

CTED contribution to the Secretary-General's High-Level Panel on Digital Cooperation

In 2014, Member States faced an acute and growing threat posed by the significant flow of foreign terrorist fighters (FTFs)¹ to the conflict zones of the Middle East. That threat was exacerbated by a marked increase in online radicalization and recruitment. Moreover, those who were radicalized included, inter alia, families with children, teenagers, and school teachers. In this regard, it became quickly apparent that the emerging capacity for people to connect remotely with others located all over the world offered both opportunities and risks. Use of the Internet was enabling terrorist groups to reach deep into every layer of society. By 2015, over 30,000 FTFs, from more than 100 States, had joined terrorist organizations such as Al-Qaida and the Islamic State in Iraq and the Levant (ISIL, also known as Da'esh). The threat posed by FTFs to their States of origin; to States of transit and destination; and to neighbouring zones of armed conflict in which they were active was compounded by the use of information and communications technologies (ICT) to disseminate propaganda, incite hatred, radicalize, recruit, finance, train, plan and execute terrorist attacks.

The Counter-Terrorism Committee Executive Directorate (CTED) — an expert body that serves the Security Council and the broader United Nations membership — is required to assist the Counter-Terrorism Committee to monitor, facilitate and promote Member States' implementation of the relevant Council resolutions on terrorism. CTED's response to the above challenges sought to reconcile the positive and negative aspects of new technologies: their considerable potential to improve our quality of life and their vulnerability to abuse by terrorists. Accordingly, CTED assists Member States to develop ways to prevent use of the Internet for terrorist purposes, counter terrorist narratives, and develop innovative technological solutions, in respect for human rights and fundamental freedoms and in compliance with their other obligations under international law. CTED also emphasizes the need for States to identify an appropriate balance between countering hate speech and safeguarding freedom of expression, as well as to work together to identify durable solutions to these challenges, regardless of their differences of opinion.

In doing so, CTED promotes a holistic, all-of society, and comprehensive approach to addressing the conditions conducive to the spread of violent extremism that could be conducive to terrorism, including by encouraging dialogue and collaboration with civil society, the private sector, and other relevant stakeholders. In accordance with a number of resolutions² adopted by the Security Council between 2013 and 2017, as well as the Comprehensive International Framework to Counter Terrorist Narratives³ and the [*Addendum to the guiding principles on foreign terrorist fighters \(2018\)*](#)⁴.

CTED with the full support of the Committee has actively engaged in a number of initiatives with the private sector in this area:

¹ In its resolution 2178 (2014), the Security Council defines foreign terrorist fighters as “individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict”.

² Security Council resolutions 2129 (2013), 2178 (2014), 2322 (2016), 2341 (2017), 2354 (2017), 2395 (2017) and 2396 (2017).

³ The Comprehensive International Framework to Counter Terrorist Narratives calls for improved public-private cooperation in tackling the use of the Internet for terrorist purposes while also respecting human rights.

⁴ The *Madrid Guiding Principles* were adopted in 2015 as a practical tool to assist Member States to stem the flow of FTFs. In December 2018, the Counter-Terrorism Committee updated the Principles, through the adoption of the *Addendum* to reflect the rapidly evolving FTF situation, including in the context of Security Council resolution 2396 (2017).

Counter-Terrorism Committee Executive Directorate (CTED)

- ***Tech Against Terrorism***. A public/private partnership launched in April 2017 by CTED, *Tech Against Terrorism* aims to support the technology industry to develop more effective and responsible approaches to tackling terrorists' use of the Internet, while respecting human rights. The guiding principle of *Tech Against Terrorism* is that smaller platforms are most vulnerable to use of the Internet for terrorist purposes. Larger companies are generally better able to address the threat to their systems. *Tech Against Terrorism* supports technology platforms in the areas of social media, cloud computing, storage, and financial technology (FinTech), helping them to identify and mitigate risk and share knowledge and best practices. It also develops resources to assist such platforms, providing capacity-building and operational support and facilitating their cooperation with Government, civil society, and academia. A further important resource for the promotion of good practices is the [Knowledge-Sharing Platform](#) (KSP), a website that is exclusive to members of the *Tech Against Terrorism* initiative and contains a collection of tools and resources to support their efforts.
- **Global Internet Forum to Counter Terrorism (GIFCT)**. CTED supports the efforts of this industry-led initiative to develop technological solutions, conduct research, and share knowledge with smaller companies to contribute to the global fight against terrorism. The GIFCT implements many of its activities within the framework of the *Tech Against Terrorism* initiative. As part of the GIFCT's efforts to share knowledge and best practices, CTED and *Tech against Terrorism* have cooperated on a series of activities, such as the development and promotion of the KSP and the organization of joint workshops to enhance public/private partnerships. Committed to preserving and respecting the fundamental human rights that terrorism seeks to undermine, the GIFCT also collaborates with a broad range of NGOs, academic experts, Governments, and human rights experts.
- **Global initiative on accessing digital evidence**. Accessing digital data produced by terrorists is necessary to bring terrorists to justice. Mindful of the challenges faced by States in their efforts to obtain electronic evidence from Internet Service Providers, CTED is currently engaged in a global initiative, jointly implemented with the United Nations Office on Drugs and Crime and the International Association of Prosecutors, aimed at strengthening the capacity of central authorities, prosecutors and investigators to preserve and obtain electronic evidence within the framework of cross-border counter-terrorism investigations. A key project output is the [Practical Guide for Requesting Electronic Evidence Across Borders](#), which was developed through a consultation process that involved numerous stakeholders, including private-sector entities.

Thanks to the joint efforts of Member States, international organizations, the private sector and civil society, it has become increasingly difficult for terrorist groups - particularly ISIL and its affiliates - to exploit social media platforms for terrorist purposes. Within the framework of the GIFCT, major social media companies have expanded their self-regulation methodologies, focusing on responding to breaches of terms-of-service agreements, and developed systems to proactively flag and remove terrorist material and the accounts responsible for their transmission. Technology firms have taken steps to improve their response to government requests for content removal or data in the context of an investigation and introduced measures to ensure greater transparency in handling such requests. Member States have increasingly criminalized unlawful acts committed by terrorists on the Internet. Guided by its mandate, the principles of the Secretary-General's strategy on new technologies, and the work of the High-Level Panel on Digital

Counter-Terrorism Committee Executive Directorate (CTED)

Cooperation, CTED will continue to engage closely with Member States and with its implementing partners to promote public/private sector cooperation in countering terrorism and violent extremism while respecting human rights.