019, <https://gifct.org/2019/10/17/update-to-gifct-statement-on-halle-statement/>.

3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 5: Assess

1. **Life, liberty, and security of person** – No known violations.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 6: Activate and notify

During this stage a Twitch statement was released, but it is not clear what level of action GIFCT members were told should be taken.

1. **Life, liberty, and security of person** – At this stage, the live streaming and the video could have a high impact on life, liberty, and security of a person, had the content gone viral. But since it did not, the impact on this human right is unknown.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – Unlikely to have been impacted at this stage; however, if the content was not preserved as a result of protocol operator guidance, it could affect access to effective remedy.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 7: Prepare and Act

1. **Life, liberty, and security of person** – This stage had a high impact on life, liberty, and security of person; despite the fact that the content was found at a very late stage, the actions by the protocol operators potentially stopped it from going viral.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – This stage potentially had a high impact on access to effective remedy as it relates to preserving evidence.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations; at this stage the hash database might not have a high impact on freedom of opinion, thought, conscience, and religion, but at a later stage, if hashes are inaccurate it could have an impact on human

rights in the future.

5. **Privacy** – No known violations.; however, gathering OSINT materials can lead to profiling.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 8: Conclude

There might be limited human rights implications during this stage; however, the decisions that are taken based on the lessons learned from the attack (like expanding the hash database) could have future human rights implications. For this report, we are not aware of cases of human rights impact at this stage.

Glendale (The Westgate Shooting)

An involuntary celibate (incel) sympathizer shot couples at a mall. There was an online component to this, as the GIFCT transparency report mentions: “On Wednesday, May 20, 2020, the GIFCT activated its Content Incident Protocol following the shooting in Glendale, AZ, adding hashes of visually distinct videos depicting the attacker’s content during the shooting.”

In Snapchat videos released by police, the perpetrator said he was going to be the shooter, along with another clip showing his gun where he says, “Let’s get this done, guys.” In this case, the perpetrator did not have any criminal background. The protocol was not activated during the incident and it seems to be an after the fact reaction to the incident.¹⁰

Stage 1: Horizon

The perpetrator streamed the video on Snapchat shortly before the incident. There was no monitoring and there was no reporting. It is not publicly known if the brother reported him or the content to the police.

Because the video was found after the incident, there were no known violations. of human rights implications. There might have been some greater human rights implications during the horizon that could potentially incite others, such as members of Incel groups or the actor’s followers.

1. **Life, liberty, and security of person** – Nobody died because of streaming, but it had the potential to incite further violence.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

.....
¹⁰ “CIP declared following Glendale, AZ shooting,” GIFCT, May 21, 2020, <https://gifct.org/2020/05/21/cip-declared-following-glendale-az-shooting/>.

Stage 7: Prepare and Act

Since hash sharing occurs at this stage, it could have had some human rights implications on future events. In this case, the information sharing led to the expansion of hash databases that could have potential implications for human rights.

1. **Life, liberty, and security of person** – The ongoing information sharing and sharing hashes might have prevented the content from going viral.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 8: Conclude

Depending on what kind of information GIFCT and others shared with each other, this stage could have different human rights implications. There are no known violations. of impact on human rights.

Samuel Paty, France, Conflans

Samuel Paty was a teacher at a high school in Conflans. He allegedly showed cartoons of the prophet Muhammad to students. A parent of a student filed a criminal complaint with police. On Youtube and Facebook the parents claimed that Paty displayed an image of Muhammad, named Paty in the video and gave the school address. An Imam posted a video on a social media platform and called Paty a thug. In October 2020, the perpetrator saw the video made by the imam and decided to punish Paty. Minutes after the attack, the perpetrator posted a picture of Paty's severed head on Twitter. The picture was seen by many of Paty's students. The EU Crisis Protocol was activated.

Stages 1-4: Horizon, Identify and validate, Incident detection, and Information gathering and validation

Before the attack, in the horizon phase, it is unclear whether there was monitoring and surveillance by those in charge of CIP. This stage has high human rights implications, the right to privacy, assembly but also security, liberty, and freedom are just a few that can be hampered.

1. **Life, liberty, and security of person** – Monitoring and surveillance (if targeted and proportional) might have helped protect Paty's right to life, liberty, and security.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – If monitoring took place it could lead to arrest or also hampering assembly rights (the right for Muslims to organize a protest online against the teachers or express their beliefs through online content).
5. **Privacy** – At these preactivation stages, the identification and validation must have been easier and more straightforward since the action was materialized and the picture was

posted. Because of these factors, there might have been a low level of human rights implications.

6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 7: Prepare and Act

It does not look like that the image was posted across different platforms, but removal of content at this stage (instead of making it private) might make future investigations harder. The rapid deletion by the platforms of the images of the attack have indeed hindered police investigations by depriving them of visual information on the terrorist and the place to which he headed after the attack for example. This important information could not be provided to the police. This could have hindered human rights by allowing the terrorist to carry out further attacks before his arrest. It is therefore important to take this into account when assessing the human rights impacts of crisis protocols. A suppression in the public sphere but the preservation of the files by the platforms would be relevant in this sense.

This incident might have led to the creation of new hashes. Using OSINT by the CIP could lead to finding others in the friends circle which could hamper privacy, freedom of opinion and thought. It is unclear if the OSINT that were used during the crisis led to the arrest of others, but it is a human rights implication that should be considered.

1. **Life, liberty, and security of person** – Activation happened after Paty was murdered; no other threat to life, liberty, and security as a result of activation could be predicted in this case. Paty's picture was posted by the terrorist on Twitter and was seen by students before it could be taken down. While this is not the direct result of late activation of protocol, potentially Paty's students' right to security could be hampered.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – Removal of materials made it difficult to investigate the attack and provide effective remedy.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – Using OSINT by CIP operators could lead to finding others in the friends circle which can hamper privacy, freedom of opinion and thought. In fact a person who liked the terrorist tweet was arrested.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – It does not seem that anybody was arrested as a direct result of activation of the protocol. There were some arrests made by the French police.

