Counter-terrorism in cyberspace

Factsheet

June 2021

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. The COVID-19 pandemic, which witnessed lockdowns and social distancing in many Member States, also saw a dramatic increase in use of the Internet, raising significant concern about the abuse of information and communications technologies (ICT) by terrorists and terrorist groups, as well as persons and groups espousing extreme right-wing (or racially or ethnically motivated) ideologies. In its work to address the those underlining issues, the Counter-Terrorism Committee is guided by several Security Council resolutions, including:

- **Security Council resolution 1373 (2001),** adopted shortly after the 11 September 2001 attacks against the United States, which 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 (2005),** which 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),** which directs the Counter-Terrorism Committee Executive Directorate (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.
- **Security Council resolution 2178 (2014),** on stemming the flow of foreign terrorist fighters (FTFs), which 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 its resolutions, 2322 (2016), 2331 (2016), 2341 (2017) and 2396 (2017),** the Security Council calls on States to collect and 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 partnerships, through voluntary cooperation, to address the exploitation of ICT for terrorist purposes, including in developing counter-narratives and technological solutions, while respecting human rights and fundamental freedom, and ensuring compliance with domestic and international law. Security Council resolution 2395 (2017) recognizes CTED's work in this regard.
- **Security Council 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 crowdfunding platforms for raising funds for terrorism purposes as well as the use of emerging payment methods, such as prepaid cards and mobile-payments or virtual-assets, to move and transfer such funds. It also calls for assessing and addressing potential risks associated with virtual assets and new financial instruments.

The Counter-Terrorism Committee has also developed guidance for Member States in this area through the **2015 Madrid Guiding Principles (S/2015/939) and 2018 Addendum (S/2018/1177) on FTFs**. Guiding principles 13, 14, 33, 43 and 44 focus on methods for monitoring and studying terrorist content transmitted over the Internet and other communications technologies; reviewing national mutual legal assistance (MLA) laws and mechanisms in view of increased requests for digital data; and gathering digital data and evidence in cases relating to FTFs. Under the policy guidance of the Committee, CTED's work on ICT focuses on four 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; and (iv) promoting counter-messaging techniques, including online.

CTC ASSESSMENT VISITS OF MEMBER STATES

The use of ICT for terrorist purposes is one of the key thematic areas of the assessment visits to Member States conducted on behalf of the Committee by its Executive Directorate and is currently being integrated into the hybrid visits being conducted in the context of the COVID-19 pandemic. ICT-related issues are outlined in the technical guide to the implementation of Council resolution 1373 (2001) and other relevant resolutions (S/2017/716) and in the updated "Framework document for Counter-Terrorism Committee visits to Member States aimed at monitoring, promoting and facilitating the implementation of Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017), 2462 (2019) and 2482 and other relevant Council resolutions" (S/2020/731). The specific issues relating to the misuse of ICT for terrorist purposes, which are discussed with Member States during assessments visits, include:

- Regulatory and policy frameworks relating to ICT
- Legislation to counter the misuse of ICT for terrorist purposes
- Capacity to use special investigative techniques to monitor the use of ICT for terrorist purposes
- Methods of identifying terrorist content and activities; operational practices to block, filter, and take down terrorism-related online content
- Cooperation with the private sector and civil society (public-private partnerships) to counter the use of ICT for terrorist purposes, including through technological solutions
- Use of digital evidence to bring terrorists to justice, including access to digital evidence stored in another jurisdiction (legislation, national structure, level of law-enforcement and judicial cooperation)
- Policies for critical infrastructure security and resilience against malicious activities by terrorists, including through the use of ICT
- Human rights aspects of Member States' counter-terrorism measures, including appropriate safeguards for freedom of expression relating to ICT.

ICT issues (digital evidence, protection of critical infrastructure, online incitement, online moderation, etc.) have also been included in the Overview of Implementation Assessment (OIA) and the electronic Detailed Implementation Survey (e-DIS), the recently updated survey tools of the Committee and its Executive Directorate, which are hosted in a new cloud-based assessment and analysis portal.

WORK WITH THE PRIVATE SECTOR

Since 2014, CTED, working under the Committee's policy guidance, 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 forums, aims to support the global tech industry to tackle terrorist exploitation of its 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.

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 permanent observer to the GIFCT 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 members have 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 its 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.

COUNTERING VIOLENT EXTREMISM AND TERRORIST NARRATIVES

Terrorist groups have been successful in using propaganda for multiple purposes, including for recruitment and radicalization to violence. Security Council resolution 2354 (2017), builds on the Security Council's presidential statement of 11 May 2016 (S/PRST/2016/6) and the "comprehensive international framework" (S/2017/375), which includes legal and law enforcement measures, public-private partnerships and development of counter-narratives. The resolution sets out a series of guidelines that stress, among other factors, that United Nations actions in the field of countering terrorist narratives should be based on the Charter of the United Nations; that Member States have the primary responsibility in countering terrorism and violent extremism conducive to terrorism; that relevant United Nations entities should ensure greater coordination and coherence with donors and recipients of counter-terrorism capacity-building; that counter-narrative measures and programmes should be tailored to different contexts; that all measures must comply with Member States' obligations under international law, including international human rights law, international refugee law, and international humanitarian law; and that research into the drivers of terrorism and violent extremism is necessary to develop more focused counter-narrative programmes.

