United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

# Insight Briefing

## Countering the Dissemination of Online Content Relating to Violent Extremist and Terrorist Incidents

**Concept Note**

Thursday, August 25 2022

13:30 – 14:30 EDT / 17:30 – 18:30 UTC

## I. Introduction and background

This Insight Briefing is aimed at enriching Member States' understanding of current developments relating to acts of terrorism and violent extremism, as well as responses to such acts. This briefing has been developed in accordance with Security Council resolution 2395 (2017), which reaffirms the essential role of CTED within the United Nations to identify and assess issues, trends and developments relating to the implementation of Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2322 (2016), 2396 (2017), and other relevant resolutions.

In numerous resolutions the Security Council recognized the far-reaching risks associated with the exploitation of the Internet and information communications and technology (ICT) for terrorist purposes.

The Council also repeatedly stressed the importance of cooperation with civil society and the private sector in combatting the misuse and exploitation of the Internet for terrorist purposes. In Security Council resolution 2129 (2013), the Council notes "the evolving nexus between terrorism and information and communications technologies, in particular the Internet, and the use of such technologies to commit terrorist acts, and to facilitate such acts through their use to incite, recruit, fund, or plan terrorist acts, and directed CTED to continue to address this issue, in consultation with Member States, international, regional and subregional organizations, the private sector and civil society and to advise the CTC on further approaches".

More specifically, in resolution 2617 (2021) the Council stressed the need for Member States to act cooperatively to prevent terrorists from exploiting information and communication technologies, as well as the need for Member States to continue voluntary cooperation with the private sector and civil society to develop and implement more effective means to counter the use of the Internet for terrorist purposes, including by developing counterterrorist narratives and through technological solutions, all while respecting human rights and fundamental freedoms and in compliance with domestic and international law. The Council further took note of the industry-led Global Internet Forum to Counter Terrorism (GIFCT) and called for the GIFCT to continue to increase engagement with governments and technology companies globally.

In the same resolution the Council also recognized the efforts of the UN-affiliated Tech Against Terrorism initiative to foster collaboration with representatives from the technology industry, including smaller technology companies, civil society, academia, and government to disrupt terrorists' ability to use the internet in furtherance of terrorist purposes, while also respecting human rights and fundamental freedoms.

## II. Objective

**The Briefing will offer Member States opportunity to learn and examine the development and recent use of the Global Internet Forum to Counter Terrorism's (GIFCT) "Incident Response Framework" (IRF), a suite of protocols which guide the use of various technologies to ensure that GIFCT member companies have the ability to respond in a coordinated manner to terrorist incidents with a significant online aspect, particularly where perpetrator produced content is circulated as part of incident.**

In March 2019, following the broadcasting and livestreaming of the terrorist shootings in Christchurch, New Zealand, GIFCT launched the Content Incident Protocol (CIP), a centralized communications tool among its members for sharing information about ongoing incidents that could potentially spread violent extremist content online. Since then, this tool has been used to identify the publication and dissemination of online content relating to violent extremist and terrorist attacks and then remove related content.

The tool was deployed May 2022 following the domestic terrorism shooting attack in Buffalo, New York, which was livestreamed on Twitch and then proliferated across multiple social media platforms. It was deployed again in June 2022 following the uploading and viral online spread of a video depicting a terrorism-related murder in Udaipur, Rajasthan, India.

## III. Format of discussions

The proposed briefing will consist of opening remarks; presentations from GIFCT and Tech against Terrorism on the use of the CIP in responding to instances of the dissemination of content related to violent extremist and terrorist attacks in online spaces, to include the Internet and social media platforms; and a moderated, interactive question-and-answer session. The briefing will conclude with closing remarks.

## IV. Date and venue

The briefing will be streamed live via Microsoft Teams on Thursday, 25 August 2022 from 13:30 to 14:30 EDT (17:30 – 18:30 UTC). Log-in details will be provided upon registration.