## INFORMATION AND COMMUNICATIONS TECHNOLOGIES

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 15 counter-terrorism related resolutions[1] and four policy documents on the matter:[2]
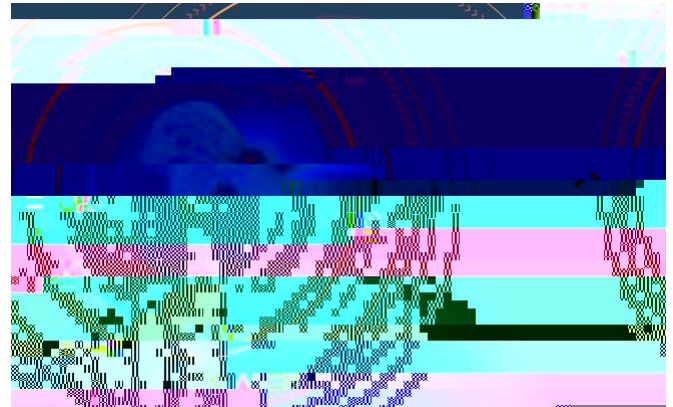
The Security Council adopted resolution 1373 (2001) shortly after the 11 September attacks against the United States in 2001, calling upon all Member States to find ways to intensify and accelerate the exchange of operational information concerning the use of ICT by terrorist groups and to suppress terrorist recruitment.

the Council 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.

the Council notes the evolving nexus between terrorism and ICT, 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. It also directs CTED 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.

on stemming the flow of foreign terrorist fighters, the Council calls upon 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.

---

[1] These include resolutions 1373 (2001), 1624 (2005), 1963 (2010), 2129 (2013), 2178 (2014), 2199 (2015), 2322 (2016), 2331 (2016), 2341 (2017), 2354 (2017), 2370 (2017), 2395 (2017), 2396 (2017), 2462 (2019), and 2617 (2021).

[2] These consist of the Madrid Guiding Principles (S/2015/939), the Statement by the President of the Security Council (S/PRST/2016/6), the Comprehensive international framework to counter terrorist narratives (S/2017/375), and the Addendum to the Guiding Principles on foreign terrorist fighters (2018) (S/2018/1177).

the Security Council
calls upon Member States to collect and preserve digital evidence so that investigations and prosecutions may occur to hold those responsible for terrorist attacks accountable.

the Council
acknowledges the need to develop public-private partnership, through voluntary cooperation, to address the exploitation of ICT by terrorists, including in developing counter

an independent non-governmental organization (NGO). This initiative, which involves numerous partners from government, the private sector, trade associations, civil society, academia, and multi-stakeholder forums, aims to support the global technology industry, with a focus on small platforms and service providers, to tackle terrorist exploitation of their technologies, while respecting human rights.

CTED has also been an important partner of the Global Internet Forum to Counter Terrorism (GIFCT), founded