GIFCT Transparency Report July 2020

On August 1, 2017, Facebook, Microsoft, Twitter and YouTube launched the Global Internet Forum to Counter Terrorism (GIFCT) to formalize the existing industry cooperation established 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 supranational 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.

In September 2019 during the UN General Assembly the GIFCT announced that it would be reorganized as an independent Non-Governmental Organization. This came with an updated mission statement, that includes violent extremism to broaden the scope of focus in line with the Christchurch Call to Action. The announcement also included plans to re-organize the GIFCT goals, while maintaining its output and impact to date.

NEW STRUCTURE

The Global Internet Forum to Counter Terrorism is now an independent 501(c)(3) registered in the United States and has an independent Executive Director and staff. Here is more information about the new structure.

The GIFCT's mission statement has been redrawn. It now reads: "Prevent terrorists and violent extremists from exploiting digital platforms."

The GIFCT has four core goals:

- Improve the capacity of a broad range of technology companies, independently and collectively, to prevent and respond to abuse of their digital platforms by terrorists and violent extremists
- Enable multi-stakeholder engagement around terrorist and violent extremist misuse of the internet and encourage stakeholders to meet key commitments consistent with the GIFCT mission
- Encourage those dedicated to online civil dialogue and empower efforts to direct positive alternatives to the messages of terrorists and violent extremists
- Advance broad understanding of terrorist and violent extremist operations and their evolution, including the intersection of online and offline activities

Strategic Pillars

Existing GIFCT workstreams, such as employing and leveraging technology, exemplified by the shared industry hash database of "digital fingerprints" of violent terrorist imagery and propaganda; knowledge-sharing efforts, and the Global Network on Extremism and Technology will be folded into three strategic pillars designed to house and foster additional work programs and maximize transparency. The strategic pillars are:

● “Prevent” to equip digital platforms and civil society groups with awareness, knowledge and tools, including technology, to develop sustainable programs in their core business operations to disrupt terrorist and violent extremist activity online.

● “Respond” develops tools and capacity, including via regular multi-stakeholder exercises, for platforms to cooperate with one another and with other stakeholders to mitigate the impact of a terrorist or violent extremist attack.

● “Learn” is empowering researchers to study terrorism and counterterrorism, including creating and evaluating best practices for multi-stakeholder cooperation and preventing abuse of digital platforms.

Importantly, GIFCT members will continue to enforce their own policies and standards, and engage in other standard operating procedures associated with content removals, account closures, and similar enforcement actions related to violations of terms of service or community standards. Membership in the GIFCT and participation in operational programs like the shared industry hash database, does not replace or supplant a company’s internal policies, standards and procedures.

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 integrate this central tenet to all GIFCT work.

Executive Director

In June, GIFCT announced the hiring of its first full-time executive director, Nicholas J. Rasmussen, overseeing all day-to-day activities and operations of the non-governmental organization. Before beginning his role on June 29, 2020, Rasmussen served as the Senior Director for National Security and Counterterrorism of the McCain Institute for International Leadership. He previously held high-level roles in government, including Director of the National Counterterrorism Center under both Presidents Obama and Trump, Special Assistant to the President and Senior Director for Counterterrorism on the National Security Council (NSC) staff under President Obama, Director of Regional Affairs in the NSC’s Office of Combatting Terrorism under President George W. Bush and in critical roles at the U.S. Department of State for more than a decade. He holds academic posts at the Sandra Day O’Connor College of Law at Arizona State University, the University of Texas at Austin School of Law, the National Security College of Australia National University and the Reiss Center on Law and Security at New York University School of Law.

Independent Advisory Council

On June 16, 2020, the GIFCT announced full membership of the inaugural Independent Advisory Committee (IAC). The 21 members include representatives from seven governments, two international organizations, and 12 civil society organizations (CSO), spanning a range of expertise. CSO specialties include counter terrorism and countering violent extremism non-governmental organizations, digital and human rights groups, foundations, and academics. The governments represented on the IAC are Canada, France, Ghana, Japan, New Zealand, the United Kingdom, and the United States. The European Union and the United Nations Counter Terrorism Executive Directorate are the two international organizations on the IAC. Civil society representatives come from four continents and eight countries.