Stage 8: Conclude

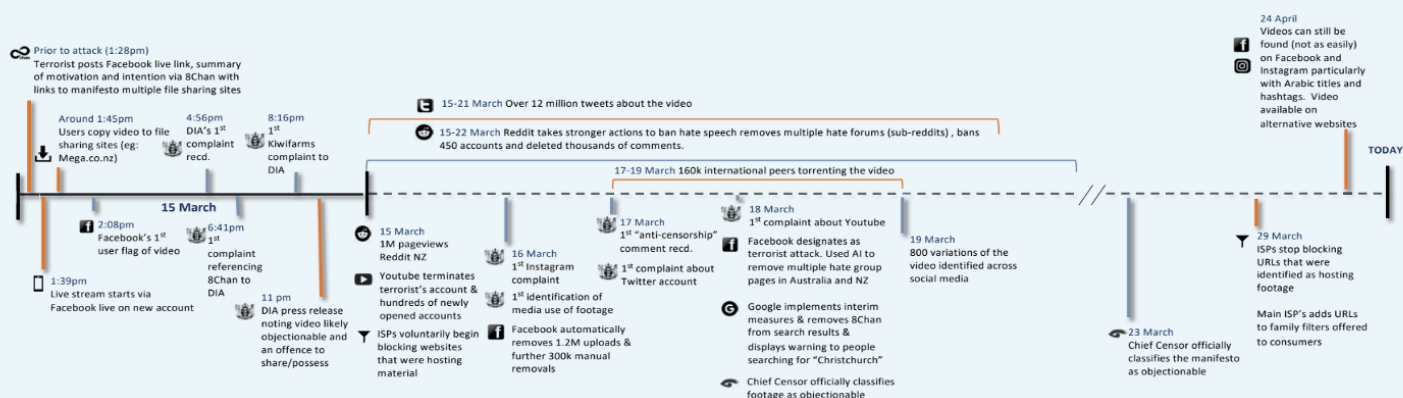
The conclude phase did not happen at GIFCT because the protocol was not activated, but GIFCT could have benefited from learning from this experience and debriefing the stakeholders which could contribute to life, liberty, security as well as privacy. Since monitoring continues, despite the lower human rights implications, there might be more human rights implications in the future. A year after the attack, a blogger talked to the father of the perpetrator who endorsed the acts of his son. Somebody who liked the decapitated image of Paty on Twitter was also arrested.

Following the attack on Samuel Paty, the offense of endangering the life of others by providing personal data was created by law no. 2021-1109 of August 24, 2021, reinforcing the respect of the principles of the Republic, article 36. A penalty of 3 years imprisonment and 45,000 euros fine was created (5 years and 75,000 euros if the victim is a minor or a representative of the public authority, a person in charge of a public service mission, or has an elective mandate). It is now illegal to disclose someone's name and home or work address while calling for online hate or violence against them. This provision aims at monitoring and condemning this type of publication while trying to preserve freedom of speech online. This is not a protocol but a measure that can help avoid dramatic situations such as the one in Conflans.

Christchurch Attack (hypothetical analysis)

No multi-party protocols existed at the time of the Christchurch terrorist attack (other than Facebook's own three step crisis protocol), so what follows here is a hypothetical analysis. In an extensive violent extremism transparency report, New Zealand Department of Internal Affairs (DIA), provided details and a timeline about the attack and its online angle. The chart below is taken from the transparency report that the DIA published in April 2022.¹¹

Timeline of Spread and response



Stages 1-4: Horizon, Identify and validate, Incident detection, and Information gathering and validation

The perpetrator posted an anonymous message to an online discussion board called 8chan and revealed his intentions to undertake an attack and livestream it. There was a link to his Facebook page that was repeatedly shared. He also sent messages and emails to family and the New Zealand Prime Minister's office. He started live streaming as he went towards Masjid an-Nur.

¹¹ New Zealand Department of Internal Affairs, "2021 Digital Violent Extremism Transparency Report," April, 2022, [https://www.dia.govt.nz/diawebsite.nsf/Files/Countering-violent-extremism-online/\\$file/DVE-Transparency-Report-2021-a.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/Countering-violent-extremism-online/$file/DVE-Transparency-Report-2021-a.pdf).

1. **Life, liberty, and security of person** – This stage clearly had an impact on life, security and liberty of the Muslims who were murdered; the live streaming at this stage could lead to other incidents as well.
2. **Nondiscrimination and equality before the law** – Disproportionate focus on Islamic Extremism resulted in discrimination against Muslims.
3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 5: Assess

1. **Life, liberty, and security of person** – This was a clear cut terrorist act, and the assessment at this stage would have had high impact on life, liberty, and security of person, since it had the potential to go viral (and it did), and had a clear terrorist violent intention.
2. **Nondiscrimination and equality before the law** – Biases observed in the development and implementation of counter terrorist policy must be guarded against, and assessments and decisions made must be able to show that biases were considered and addressed.
3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – Some users who shared the video in good faith to spread awareness about the incident felt that assessing their post as spreading extremist content was against their freedom of expression; freedom of religion could be impacted if assessment of materials have a lower threshold (as it instills fear in people).
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 6: Activate and notify

1. **Life, liberty, and security of person** – As the perpetrator made his way to another Islamic Center, activation of protocol and informing civil society groups about it might have helped by warning the Muslim community about the online material and the incident, protecting security, life and liberty at this stage.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – No known violations.
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 7: Prepare and Act

1. **Life, liberty, and security of person** – In the future, sharing hashes at this stage might reduce the virality and cross platform movement of the terrorist content.
2. **Nondiscrimination and equality before the law** – No known violations.

3. **Access to effective remedy** – No known violations., but if there were mistakes in taking down the content without preserving it, it could hamper access to effective remedy (since the terrorist content went viral and shared on multiple platforms, hypothetically not all the content could be taken down and some could be preserved).
4. **Freedom of opinion, thought, conscience, and religion** – No known violations.
5. **Privacy** – No known violations.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – No known violations.

Stage 8: Conclude

The online angle of Christchurch terrorist attack led Prime Minister of New Zealand and President of France to launch the Christchurch Call to Act in May 2019. The Call led to strengthening and expansion of the GIFCT and multi-stakeholder efforts to develop and implement protocols (including the Christchurch Call Crisis Response Protocol, the GIFCT Content Incident Protocol and Incident Response Framework, and the EU Crisis Protocol), enabling a rapid, coordinated, and effective response to the dissemination of terrorist or violent extremist content following a real-world attack.