Security Council resolution 2354 (2017) requests the Counter-Terrorism Committee to "identify and compile existing good practices in countering terrorist narratives, in coordination with the CTITF [Counter-Terrorism Implementation Task Force] Office [now the United Nations Office of Counter-Terrorism (UNOCT)], and where appropriate in consultation with other relevant non-United Nations entities." The Counter-Terrorism Committee will also "continue to review legal measures taken by States to enhance implementation", "develop further public-private partnerships", conduct outreach to civil society organizations and religious actors, and to work with members of the CTED Global Research Network and others to measure the impact and effectiveness of counter-narratives.

In its assessments of Member States' implementation of the relevant Council resolutions, the Committee and CTED therefore place an emphasis on the steps taken by States to institute programmes and strategies to counter incitement, in accordance with resolution 1624 (2005), criminalizing incitement and countering terrorist-narratives in accordance with resolution 2354 (2017), as well as to counter violent extremism in accordance with 2178 (2014) and others. Wherever there are gaps, the Committee and CTED seek to bring States together with technical assistance providers to develop further initiatives in these areas.

The Committee and CTED are committed to ensuring coordination of their efforts with those being made in support of the United Nations Global Counter-Terrorism Strategy, including through CTED's participation in the United Nations Global Counter-Terrorism Coordination Compact.

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 FTFs and FTF 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 acting pursuant to resolutions 2322 (2016), 2331 (2016), 2341 (2017), and 2396 (2017) and the above-mentioned Madrid Guiding Principles on FTFs and 2018 Addendum, CTED, acting together with the International Association of Prosecutors (IAP) and the United Nations Office on Drugs and Crime (UNODC), launched a global initiative to strengthen the capacity of central authorities, prosecutors and investigators to preserve and obtain electronic evidence within 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, specialist symposiums and expert group meetings. Several reference tools have been developed in the framework of the initiative, including two editions of the *Practical guide for requesting electronic evidence across borders*, an extensive mapping of Communication Service Providers (CSPs) and Standardized Data Requests Forms (developed in partnership with Europol SIRIUS, EuroMed and the European Union Agency for Criminal Justice Cooperation (Eurojust).

DATA PROTECTION AND PRIVACY

As counter-terrorism measures increasingly raise challenges relating to privacy and data protection, experts recognize a lack of data-protection legal frameworks and guidance for 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, from sharing protected and personal data with States 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, together with UNODC and UNOCT, and within the framework of the Working Group on Criminal Justice and 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 for States to have the capacity to conduct open source and Dark Web investigations is recognized as a counter-terrorism priority by the Security Council and the Counter-Terrorism Committee, and the Committee's assessments have begun to look into such matters, including Small Arms and Light Weapons (SALW) Dark Web traffic. UNODC, UNOCT and INTERPOL have all launched capacity-building programmes in this area. CTED has participated in several of these projects and has also provided expertise. Currently, CTED is working closely with the United Nations Counter-Terrorism Centre (UNCCT/UNOCT) on a joint project on online investigations in South Asia and South-East Asia, specifically leading the drafting of a report on recent developments and trends in the use of the Internet for terrorist purposes and social media and dark web investigations.

ARTIFICIAL INTELLIGENCE

The use of artificial intelligence (AI) in counter-terrorism, from automatic content moderation by CSPs to the use of biometrics, is widespread. Machine learning and decision-making are seen as extremely powerful surveillance and investigative tools but also as serious threats to the enjoyment of civil and political rights (including with respect to privacy and freedom of expression to racial and gender discrimination). CTED has been collaborating with various partners that are working on this area, notably the United Nations Interregional Crime and Justice Research Institute (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 Secretary-General's Roadmap for Digital Cooperation notes the importance of AI for the promotion of peace and notes the work of CTED on several AI-related matters. CTED advices the Executive Office of the Secretary-General on the implementation of the Roadmap.

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 systems, or the Internet of Things (IoT) devices. Security Council resolution 2341 (2017) directs the Counter-Terrorism

Committee, with the 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 UNOCT developed, in 2018, "The protection of critical infrastructure against terror attacks: Compendium of good practices", which may be complemented by an addendum addressing cyber issues with more specificity.

NEW FINANCIAL INSTRUMENTS

New technologies using decentralized and distributed structures, such as blockchain-related technologies, can be used and leveraged by various parties to exchange, move, withdraw or account for various classes of assets outside classical financial networks. Virtual assets, such as Bitcoin, allow for the anonymous transfer of funds internationally, which is known to have been increasingly used to finance terrorism. Globally, the use of crowdfunding techniques also represents a recognized terrorism-financing risk. Crowdfunding is an Internet-enabled way for businesses, organizations or individuals to raise money, through donations or investments, from multiple individuals. In its work on countering the financing of terrorism (CFT), CTED has been paying increasing attention to terrorism-financing risks associated with new technologies, including virtual assets and crowdfunding platforms, and the need to establish related effective partnerships with the private sector. CTED monitors and analyses the latest trends in this area through its dialogue with Member States (including in the framework of CFT assessments); participation in relevant expert forums (including specialized projects of the Financial Action Task Force (FATF)); exchanges with the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida and the Taliban and associated individuals and entities and other relevant partners; consultations with private sector and civil society organizations); and ongoing research (including through its Global Research Network). In accordance with resolution 2462 (2019), CTED also works with States to ensure that they apply risk-based CFT regulations, monitoring and supervision to virtual asset service providers.