

A BE GBA A B HA GBAFG AB B F G

errorists 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:



More info.08 r9N3 Tmbo2info.08 r

Adopted shortly after the 11 September attacks against the United States in 2001, Security Council resolution 1373 calls on all Member Statesto find ways to intensify and accelerate the exchange of operational information concerning the use of ICT by terrorist groups and to suppressterrorist recruitment.

Security Council resolution 1624, adopted in 2005, calls for necessary and appropriate measures in accordance with Member 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 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 view of the challenges and pursuant to resolutions 2322 (2016), 2331 (2016), 2341 (2017), and 2396 (2017) and the CTC Madrid Guiding Principles on FTF and its Addendum, CTED together with the International Association of Prosecutors (IAP) and the United Nations Office on Drugs and Orime (UNODC) launched a , in September 2018. This initiative is strengthening the capacity of central authorities, prosecutors and investigators

A

T

EG AG A

he use of AI in CT, from automatic content moderation by communication service providers to the use of biometrics, is widespread. Machine learning and decision-making are seen both as extremely powerful surveillance and investigative tools but also as serious threats to the enjoyment of civil and political rights, from privacy and freedom of expression to racial and gender discrimination. CTED has been collaborating with various partners that are working on this area, notably UNICRI and the World Economic Forum. Additionally, CTED has been following developments in the use of AI-