Some tech companies after the attack took measures such as removing 8Chan from search results or displaying warnings about the Christchurch attack. Tech companies also made safety improvements to livestream services.¹²

U.S. Capitol Attack

Stage 1: Horizon

A large crowd gathered outside the U.S. Capitol during a Joint Session of Congress which began at approximately 1:00 PM Eastern Time (ET). The FBI had a command post operation based out of Headquarters in Washington, D.C. in support of preventing violence and criminal activity in the National Capital region. Law enforcement agencies could see social media posts about the event, and mainstream news coverage on the major networks and local channels.

1. **Life, liberty, and security of person** – People had the choice to gather outside the U.S. Capitol during the Joint Session of Congress. U.S. Capitol Police (USCP) were present as it is their responsibility to keep members of Congress and Senators safe, as well as the public visiting U.S. Capitol grounds. In addition, USCP is responsible for protection of government property. While law enforcement agencies used tools to monitor social media platforms right before the incident, no action was taken with regards to content moderation in coordination with law enforcement agencies. At this stage, life, liberty, and security of persons such as the government representatives and the public could have been endangered.
2. **Nondiscrimination and equality before the law** – Any person of any race, creed, gender, etc., could gather outside the U.S. Capitol and each person is promised to be treated equally by Capitol Police regardless of race, creed, gender, etc. On social media, as they

.....
¹² Ben Collins, "Facebook to restrict livestream feature after Christchurch attack," NBCNews, May 14, 2019, <https://www.nbcnews.com/tech/tech-news/facebook-restrict-livestream-feature-after-christchurch-attack-n1005741>.

are private entities, the obligation of equal treatment does not legally exist; however, some tech-corporations have their own human rights policies. There are no known violations of discrimination based on creed, gender etc. that happened during this stage.

3. **Access to effective remedy** – N/A at this stage of the event.
4. **Freedom of opinion, thought, conscience, and religion** – There are conflicting reports that some law enforcement agencies monitored online activities. This could potentially have had an effect on freedom of opinion, thought, conscience, and religion. However, there are reports that the law enforcement missed the threats on social media platforms and was not prepared and therefore all were free to express those opinions through social media.¹³
5. **Privacy** – People had the choice whether to gather outside the U.S. Capitol during the Joint Session of Congress on public grounds, and whether to publicly post videos or images of themselves inside the Capitol. If law enforcement undertook monitoring of the online activities, despite them being public, it could affect privacy of people in the later stages of the protocol.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – N/A at this stage of the event.

Stage 2: Identify and Validate

At approximately 2:00 PM EST, individuals in the crowd forced their way through the barricades and the crowd advanced to the U.S. Capitol while the Joint Session was still underway. Law enforcement agencies evaluated public social media posts for threats or indications of violent activity or violations of federal criminal law.

1. **Life, liberty, and security of person** – U.S. Capitol Police were unable to fulfill their responsibility to keep members of Congress and Senators safe, as well as the public visiting U.S. Capitol grounds. This right was affected by the number of officers, their communications with one another, the number and quality of barricades, and the number of people gathered.
2. **Nondiscrimination and equality before the law** – Any person of any race, creed, gender, etc., could force his/her way through the barricades and advance with the crowd at this stage of the event. Law enforcement agencies' evaluation of public social media posts did not consider the poster's race, creed, gender, etc., and each post was evaluated as a stand-alone post, and in the context of the user's other posts.
3. **Access to effective remedy** – N/A at this stage of the event if rights were not harmed.
4. **Freedom of opinion, thought, conscience, and religion** – Even as people forced their way through the barricades and advanced with the crowd, the people choose to speak or not speak. All were free to express those opinions on the grounds of the U.S. Capitol. Opposite viewpoints, however, expressed within earshot of each other, could have implications, if that expression led to a physical altercation. All were free to express those opinions through social media.
5. **Privacy** – Once people crossed into the restricted space of the U.S. Capitol, they had a diminished expectation of privacy. The U.S. Capitol is a restricted building, and the Joint Session was closed to the public.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of**

.....
 13 Sam Levin, "US Capitol attack: is the government's expanded online surveillance effective?," January 7, 2022, <https://www.theguardian.com/us-news/2022/jan/07/us-capitol-attack-government-online-surveillance>.

innocence before being proven guilty – N/A to the online angle at this stage.

Stage 3: Incident Detection

At approximately 2:20 PM EST, the order was given for evacuation of the chambers by members of Congress and the Senate and the session was suspended until approximately 8:00 PM EST. The incident was detected by several law enforcement agencies through social media exploitation.

Life, liberty, and security of person – The USCP, members of Congress and Senators, and the trespassing public all still retained these rights, however it was difficult for USCP to keep everyone safe in the ensuing mayhem. There were difficulties in identifying violent extremist content which could potentially impact life, liberty, and security of a person and distinguish it from other opinions.

1. **Nondiscrimination and equality before the law** – This would have been difficult for USCP to discern during the chaos. It would also be difficult for law enforcement if they intended to work with tech-platforms to moderate content on social media platforms as well.
2. **Access to effective remedy** – Rights might not have been harmed just yet, as the incident is being detected and recognized as an incident.
3. **Freedom of opinion, thought, conscience, and religion** – The detection stage could create a lot of problems for freedom of opinion, thought, and conscience as the content being shared on social media platforms was not clear-cut terrorist content material; detecting and isolating terrorist content was very difficult.
4. **Privacy** – Once people crossed into the restricted space of the U.S. Capitol, they had a diminished expectation of privacy. The U.S. Capitol is a restricted building, and the Joint Session was closed to the public. Areas inside the U.S. Capitol might have restrictions posted prohibiting photography and audio or video recording. Violators of that posted policy who were observed by the police could expose themselves to confiscation of their devices.
5. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – N/A to the online angle at this stage.

Stage 5: Assess

This incident appeared and has been shown for some people (not all) to have a domestic violent extremist motivation. Abundant online content was produced and posted and streamed by perpetrators and bystanders alike.