Mr. Bjørn Ihler of Norway was selected by his fellow IAC members to serve as the inaugural IAC Chair. Mr. Ihler's two-year term began on July 20, 2020. As IAC Chair, Mr. Ihler will serve as a non-voting member of the Operating Board.

Operating Board

The Operating Board selected the Executive Director, provides the operational budget, and ensures overall GIFCT operations align with its mission.

The Operating Board is composed of:

- GIFCT's founding members - Facebook, Microsoft, Twitter, and YouTube
- At least one rotating company from the broader membership cadre
- New companies that meet leadership criteria
- The rotating chair of the Independent Advisory Committee, who participates as a non-voting member

The Operating Board chair rotates annually. Microsoft is the Operating Board chair for 2020.

TRANSPARENCY ON JOINT TECH INNOVATIONS

Hash Sharing Consortium

The largest cross-platform technical tool supported by the GIFCT is the 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, which means it cannot be easily reverse engineered to create the image and/or video. It is up to each consortium member how they leverage the database, depending on, among other things, their own terms of service, how their platform operates, and how they utilize technical and human capacities.

Just like governments, intergovernmental institutions, civil society organizations, and academics, companies often have slightly different definitions of "terrorism" and "terrorist content". To find common ground, the original scope of the hash-sharing database was therefore limited to content related to organizations on the United Nations Security Council's consolidated sanctions list. The only hashes that appear in the Hash Sharing database that do not correspond to entities on the UN list were added during a declared Content Incident Protocol, which will be discussed in more detail below.

Taxonomy and numbers

To date, the Hash Sharing Consortium has reached 300K unique hashes in the database - the result of approximately 250K visually distinct images and approximately 50K visually distinct videos having been added. Hashes in the database are labeled per the following taxonomy:

• Imminent Credible Threat (ICT): A public posting of a specific, imminent, credible threat of violence toward non-combatants and/or civilian infrastructure.

• Graphic Violence Against Defenseless People: The murder, execution, rape, torture, or infliction of serious bodily harm on defenseless people (prisoner exploitation, obvious non-combatants being targeted).

• Glorification of Terrorist Acts (GTA): Content that glorifies, praises, condones or celebrates attacks after the fact.

• Recruitment and Instruction (R&I): Materials that seek to recruit followers, give guidance or instruct them operationally.

• 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 in the hash database to help mitigate the spread of this content.

• Halle, Germany, Perpetrator Content: 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.

• Glendale, Arizona, U.S., Perpetrator Content: On Wednesday, May 20, 2020, the GIFCT activated its Content Incident Protocol following the shooting in Glendale, AZ, adding hashes of visual distinct videos depicting the attacker's content during the shooting.

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 to date.

• Imminent Credible Threat: 0.1%

• Graphic Violence Against Defenseless People: 16.9%

• Glorification of Terrorist Acts: 72%

• Radicalization, Recruitment, Instruction: 2.1%

• Christchurch, New Zealand, attack and Content Incident Protocols

Christchurch, New Zealand Perpetrator Content: 6.8%

Halle, Germany, Perpetrator Content (CIP): 2%

Glendale, Arizona, U.S., Perpetrator Content (CIP): 0.1%

The Hash Sharing Consortium also launched new tooling in 2019 to better allow tech companies within the consortium to express disagreement with hashes shared within the database. If a company believes that a hash in the database was added erroneously or has been mislabeled, they can express that disagreement in two ways: First, a company can add a label indicating agreement that the hash is terrorist

content, but that they believe it was labeled incorrectly via the taxonomy. Second, a company can add a label to a hash indicating that they do not feel the content is explicitly terrorist content (disputed content). These labels are visible for all companies within the Hash Sharing Consortium so that third companies can make their own decision on how best to use the hashes within various taxonomy buckets, dependent on their own processes and review systems. We are currently still determining the best way to measure and quantify the feedback captured with these labels within the tool in order to share an accurate measurement of alignment and disagreement between and among members regarding different hashed content. We look forward to providing metrics in this regard in future Transparency Reports.

Because the GIFCT is a consortium of companies working together, the GIFCT is not a social media platform and does not own or store any original source data or privacy data of any users associated with platform members.

