GIFCT
Global Internet Forum to Counter Terrorism

GLOBAL INTERNET FORUM TO COUNTER TERRORISM
TRANSPARENCY REPORT #1
July 2019

This serves as the first GIFCT Transparency Report, updating on joint-tech and cross-sector progress and relations. On August 1, 2017, Facebook, Microsoft, Twitter and YouTube launched the Global Internet Forum to Counter Terrorism (GIFCT) to formalize and give structure to existing industry cooperation, to curtail the spread of terrorism and violent extremism online. Building on the ongoing work of the EU Internet Forum, the GIFCT aims to foster collaboration with smaller tech companies, civil society groups, academics, governments and supra-national bodies such as the EU and the UN. We believe that by working together and sharing the best technological and operational elements of our individual efforts, we can have a significantly greater impact on the threat of terrorist content online.

OBJECTIVE

The objective of the GIFCT is to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence. We do this by joining forces with counterterrorism experts around the world and employing four, inter-related strategies:

- Joint Tech Innovation
- Knowledge-Sharing
- Conducting and Funding Research
- Content Incident Protocol

Central to our efforts is preservation of and respect for the fundamental human rights that terrorism seeks to undermine, including free expression. We continue to involve human rights experts and other civil society stakeholders in the GIFCT's work to ensure we stay attuned to and further this aim.

Joint Tech Innovation

In working together to build technological solutions that will prevent and disrupt the spread of terrorist content online, the largest cross-platform advancement supported by the GIFCT has been the creation of a Hash Sharing Consortium. The consortium shares "hashes" (or digital fingerprints) of known terrorist images and videos. The image or video is "hashed" in its raw form and is not linked to any source original platform or user data. Hashes appear as a numerical representation of the original content and can't be reverse engineered to create the image and/or video. A platform needs to find a match with a given hash on their platform in order to see what the hash corresponds with. It is up to each consortium member how they utilize the database, depending on their own terms of service, how their platform operates, and how they utilize technical and human capacities.

Members

The GIFCT launched its Membership Criteria in December 2018 and are pleased to have DropBox and Pinterest join as the newest members of GIFCT. Beyond broader membership, the Hash Sharing Consortium consists of 13 companies who have access to the shared industry database. This includes, Microsoft, Facebook, Twitter, YouTube, Ask.fm, Cloudinary, Instagram, JustPaste.it, LinkedIn, Verizon Media, Reddit, Snap, and Yellow.

Taxonomy and Numbers

At the end of 2018 the GIFCT gave itself the goal of reaching 200k hashes by the end of 2019. We are pleased to say that the Hash Sharing Consortium has reached over 200k unique pieces of terrorist content.

Companies often have slightly different definitions on "terrorism" and "terrorist content". For the purposes of the hash sharing database, and to find an agreed upon common ground, founding companies in 2017 decided to define terrorist content based on content relating to organizations on the UN Terrorist Sanctions lists. Companies also agreed upon a basic taxonomy around the type of content ingested relating to these listed organizations. The taxonomy includes the following labels that are applied to the content when a company ads hashes to the shared database.

- Imminent Credible Threat (ICT): A public posting of a specific, imminent, credible threat of violence toward non-combatants and/or civilian infrastructure.
- Graphic Violence Against Defenceless People: The murder, execution, rape, torture, or infliction of serious bodily harm on defenceless people (prisoner exploitation, obvious non-combatants being targeted).
- Glorification of Terrorist Acts (GTA): Content that glorifies, praises, condones or celebrates attacks *after the fact*.
- Recruitment and Instruction (R&I): Materials that seek to recruit followers, give guidance or instruct them operationally.
- New Zealand Perpetrator Content: The GIFCT set a new precedent in the wake of the New Zealand terrorist attack. Due to the virality and cross-platform spread of the attacker's manifesto and attack video, and because New Zealand authorities deemed all manifesto and attack video content illegal, the GIFCT created a crisis bank to mitigate the spread of this content.

Hashes relating to the various categories

The following shows the breakdown of how much content has been ingested into the shared database of hashes based on the above taxonomy.