1. **Life, liberty, and security of person** – Once members of Congress and Senators were safe, USCP would have turned to the public inside the chamber and worked to clear spaces one room/hallway at a time. USCP officers would have initially begun with verbal commands, and if people did not comply, they may have been detained or arrested. Some would have likely complied or tried to comply and retreat outside the U.S. Capitol grounds.
2. **Nondiscrimination and equality before the law** – This would still have been difficult for USCP to discern during the assessment phase of the incident, likely from after the recognition of an incident (after 2:20 PM) up until the session was reconvened about 8 PM. Who had a right to be inside and who did not? Who should be evacuated to safety, and how could officers tell the difference? Would they use visual cues such as clothing and dress, weapons in hand, etc., to determine who was trespassing? Could they determine who was trying to escape? This also applies to social media platforms and the same challenges could have been faced when

working with that sort of content.

3. **Access to effective remedy** – Once a cell phone or other device has been confiscated, either incident to arrest, or for photographing in a prohibited area, it would require paperwork to recover that device. This process might seem arduous from a human rights perspective.
4. **Freedom of opinion, thought, conscience, and religion** – Because of the problems with discerning protest content and violent extremist content, at this stage freedom of opinion, thought, and conscience could have been impacted.
5. **Privacy** – Once people crossed into the restricted space of the U.S. Capitol, they and the content they posted publicly on social media platforms had a diminished expectation of privacy. The U.S. Capitol is a restricted building, and the Joint Session was closed to the public.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – If arrested, a person's cell phone or other technology device would likely be confiscated and inventoried. A search warrant would have to be obtained for police to search the device, unless exigent circumstances warranted otherwise. Wrongful assessment of the online materials as violent extremism and terrorism could lead to arbitrary arrest.

Stage 6: Activate and Notify

A report of shots fired on the floor of the U.S. Capitol was sent out across government agencies at approximately 3:00 PM EST. The Mayor of Washington, D.C. imposed a 6:00 PM EST curfew for the city. Since no protocol was activated, we can only speculate what could happen.

1. **Life, liberty, and security of person** – At this stage, life, liberty, and security of person could be impacted if violent, extremist content was being shared consistently; however, since a curfew was in place it might have had lower impact.
2. **Nondiscrimination and equality before the law** – No known violations.
3. **Access to effective remedy** – Since this was the notification stage, access to effective remedy was unlikely to be highly impacted.
4. **Freedom of opinion, thought, conscience, and religion** – During activation stage, increased monitoring can take place which affects freedom of opinion and thought.
5. **Privacy** – Might not be impacted.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – might not be impacted.

Stage 7: Prepare and Act

The Washington, D.C. National Guard was activated at approximately 4:00 PM EST. Bomb technicians were deployed for the device near the DNC. The same evening, the FBI opened an investigation into the civil disorder and riot allegations associated with the events at the Capitol.

1. **Life, liberty, and security of person** – By that evening, the FBI had opened an official investigation into the events that had occurred in the U.S. Capitol. This opened up many more resources for law enforcement to locate and identify those who were inside restricted space at the U.S. Capitol. Law enforcement agencies used a variety of lawful investigative techniques during the initial 24–48 hours of investigation. Many techniques were intrusive and involved

collection of personal cell phone location information, subscriber data, and even content of communications in the restricted space.

2. **Nondiscrimination and equality before the law** – Law enforcement agencies opened individual investigations on each person who may have broken laws, including Entering and Remaining in a Restricted Building; Disorderly and Disruptive Conduct in a Restricted Building; Violent Entry and Disorderly Conduct in a Capitol Building; Parading, Demonstrating, or Picketing in a Capitol Building. Each person was treated individually before the law. Law enforcement also worked with private threat intelligence firms and activists to crowdsource pictures and footage of those who were involved in some way with the protest (use of OSINT at this stage was very extensive).
3. **Access to effective remedy** – Each person arrested and charged could choose to have his/her day in court, or agree to plead to charges levied against him/her. See “Capitol Breach Cases” posted through the United States Department of Justice, <https://www.justice.gov/usao-dc/capitol-breach-cases>. However, because of the use of OSINT and social media profiling that could increase error in identification, access to effective remedies could be highly hampered.
4. **Freedom of opinion, thought, conscience, and religion** – The public and those who agreed with the protest could be affected by take-downs of online content.
5. **Privacy** – This incident was very public. People who are formally charged are named in publicly available documents posted on the Internet. Privacy was diminished when formal charges were filed. A lot of profiling took place using OSINT when law enforcement cooperated with OSINT providers. Despite the fact that the footage and information were public, the activities that took place during this stage could hamper privacy of social media users.
6. **Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty** – Depending on which actions are taken, if guidance about the violent, and terrorist nature of the online content is inaccurate, it might lead to wrongful arrest.

Stage 8: Conclude

Lists of arrested individuals were circulated for database checks. Numerous lists were shared between government agencies and departments in the immediate aftermath of the unrest at the Capitol. Although the crisis concluded, this remains an active investigation. Not all people have been identified and located who were in the Capitol that day.

Human Rights Analysis for Each Stage of the CRP

In this section, we provide the human rights matrix for each stage of the crisis response protocol. In order to have a more accurate and useful matrix, we have listed some qualitative indicators that might be present at each stage of the protocol and impact certain human rights.

Qualitative indicators are actions or elements that impact human rights when tackling a crisis online. We have identified these indicators through attending the table top exercises arranged by GIFCT, undertaking the case studies, and through discussions with different stakeholders. Some of these

qualitative indicators loosely fit the definition that the United Nations has provided: “a human rights indicator is defined as specific information on the state or condition of an object, event, activity or outcome that can be related to human rights norms and standards; that addresses and reflects human rights principles and concerns; and that can be used to assess and monitor the promotion and implementation of human rights.”¹⁴

The qualitative Indicators are as Follows:

1. Assessment of violent extremist or terrorist content
2. Virality
3. Cross platform
4. Broadening GIFCT's scope (for example not including hate speech since it broadens scope)
5. Diversity of stakeholders' consultation
6. Monitoring
7. Use of OSINT that can lead to profiling
8. Probability of false positive
9. Verification of information (how it's being verified, who gave it etc)
10. Accuracy in identifying perpetrator-only content
11. Criteria to assess significance of online presence
12. Expansion of hash database
13. Accuracy and completeness of guidance given to the GIFCT members
14. Accuracy and completeness of information sharing (companies act based on their own policy)
15. Take down of content and other actions taken
16. Sharing hashes with a stakeholders
17. Mitigation plan with a human rights analysis for future events

Assessment of violent or extremist content

- **What is it?** Activities that GIFCT or protocol operators undertake in order to assess whether the incident involves violent extremist or terrorist content.
- **Whose rights?** Victims of terrorism, victims of counter terrorism activities, the accused, human rights defenders.
- **Which rights?** Life, liberty, and security of person, freedom of opinion, thought, conscience, and religion, freedom of assembly and association, freedom from arbitrary arrest, detention and exile.

