UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED)

INFORMATION AND COMMUNICATIONS TECHNOLOGIES (ICT)

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.
- **In resolutions, 2322 (2016), 2331 (2016), 2341 (2017) and 2396 (2017),** the Security Council calls upon Member States to collect and

MORE INFORMATION

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

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

preserve digital evidence so that investigations and prosecutions may occur to hold those responsible for terrorist attacks accountable.

- **Security Council resolutions 2341 (2017), 2354 (2017), 2395 (2017) and 2396 (2017)** acknowledge the need to develop public-private partnership, through voluntary cooperation, to address the exploitation of ICT by terrorists, including in developing counter-narratives and technological solutions, while respecting human rights and fundamental freedom, and ensuring compliance with domestic and international law. Resolution 2395 (2017) recognizes CTED 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.
- **Resolution 2462 (2019)** notes the use of crowdsourcing and the use of emerging payment methods, such as prepaid cards and mobile-payments or virtual-assets.

The related work of CTED focuses on four pillars: (i) mainstreaming ICT in its assessment of Member States' implementation of relevant Security Council resolutions; (ii) promoting industry self-regulation and public-private partnerships; (iii)Strengthening international cooperation for legal access to 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 2017, this collaboration was formalized in a public-private partnership 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 world-wide 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.

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). Tech Against Terrorism works in close collaboration with GIFCT in support of small platforms and the development of technological solutions. Since 2016, GIFCT's members amended their terms of use to prohibit posting of terrorist content, or in support of, organizations of the Consolidated United Nations Security Council Sanctions List. In resolutions 2395 (2017) and 2396 (2017), the Council recognized the development of GIFCT and Tech Against Terrorism and called for these initiatives to continue their efforts to foster public-private collaboration to disrupt terrorists' ability to use the Internet for terrorist purposes.

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), returnees and relocators 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.

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 Crime (UNODC) launched a *Practical guide for requesting electronic evidence across borders*, in September 2018. This initiative is strengthening the capacity of central authorities, prosecutors and investigators to preserve and obtain electronic evidence in the framework of cross-border counter-terrorism investigations and enhancing international cooperation with the private sector in this regard. The initiative has become a multi-stakeholder platform that promotes cooperation and good practices and focused activities such as regional and national workshops, specialists' symposiums and expert group meetings. The pipeline of the future deliverables includes Standardized Data Requests Forms and guidelines for small and medium enterprises.

PROTECTION OF CRITICAL INFRASTRUCTURE

Terrorist groups may eventually acquire the capacity to launch terrorist attacks through the Internet, thereby causing damage to critical infrastructure, industrial control system, or Internet of Things (IoT) devices. Security Council resolution 2341 (2017) directs the CTC with support of CTED to examine Member-States' efforts to protect critical infrastructure from terrorist attacks, related to the implementation of 1373 (2001) and with the aim of identifying good practices, gaps and vulnerabilities in this field. CTED, INTERPOL and OCT developed, in 2018, The protection of critical infrastructure against terror attacks: Compendium of good practices, which may get an addendum addressing with more specificity cyber issues.

DATA PROTECTION AND PRIVACY

As counterterrorist measures are increasingly raising challenges related to privacy and data protection, experts recognize a lack of data protection legal frameworks and guidance to private companies and governments addressing technical issues such as legal enrolment criteria, data retention or deletion policy, data processing, data sharing, preventing misuse of data, data security, validation and oversight. This creates a serious impediment to international cooperation and international sharing of data as many States are prohibited under their national laws to share protected and personal data with countries with weaker data protection regimes. Also, new developments, such as advances in the field of artificial intelligence (e.g. machine learning), and increased reliance on tools powered by this technology make the development of guidance necessary.

CTED is co-leading with UNOC and OCT, and within the framework of the Working Group on Criminal Justice & Legal Responses to Counter-Terrorism and Countering the Financing of Terrorism of the Global Counter-Terrorism Coordination Compact, a project on Developing recommended legislative provisions and a compendium of existing good practices on data protection rules to facilitate international cooperation in counter-terrorism.

ONLINE INVESTIGATIONS

The need of States to have the capacity to conduct open source and Dark Web investigations is recognized as a CT priority by the SC/CTC, and CTC assessments started to look into these matters, such as Small Arms Light Weapons (SALW) Dark Web traffic for example. UNODC, OCT and INTERPOL have all launched capacity building programmes in this area. CTED has participated in several of these projects and has provided expertise. Currently, CTED is working closely with UNCCT on a project of online investigations in South Asia and Southeast Asia, specifically serving as the penholder in the elaboration of a report on recent developments and trends in the use of the internet by terrorists and social media and dark web investigations.

ARTIFICIAL INTELLIGENCE

The 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-powered algorithms by tech platforms (including GIFCT companies) to support their content moderation efforts.

The SG Roadmap for Digital Cooperation notes the importance of AI for the promotion of peace and noted the work of CTED on several AI-related matters. CTED advices EOSG on the implementation of the Roadmap.

NEW TRENDS: EXTREME RIGHT WING TERRORISM, COVID-19, GAMING PLATFORMS AND BEYOND

The rise of Extreme-Right Wing terrorism and the COVID 19 pandemic have seen new forms of use and abuse of new technologies, such as the use of gaming platforms and gamification of terrorist propaganda, which CTED has been monitored and presented in recent CTED Trend Alerts.