- Imminent Credible Threat: 0.4%
- Graphic Violence Against Defenceless People: 4.8%
- Glorification of Terrorist Acts: 85.5%
- Radicalization, Recruitment, Instruction: 9.1%
- New Zealand Perpetrator Content: 0.6%

Law Enforcement and/or Government Requests for GIFCT Content = 0

Because the GIFCT is a consortium of companies working together, the GIFCT is not a social media platform and does not own any original source data or privacy data of any users associated with platforms members. There have been no formal requests from Law Enforcement or Governments to gain access to the hash sharing consortium database. No access to non-industry members has been given.

URL Sharing

Increasingly, terrorist content is shared on one platform, linking to content hosted on another platform. Companies only have jurisdiction to remove the primary source content from what is hosted on their services, meaning they can remove a post, but the source link and hosted content remains intact on the 3rd party platform. In 2018, Twitter began a program to share URL's to the platforms that were linked to Twitter posts associated with terrorist content. Twitter has shared over 10k URLs with 12 companies since it began the program.

The GIFCT expanded off of this program starting in January 2019 to allow GIFCT companies to safely share URL links to the industry partner the URL belongs to, that have indicators that the link leads to terrorist hosted content. The one-to-one sharing allows the notified platform to review the link in accordance with its own terms of service to decide if the content is violating. The GIFCT has shared over 9.2k URLs since piloting the project.

Knowledge Sharing

Although our companies have been sharing best practices around counterterrorism for several years, the GIFCT provides a more formal structure to accelerate and strengthen this work, in particular, focusing on knowledge sharing with smaller tech companies and bringing other sectors' expertise to the table. One of the GIFCT's key partners in enhancing our work in this area is the Tech Against Terrorism initiative.

Since its foundations in 2017, the GIFCT, in partnership with Tech Against Terrorism, has held 11 workshops around the world. Workshops bring together tech platforms with policy makers, law enforcement, civil society, academic experts and practitioners to share experiences, best practices and models for cross-sector collaboration.

These workshops have engaged 120+ tech companies, 25+ NGOs and 12 Government bodies taking place in:

- USA (California and New York)
- Paris, France
- Brussels, Belgium
- Berlin, Germany
- Abu Dhabi, United Arab Emirates
- Tel Aviv, Israel
- Jakarta, Indonesia
- Sydney, Australia
- Amman, Jordan

Further events in 2019 are taking place in

- USA (California)
- Delhi, India
- London, United Kingdom

Conducting and Funding Research

The GIFCT supports the Global Research Network on Terrorism and Technology (GRNTT), aimed at developing research and providing policy recommendations around the prevention of terrorist exploitation of technology. The research conducted by this network seeks to better understand radicalization, recruitment and the myriad of ways terrorist entities use the digital space around the world.

The network is led by the Royal United Services Institute (RUSI) in the UK and brings together partners from around the world, including the Brookings Institution (US), the International Centre for Counter-Terrorism (Netherlands), Swansea University (UK), the Observer Research Foundation (India), the International Institute for Counter-Terrorism (Israel) and the Institute for Policy Analysis of Conflict (Indonesia).

Six papers have been published in 2019 from the GRNTT and a further six will be published by the end of 2019. Current publications include:

- Paper No. 1- Public–Private Collaboration to Counter the Use of the Internet for Terrorist Purposes: What Can be Learnt from Efforts on Terrorist Financing?
- Paper No. 2- A Study of Outlinks Contained in Tweets Mentioning *Rumiyah*
- Paper No. 3- Shedding Light on Terrorist and Extremist Content Removal
- Paper No. 4- Following the Whack-a-Mole Britain First's Visual Strategy from Facebook to Gab
- Paper No. 5- The Evolution of Online Violent Extremism in Indonesia and the Philippines
- Paper No. 6- Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability
- Paper No. 7- Terrorist Definitions and Designations Lists: What Technology Companies Need to Know

Content Incident Protocol

Content Incident Protocol is the newest work stream for the GIFCT, launching July 2019 in response to the Christchurch Call to Action, creating an action plan for companies when faced with attacks coordinated with the specific and planned intent of content going viral. The Content Incident Protocol has a triaged system aiming to minimize the online spread of terrorist or violent extremist content resulting from a real-world attack on defenseless civilians/innocents. The GIFCT commits to working collaboratively across industry, governments, and NGOs on protocols for responding to emerging or active events, on an urgent basis.

For more information on the Global Internet Forum to Counter Terrorism, please visit http://www.gifct.org. To get in contact please reach out to industry@gifct.org, government@gifct.org, outreach@gifct.org or press@gifct.org.