Virality

- **What is it?** Virality is achieving a large number of views in a short time period due to sharing.
- **Whose rights?** Victims of terrorism, victims of counter terrorism efforts, vulnerable groups.
- **Which rights?** A viral terrorist content could have an impact on the right to life, liberty, and security of person and privacy.

.....
¹⁴ United Nations, Office of the High Commissioner, “Human Rights Indicators: A Guide to to Measurement and Implementation,” December 5, 2012, https://www.ohchr.org/sites/default/files/Documents/Publications/Human_rights_indicators_en.pdf.

Cross platform

- **What is it?** Cross platform terrorist content is a piece of content that has been shared across multiple platforms and not limited to just one platform. Cross platform content does not necessarily go viral, but it can have a potential impact on human rights. This is especially the case when all the platforms are members of GIFCT and as a result might take similar actions that impact content across different platforms.
- **Whose rights?** Victims of terrorism, victims of counter terrorism efforts, vulnerable groups, the accused.
- **Which rights?** Nondiscrimination, freedom of opinion, freedom of assembly and association, access to effective remedy.

Broadening GIFCT's scope

- **What is it?** Actions that a protocol operator or GIFCT take that affect the scope of the protocol and broadens it.
- **Whose rights?** Victims of counter terrorism efforts, users of platforms, vulnerable groups.
- **Which rights?** Life, liberty, and security of person, freedom of assembly and association, freedom of opinion, expression.

Diversity of stakeholders' consultation

- **What is it?** At various stages of crisis management, protocol operators talk to third parties from civil society or law enforcement. The third parties might be involved in notifying the protocol operators about a potential incident. Whether the operators talk to a diverse set of stakeholders or not can impact human rights.
- **Whose rights?** Minorities and vulnerable groups, victims of terrorism, victims of counter-terrorism efforts.
- **Which rights?** Life, liberty, security of person, access to effective remedy, freedom of opinions, right to participation.

Monitoring

- **What is it?** Monitoring data sources, searching for and analyzing information to provide situational awareness, or inform response options.
- **Whose rights?** Victims, the accused, minorities/vulnerable groups.
- **Which rights?** Life, security of person and liberty, arbitrary arrest and the right to fair trial, privacy.

Use of OSINT that can lead to profiling

- **What is it?** Open Source Intelligence techniques use the publicly available information on the Internet in order to identify a violent situation, the attacker, or pattern of attack.
- **Whose rights?** The accused, human rights defenders, minorities/vulnerable groups.
- **Which rights?** Freedom of opinion, thought, conscience, and religion, freedom from arbitrary arrest, detention, and exile, privacy.

Probability of false positive

- **What is it?** During some of the crisis protocol stages, it is more probable that content or

conduct is identified falsely as terrorist and violent extremist.

- **Whose rights?** The accused, the victims of counter terrorism activities, human rights defenders, minorities, vulnerable groups
- **Which rights?** Freedom of opinion, thought, conscience, and religion, Freedom of assembly and association.

Verification of information

- **What is it?** The protocol operator receives information from third parties about a possible terrorist, violent extremist event with an online angle. The operator has to verify that information, using specific verification tools.
- **Whose rights?** Victims of efforts to counter terrorism, human rights defenders, vulnerable/minority groups.
- **Which rights?** Freedom of opinion, thought, conscience, and religion, freedom of assembly and association, freedom from arbitrary arrest, detention, and exile, right to privacy.

Accuracy in identifying perpetrator-only content

- **What is it?** The protocol operator has to identify perpetrator-only content because the implications for bystanders who are platform users could be grave. For example it could lead to blocking their accounts for some time.
- **Whose rights?** Victims of efforts to counter terrorism, the accused, users of platforms and bystanders, human rights defenders.
- **Which rights?** Freedom of opinion, thought, conscience, and religion, Freedom of assembly and association.

Criteria to assess significance of online presence

- **What is it?** The criteria that the protocol operator uses to assess the significance of online presence. This could also be a part of assessing threshold.
- **Whose rights?** Victims of terrorism, victims of efforts to counter terrorism.
- **Which rights?** Right to life, security of person and liberty.

Expansion of hash database

- **What is it?** A database of distinct hashed images of terrorist and violent extremist content. The hash database could potentially lead to removal of content that is not terrorist and violent. Moreover, because the companies share the hashes with each other, if there is a mistake, it happens across platforms.
- **Whose rights?** Victims of terrorism, victims of counter terrorism efforts, human rights defenders, vulnerable communities.
- **Which rights?** Access to effective remedy, freedom of opinion, thought, conscience, and religion, freedom of assembly and association.

Accuracy and completeness of guidance given to the GIFCT members

- **What is it?** The protocol operator (in this case GIFCT) might give guidance to member companies about what sort of action should be taken.
- **Whose rights?** Victims, the accused, victims of efforts to counter terrorism, minorities and

vulnerable groups, human rights defenders.

- **Which rights?** Life, liberty, and security of person, nondiscrimination and equality before the law, access to effective remedy, freedom of opinion, thought, conscience, and religion, freedom of assembly and association, privacy, freedom from arbitrary arrest, detention, and exile, right to a fair trial, assumption of innocence before being proven guilty.

Accuracy and completeness of information sharing

- **What is it?** The protocol operator shares information with member companies about the incident, especially the pattern and its characteristics on the Internet.
- **Whose rights?** Victims, the accused, victims of efforts to counter terrorism, minorities and vulnerable groups, human rights defenders.
- **Which rights?** Life, liberty, and security of person, nondiscrimination and equality before the law, access to effective remedy, freedom of opinion, thought, conscience, and religion, freedom of assembly and association, privacy, freedom from arbitrary arrest, detention, and exile, right to a fair trial, assumption of innocence before being proven guilty.

