Terrorists and terrorist groups exploit the Internet and social media not only to commit terrorist acts, but also to facilitate a wide range of terrorist activities, including incitement, radicalization, recruitment, training, planning, collection of information, communications, preparation, and financing.

In its work to address the abuse of information and communications technologies (ICT) by terrorists and terrorist groups, the Counter-Terrorism Committee (CTC) is guided by several Security Council resolutions, including:

- Adopted shortly after the 11 September attacks against the United States in 2001, Security Council resolution 1373 calls on all Member States to find ways to intensify and accelerate the exchange of operational information concerning the use of ICT by terrorist groups and to suppress terrorist recruitment.
- Security Council resolution 1624, adopted in 2005, calls for necessary and appropriate measures in accordance with Member States’ obligations under international law to prohibit by law incitement to commit a terrorist act and prevent such conduct.
- Security Council resolution 2129 (2013) directs the Counter-Terrorism Committee Executive Directorate (CTED), which was created in 2004 and declared operational in December 2005, to continue to address the use of ICT in terrorist activities, in consultation with Member States, international, regional, and subregional organizations, the private sector, and civil society, and to advise the Committee on further approaches.
- Security Council resolution 2178 (2014), on stemming the flow of foreign terrorist fighters, calls on Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications, and resources to incite support for terrorist acts. In doing so, States should respect human rights and fundamental freedoms and ensure compliance with their obligations under international law.

The related work of CTED focuses on four pillars: (i) mainstreaming ICT in its assessment of Member States’ implementation of resolutions 1373 (2001), 1624 (2005), and 2178 (2014); (ii) promoting industry self-regulation; (iii) strengthening mutual legal assistance regarding digital content; and (iv) promoting counter-messaging techniques, including online.
Since 2014, CTED has actively been engaging with the private sector in this area. In 2016, this collaboration was formalized in a public-private partnership that is now called Tech Against Terrorism. This initiative, which involves numerous partners from Government, the private sector, trade associations, civil society, academia, and multi-stakeholder fora, aims to support the global tech industry to tackle terrorist exploitation of their technologies, while respecting human rights. Based on worldwide consultations with key stakeholders, Tech Against Terrorism works with the global technology sector to share good practices, including policies, guidelines, learning materials, practical workshops, and other tools. Another key feature is the support and knowhow shared by major platforms with smaller platforms and start-ups to avoid exploitation by terrorists.

Tech Against Terrorism works in close collaboration with the Global Internet Forum to Counter Terrorism (GIFCT), which was founded by Facebook, Google, Microsoft, and Twitter in 2017. Security Council resolutions 2395 (2017) and 2396 (2017) take note of GIFCT and call on GIFCT to continue to increase its engagement with Governments and technology companies globally. The two resolutions recognize the development of Tech Against Terrorism and its efforts to foster collaboration with representatives of the technology industry to disrupt terrorists’ ability to use the Internet for terrorist purposes. Resolution 2395 (2017) recognizes CTED’s work on countering the use of the Internet and social media for terrorist purposes, while respecting human rights and fundamental freedoms. It also notes the need for Member States to comply with their obligations under international law, as well as the need to preserve global connectivity and the free and secure flow of information. The resolution further stresses the importance of cooperation with civil society and the private sector in these endeavours.

In May 2016, Microsoft informed the Security Council that it had amended its terms of use to specifically prohibit the posting of terrorist content by, or in support of, organizations included on the Consolidated United Nations Security Council Sanctions List.

DIGITAL EVIDENCE

A vital part of counter-terrorism efforts is the promotion of effective rule of law-based criminal justice responses. In practice, Member States face significant challenges in their attempts to obtain admissible evidence that can be used to help prosecute and secure convictions of terrorist suspects in judicial proceedings. The situation of foreign terrorist fighters (FTFs) who travel to, or return from, conflict zones represents a particularly acute challenge. Because information related to the activities of FTFs is often located on the battlefield, it may be inaccessible to civilian prosecutors and investigators. Therefore, the prosecution of FTFs may depend on the use of Internet-based or digital evidence and may require forms of judicial cooperation that are not provided for in established legal frameworks.

To address this serious challenge, CTED together with the International Association of Prosecutors (IAP) and the United Nations Office on Drugs and Crime (UNODC) in September 2018 launched a Practical guide for requesting electronic evidence across borders, which also responds to Security Council resolutions 2322 (2016), 2331 (2016), and 2341 (2017), calling on Member States to collect and preserve evidence for the purposes of investigations and prosecutions aimed at holding accountable those responsible for terrorist attacks.