Over the course of the last year, GIFCT received one request from a government entity regarding content in the hash-sharing database. This request came from United Kingdom Law Enforcement and, in response, GIFCT stated that questions and requests for certain content should be directed towards member companies since hashes are only numerical representations of the original content and cannot be reverse engineered to recreate an image or video.

Content Incident Protocol (CIP)

The GIFCT Content Incident Protocol (CIP) was created in April 2019 and announced in July 2019 in response to the tragedy in Christchurch. The Content Incident Protocol is a system that aims to thwart the online proliferation of content produced by a perpetrator during the course of a real-world attack. The GIFCT has initiated the CIP twice in response to two, separate real-world events. The GIFCT commits to working collaboratively across industry, governments, and NGOs on protocols for responding to emerging or active events, on an urgent basis. More information on the CIP is found here.

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. Inspired by Twitter's effort to share URL's with platforms that were linked to from Twitter posts associated with terrorist content, the GIFCT began a program in January 2019 to allow GIFCT companies to safely share URL links to the industry partner the URL belongs to, when they 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. In the first transparency report we reported that GIFCT had shared 9.2k URLs since piloting the project.

In the last year, GIFCT has adapted this program through a 12-month URL sharing pilot with SITE Intelligence, a firm that provides subscription-based monitoring and analysis regarding terrorist content and other online harms. The pilot project gave some of GIFCT's newer members access to SITE's SourceFeed, providing access to a dashboard assisting with extra context around a given URL including; organizational affiliation of the terrorist content and translation of content into English and further context support. Through this program, GIFCT has now shared nearly 24K URLs since its launch. The majority of new URLs shared amongst GIFCT member companies came from SITE.

Members

GIFCT Members include; Microsoft, Facebook, Twitter, YouTube, Instagram, DropBox, Pinterest, Mega.nz, WhatsApp, LinkedIn and Amazon

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.

Tech companies seeking to join GIFCT and participate in the Hash Sharing Consortium need to follow GIFCT's membership criteria.

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 founding in 2017, the GIFCT, in partnership with Tech Against Terrorism, has held 13 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. Over the last three years, these workshops have engaged 140 tech companies, 40 NGOs and 15 government bodies taking place in:

- Sydney, Australia
- Brussels, Belgium
- Paris, France
- Berlin, Germany
- Jakarta, Indonesia
- Tel Aviv, Israel
- Amman, Jordan
- Abu Dhabi, United Arab Emirates
- California, USA (x2)
- New York, USA
- Delhi, India

• London, United Kingdom

The final two workshops in Delhi and London took place in the latter half of 2019, before the pandemic put a halt to organizing further in-person meetings. Of significance with these two workshops, both ensured to include multi-sector practitioners in CVE and counterterrorism, including Law Enforcement agencies, who were invited to share declassified threat assessments and concerns around adversarial shifts. In the London workshop in December 2019, Tech Against Terrorism and GIFCT worked to have Law Enforcement officers from across the Five Eye countries, come to debrief the workshop. We look forward to continuing these knowledge sharing efforts when it is safe to do so.

CONDUCTING AND FUNDING RESEARCH

In Phase One (2018 - 2019) GIFCT supported the Global Research Network on Terrorism and Technology (GRNTT), aimed at developing research and providing policy recommendations around the prevention of terrorist exploitation of technology. Thirteen papers were published in 2019 from the GRNTT and can be found here.

In January 2020, GIFCT began Phase Two of support for its academic research network, led by the International Centre for the Study of Radicalisation (ICSR), based at King's College London. ICSR has established the Global Network on Extremism and Technology (GNET) and brings together an international consortium of leading academic institutions and experts with core institutional partnerships from the US, UK, Australia, Germany and Singapore to study and share findings on combating terrorist and violent extremist use of digital platforms. GNET builds on Phase One of the GIFCT academic research network known as the Global Research Network on Terrorism and Technology, building a wider network of academic institutions and think tanks as well as collaboration with existing partners.

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 outreach@gifct.org or press@gifct.org.

CONTACT

For more information about the Global Internet Forum to Counter Terrorism (GIFCT), please contact outreach@gifct.org or press@gifct.org.