Take down of content and other actions taken

- **What is it?** The operator can recommend take-down or other actions such as de-amplification. Companies might have their own internal mechanisms to mitigate harm, however smaller tech-corporations might not have the resources and act based on the operator's recommendation, so it has potential implications for human rights.
- **Whose rights?** Victims, the accused, victims of efforts to counter terrorism, minorities and vulnerable groups, human rights defenders
- **Which rights?** Life, liberty, and security of person, nondiscrimination and equality before the law, access to effective remedy, freedom of opinion, thought, conscience, and religion, freedom of assembly and association, privacy, freedom from arbitrary arrest, detention, and exile, right to a fair trial, assumption of innocence before being proven guilty, right to participation.

Sharing hashes with a stakeholder

- **What is it?** Sharing hashes with a stakeholder (for example GIFCT sharing hashes with law enforcement) does not happen, but if in the future this becomes a practice it will have human rights implications.
- **Whose rights?** Victims, the accused, victims of efforts to counter terrorism, minorities and vulnerable groups, human rights defenders.
- **Which rights?** Life, liberty, and security of person, nondiscrimination and equality before the law, access to effective remedy, freedom of opinion, thought, conscience, and religion, freedom of assembly and association, privacy, freedom from arbitrary arrest, detention, and exile, right to a fair trial, assumption of innocence before being proven guilty.

Mitigation plan with a human rights analysis for future events'

- **What is it?** Mitigation plan that considers a human rights analysis for future events learns from the past human rights violations during a just concluded crisis and tries not to make the same mistakes in future crises.
- **Whose rights?** Victims of terrorism and violent extremism, Victims of efforts to counter terrorism

and violent extremism, Human rights defenders, minorities and vulnerable groups and the accused

- **Which rights?** Life, liberty, and security of person, Nondiscrimination and equality before the law, Access to effective remedy, Freedom of opinion, thought, conscience, and religion, Freedom of assembly and association, Privacy, Freedom from arbitrary arrest, detention, and exile; right to a fair trial; assumption of innocence before being proven guilty

1. Horizon: when the attack is about to happen

During the Horizon stage, when (for example) the terrorist streams right before undertaking the attack, tech-corporations and GIFCT might undertake situational awareness, which includes monitoring various platforms.

Whose rights and which rights?

Monitoring and surveillance have human rights impact on victims of terrorism and violent extremism (threat to life, security and liberty) and the streaming might incite more violence at that moment. During horizon, the virality of the content and if multiple platforms are used to stream and disseminate the information are two indicators that can affect human rights of the victims of terrorism and the victims of counterterrorist activities. If the protocol operators at this stage undertake research that is not within their mandate or do not consult with a diverse set of stakeholder groups, it might lead to broadening the scope of the protocol. Broadening the scope of the protocol can impact the rights of human rights defenders and victims of terrorist and violent extremist acts while the victims of counter terrorist and violent extremist activities might be violated.

Qualitative indicators:

- Monitoring
- Virality
- Cross platforms
- Broadening GIFCT's scope
- Diversity of stakeholders consultation

2. Identify and validate and Incident detection (through internal monitoring, or a tip received from a partner organization, or media reporting). Information gathering and validation/part of pre-activation (seeking information to understand what has happened or is happening and ensure that understanding is valid, i.e. corresponds to reality).

This step is when a tip is received by third parties and they identify and validate whether there is livestreaming/violent content. Monitoring the incident takes place at this stage.

Whose rights and which rights?

Victims of terrorism and violent extremism's right to life, liberty, and security of person might be hampered if the attack is not validated correctly. The rights to freedom of opinion, freedom of assembly and association, privacy and freedom from arbitrary arrest and detention of victims of efforts to counter terrorism and violent extremism might be violated if there is a false positive. Verification of information received from the third party, where the third party verification comes

from, is it a trusted source and the methods used to verify the trustworthiness of the source are all indicators of human rights impact at this stage. These indicators can increase the likeliness of inaccurate validation and violate the rights of victims of terrorist activities, victims of counterterrorism activities, the accused and others.

Use of OSINT might affect the rights of the accused and minorities in case of profiling. Profiling can have human rights impacts such as unfair arrest and the right to fair trial.

Qualitative indicators:

- Monitoring
- Use of OSINT
- Probability of false positive
- Verification of information (how it's being verified, who gave the information etc)

3. Assess

At this stage efforts are made to determine whether the attempt is mass violence, has a significant online presence and is it by the terrorist or accomplice or by a bystander.

Whose rights and which rights?

Victims of terrorism and violent extremism right to life, liberty, and security of person might be violated if assessment of mass violence and significance of online presence is not accurate. Victims of efforts to counter terrorism and human rights defenders right to freedom opinion, assembly and association as well as privacy might be violated if mass violence is detected incorrectly.

Victims of efforts to counter terrorism right and the accused might be violated if bystander materials are identified as perpetrator's materials (because it might be taken down, which will remove evidence). The users of a platform right to assembly and opinion might be violated if bystander content is flagged (because it can lead to suspension and blocking of their account). Victims of terrorism and violent extremism right to life and liberty might be threatened by the bystander material.

Qualitative indicators

- Accuracy in identifying perpetrator-only content
- Criteria to assess significance of online presence
- Assessment of violent or extremist content
- Probability of false positive

4. Activate and notify

This stage is critical as the protocol operator activates the protocol, (and if the operator is GIFCT) informs the members (tech-corporations) about the incident and informs them of the level of action needed.

Whose rights and which rights?

During the activation stage, the protocol operators will reach out to their members and other stakeholders with information about the attack. As the activate and notify stage provides guidance

to various members about the level of action that is needed, it has a potential high impact on human rights.

The accuracy of information they have received, the use of OSINT and accuracy of the assessment will have an impact on human rights. Victims of terrorist activities' right to life, liberty, and security of person might be violated in case of wrong assessment of the event and lack of action. For example, if live streaming is not interrupted, it might potentially impact the right to life and liberty. If a wrong assessment was made and the material was not violent extremist, it could lead to broadening the scope of the protocol. This could have an impact on human rights defenders that might have their content taken down or users that might have their accounts blocked (right to opinion and freedom of expression).

