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

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]

MORE INFORMATION

More info about CTC and CTED, including the CTC Chair and CTED's Executive Director, can be found here: www.un.org/securitycouncil/ctc/content/about-us-0.

A list of FAQs is available here: www.un.org/securitycouncil/ctc/content/frequently-asked-questions-faqs.

- 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.

- **In resolution 1624 (2005),** 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.

- **In its resolution 2129 (2013),** 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.

- **In resolution 2178 (2014)** 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).

- **In resolutions, 2322 (2016), 2331 (2016), 2341 (2017) and 2396 (2017),** the Security Council calls upon Member States to collect and preserve digital evidence so that investigations and prosecutions may occur to hold those responsible forterrorist attacks accountable.

- **In resolutions 2341 (2017), 2354 (2017), 2395 (2017) and 2396 (2017),** the Council acknowledges the need to develop public-private partnership, through voluntary cooperation, to address the exploitationof ICT by terrorists, including in developing counter-narratives and technological solutions, while respectinghuman rights and fundamental freedoms, and ensuring compliance with domestic and international law. In resolutions 2395 (2017) and 2617 (2021), the Council recognizes CTED's work in this regard.

- **Resolution 2354 (2017)** sets out guidelines for implementing a "comprehensive international framework" on counter-narratives and amplifying positive and credible alternatives to audiences vulnerable to extremist messages.

- **In resolution 2462 (2019),** the Council notes the use of crowdsourcing and the use of emerging payment methods, such as prepaid cards and mobile-payments or virtual assets.

- **In its resolution 2617 (2021),** the Council refers to other "emerging technologies", with respect to which CTED is encouraged to deepen its engagement and cooperation with relevant private sector entities. The Council also noted the need to preserve global connectivity and the free and secure flow of information, facilitating economic development, communication, participation, and access to information, and stressed the importance of cooperation with civil society and the private sector in this endeavour.

CTED assists Member States to develop ways to prevent the use of the Internet for terrorist purposes, counter terrorist narratives, and develop innovative technological solutions, in respect of human rights and fundamental freedoms and in compliance with their other obligations under international law. CTED emphasizes the need for States to work together to identify durable solutions for ICT-related challenges, despite differences in opinion regarding methodology and desired end results. CTED strongly promotes a holistic, all-of-society, and comprehensive approach that includes civil society organizations (CSOs) and public-private partnerships, to address the many challenges that arise around countering violent extremism and terrorism online.

CTED's work on ICT currently focuses on **six main pillars**: (i) mainstreaming ICT into the assessment visits conducted on behalf of the Committee to assess Member States' implementation of the relevant Security Council resolutions; (ii) promoting industry self-regulation and public-private partnerships; (iii) strengthening international cooperation for legal access to digital content; (iv) promoting counter-messaging techniques, including online; (v) compliance with human rights and fundamental freedoms in ICT; and (vi) the identification of new trends and developments in terrorist use of ICTs.

As part of its work on **human rights and fundamental freedoms and States' compliance with obligations under international law** and their domestic legal frameworks, CTED is working in areas relating to privacy; appropriate access to and sharing of data; and human rights and gender concerns relating to the programming and use of artificial intelligence and algorithmic systems, particularly those used in law enforcement and border control (i.e., CCTV/surveillance and facial recognition technology).

CTED is looking at new trends in terrorist use of ICTs, such as cyber-based fundraising methods and the use of gaming platforms to incite violence and recruit the next generation of extremists and terrorists. CTED is also working on issues relating to **transparency**, including through its support for initiatives to increase transparency through the provision and publishing of data on basic elements of government data request-processing and wider removal compliance.

The **breadth of CTED's work has expanded via new relationships and partnerships** to include cooperation with outside partners such as CSOs, religious actors, the Global Research Network (GRN) of respected think tank and academic experts, and private sector entities; as well initiatives to strengthen public and private partnerships, as per resolution 2395 (2017). Since 2014, CTED has actively been engaging with the private sector in this area. In 2017, this collaboration was formalized in a public-private partnership called Tech Against Terrorism, now

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 by Facebook, Google, Microsoft, and Twitter in 2017, and now an independent NGO. CTED is a member of GIFCT's Independent Advisory Committee and its working groups on Academic and Practical Research and Legal Frameworks (Data). CTED also works closely with the Christchurch Call to Action and a range of other partners.