Qualitative Indicators:

- Accuracy in identifying perpetrator-only content
- Criteria to assess significance of online presence
- Assessment of violent or extremist content
- Probability of false positive

5. Prepare and Act (information sharing stage):

In prepare and act stage the protocol operators look at Open Source Intelligence materials, share hashes with their members (usually tech corporations), share awareness about where the violent extremist and terrorist content is, share the outcome of assessment, and engage in ongoing strategic communications.

Whose rights and which rights?

Victims of terrorism and violent extremism right to life, liberty, and security of person and right to effective remedy might be violated in case of transmitting wrong information that could lead to the deterioration of the situation. For example, if content is taken down, the terrorists might become more violent and kill more people. Or at this stage if content is taken down without preservation then the right to effective remedy might be violated.

Victims of efforts to counter terrorism and violent extremism right to freedom of opinion, thought, conscience, and religion, as well as freedom of assembly and association, might be violated due to take-down, deamplification and suspension of accounts. The right to privacy might also be affected due to use of OSINT (since it can lead to profiling) and hash-sharing. Human rights defenders' right to freedom of assembly and association as well as freedom of opinion might also be violated if actions such as hash-sharing lead to take-down and deamplification.

Qualitative Indicators:

- Expansion of hash database
- Accuracy and completeness of information sharing
- Take down of content
- Actions taken other than content take-down
- Sharing hashes with third parties

Conclude

Assessment against threshold, monitoring goes down, and producing summaries of what's gone on.

Whose rights and which rights?

The kinds of actions that are taken during this phase can have future human rights implications of operating a crisis protocol. In conclude the operators should pay special attention to how their actions impacted human rights at each stage of the crisis protocol and come up with a mitigation plan for future incidents.

Qualitative indicators may include:

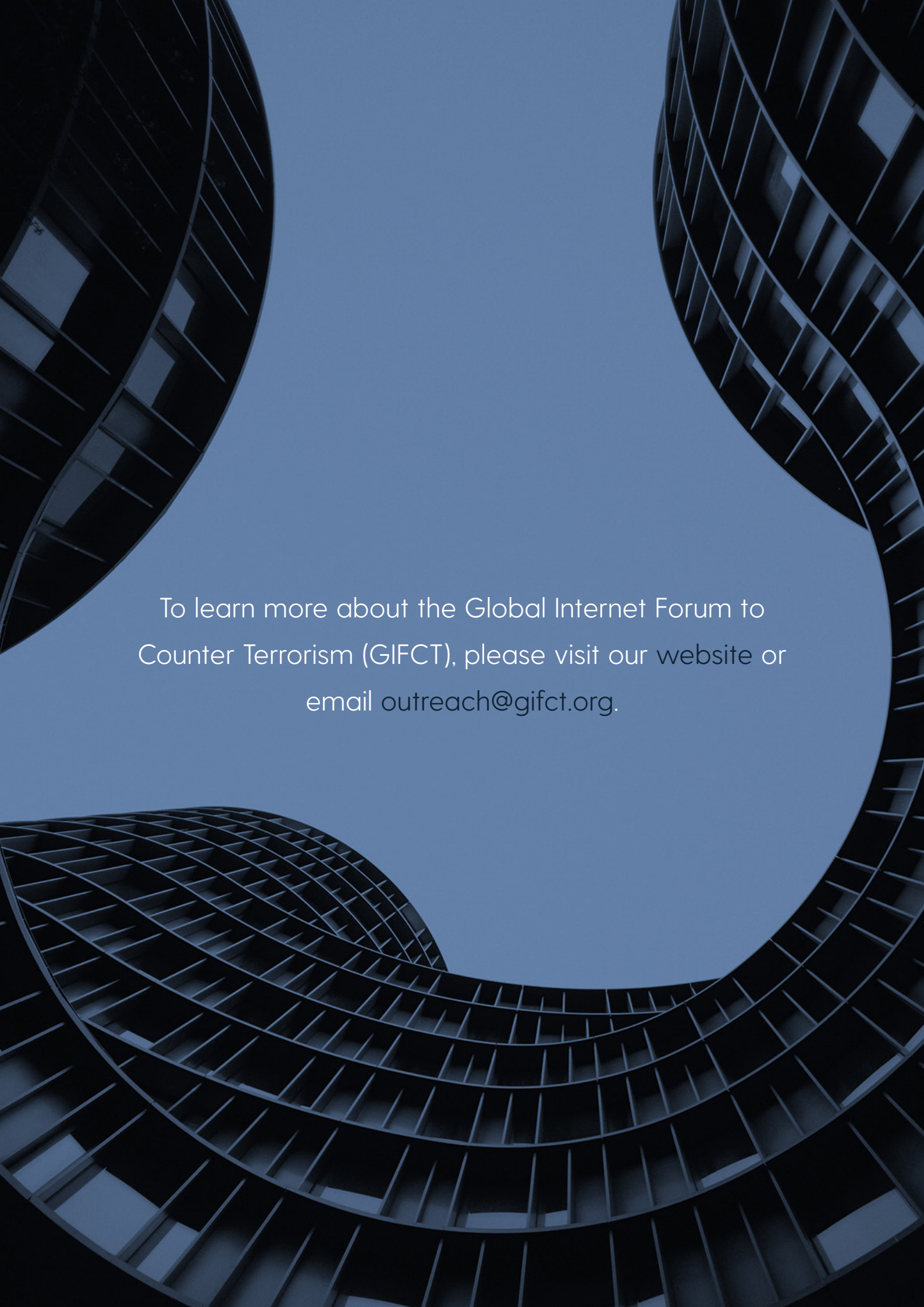
- Diversity of stakeholder consultation
- Mitigation plan with a human rights analysis for future events

Human Rights Matrix

This human rights matrix maps out and evaluates the impact of the crisis protocol at each stage on human rights. This method needs to be polished and improved upon but it can potentially illustrate how and why each stage can impact human rights.

Stages of crisis and protocol	Whose and which rights?	Which rights?	Qualitative indicators
Horizon	During the Horizon stage, when the terrorist start the streaming right before undertaking the attack, tech-corporations and GIFCT might undertake situational awareness which includes monitoring various platforms. Monitoring and surveillance has human rights impact for victims of terrorism and violent extremism (threat to life, security of person and liberty) because the streaming might incite more violence at that moment. The victims of efforts to counter terrorism might also have their right to privacy and freedom of opinion violated at the horizon stage, in case there is a false positive. Vulnerable groups (women, girls, men, families) could have their right to liberty, and security of person violated. Human rights defenders: human rights defenders could be violated if they are reporting on police brutality or other events which could potentially be falsely flagged as terrorist content or violent extremist content Accused rights, in case of false positives, at this stage because situational awareness is happening and the protocol scope might be expanded if the attack is out of scope, it is possible that the accused right to freedom of opinion be violated.	Life, liberty, and security of person Access to effective remedy Freedom of opinion, thought, conscience, and religion Freedom of assembly and association Privacy Freedom from arbitrary arrest, detention, and exile;	- Situational awareness - Virality - Multiple platforms - Broadening GIFCT's scope - Monitoring and surveillance
Identify and validate	Victims of terrorism and violent extremism right to life, liberty, and security might be violated if the attack not validated correctly. Victims of efforts to counter terrorism and violent extremism rights to freedom of opinion, freedom of assembly and association, privacy and freedom from arbitrary arrest and detention might be violated if there is false positive. Use of OSINT might affect the rights of the accused and minorities in case of profiling, right to privacy	Life, liberty, and security of person Nondiscrimination and equality before the law Access to effective remedy Freedom of opinion, thought, conscience, and religion Freedom of assembly and association Privacy Freedom from arbitrary arrest, detention, and exile; right to a fair trial; innocence, before being proven guilty	- Monitoring - Probability of false positive - Verification of information (how it's being verified, who gave it etc) - Diversity of stakeholders' consultation - Use of OSINT
Assess: whether the attempt is mass violence, has a significant online presence, is it by the terrorist or accomplice or by bystander.	Victims of terrorism and violent extremism right to life, liberty, and security might be violated if assessment of mass violence and significance of online presence is not accurate. Victims of efforts to counter terrorism and human rights defenders right to freedom opinion, assembly and association as well as privacy might be violated if mass violence is detected incorrectly. Victims of efforts to counter terrorism right and the accused might be violated if bystander materials are identified as perpetrator's materials. (because it might later on be taken down, which will remove evidence) The users of a platform right to assembly and opinion might be violated if bystander content is flagged (because it can lead to suspension and blocking of their account) Victims of terrorism and violent extremism right to life and liberty might be threatened by the bystander material	Life, liberty, and security of person Nondiscrimination and equality before the law Access to effective remedy Freedom of opinion, thought, conscience, and religion Freedom of assembly and association Privacy Freedom from arbitrary arrest, detention, and exile; right to a fair trial; innocence, before being proven guilty	- Accuracy in identifying perpetrator-only content - Criteria to assess significance of online presence - Assessment of violent or extremist content - Probability of false positive

Activate and notify: activate the protocol, notify the members, inform them the level of action needed	During the activation stage, the protocol operators will reach out to their members and other stakeholders with information about the attack. As the activate and notify stage provides guidance to various members about the level of action that is needed, it has a potential high impact on human rights. The accuracy of information they have received, the use of OSINT and accuracy of the assessment whether it's a violent, extremist attack or not, will have an impact on human rights. Victims of terrorist activities' right to life, liberty, and security might be violated in case of wrong assessment of the event and lack of action. For example, if live streaming is not interrupted, it might potentially impact the right to life and liberty. If a wrong assessment was made and the material was not violent extremist, it could lead to broadening the scope of the protocol. This could have an impact on human rights defenders that might have their content taken down or users that might have their accounts blocked (right to opinion and freedom of expression). Combined with the assessment stage, this stage has a high impact on human rights.	Life, liberty, and security of person Nondiscrimination and equality before the law Access to effective remedy Freedom of opinion, thought, conscience, and religion Freedom of assembly and association Privacy Freedom from arbitrary arrest, detention, and exile; right to a fair trial; innocence, before being proven guilty	- Accuracy and completeness of guidance
Prepare and Act (information sharing stage): look at OSINT materials, share hashes, share awareness about where the content is, share the outcome, ongoing strategic communications	Victims of terrorism and violent extremism right to life, liberty, and security of person and right to effective remedy might be violated in case of transmitting wrong information that could for example lead to deterioration of the situation. For example, if content is taken down the terrorists might become more violent and kill more people. Or at this stage if content is taken down without preservation then the right to effective remedy might be violated. Victims of efforts to counter terrorism and violent extremism right to freedom of opinion, thought, conscience, and religion, as well as freedom of assembly and association, might be violated due to take-down, deamplification and suspension of accounts. Their right to privacy might also be affected due to use of OSINT (since it can lead to profiling) and hash-sharing. Human rights defenders right to freedom of assembly and association as well as freedom of opinion might also be violated if actions such as hash-sharing lead to take-down and deamplification.	Life, liberty, and security of person, Nondiscrimination and equality before the law Access to effective remedy Freedom of opinion, thought, conscience, and religion Freedom of assembly and association Privacy Freedom from arbitrary arrest, detention, and exile; right to a fair trial; innocence, before being proven guilty	- Expansion of hash database - Accuracy and completeness of information sharing (companies act based on their own policy) - Take down of content - Actions taken other than content take-down Sharing hashes with a stakeholder
Conclude: Assessment against threshold, monitoring goes down, and producing summaries of what's gone on	The kinds of actions that are taken during this phase can have future human rights implications of operating a crisis protocol. In conclude the operators should pay special attention to how their actions impacted human rights at each stage of crisis protocol and come up with a mitigation plan for future incidents.	Life, liberty, and security of person Nondiscrimination and equality before the law Access to effective remedy Freedom of opinion, thought, conscience, and religion Freedom of assembly and association Privacy Freedom from arbitrary arrest, detention, and exile; right to a fair trial; innocence, before being proven guilty	- Diversity of stakeholder consultation - Mitigation plan with a human rights analysis for future events



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