CTED-led technical meetings informing the
Special Meeting of the Counter-Terrorism Committee (CTC) on
"Countering the use of new and emerging technologies for terrorist purposes"

Countering terrorist exploitation of information and communication technologies (ICT) and emerging technologies

30 September 2022 from 9.00 – 12.30 EDT / 13.00 – 16.30 UTC
and
3 October 2022 9.00 – 13.00 EDT / 13.00 – 17.00 UTC

Virtual meeting via Microsoft Teams

CONCEPT NOTE

Register here by COB 26 September 2022: https://forms.office.com/r/548UND6T5Y

Background

New and emerging technologies – particularly information and communications technologies (ICT) such as the Internet and social media platforms – have become a favoured tool for terrorists such as the Islamic State in Iraq and the Levant (ISIL)/Da'esh, Al-Qaida, their affiliated groups, other terrorist organizations, and their supporters to engage in terrorism. Member States already face a significant and growing threat from the exploitation of new and emerging technologies to facilitate a wide range of terrorist activities, including incitement to violent extremism conducive to terrorism, recruitment, training, planning, networking, securing logistical support, acquiring weapons and their components, fundraising, and conducting terrorist operations. The use of new and emerging technologies for terrorist purposes has become pervasive and poses a transnational and global threat.

With the exponential growth in the exploitation of online spaces by terrorists, violent extremists, and their support networks, Member States and technical sector companies are enhancing their legal, policy, and operational abilities to identify and moderate terrorist content, as well as take steps against the actors responsible for producing and spreading it. Large social media companies actively remove terrorist and violent extremist content located on their platforms, while many smaller platforms also moderate content to some extent, depending on their capacity. Member States are actively expanding their capacity to collect digital evidence, open-source electronic

intelligence, and other information on terrorist networks for use in criminal and terrorism-related investigations and prosecutions.

As terrorist use of ICT has become more sophisticated, Governments and the tech sector have struggled to address the dissemination of terrorist content online and effectively counter terrorist narratives. The challenges faced have been further complicated by the diversity of platforms and communication channels available, as well as the use of terrorist-specific online publications and videos, the growing abuse of gaming platforms and related chat rooms, the (albeit infrequent) live-streaming of attacks, and the use of unmoderated live audio feeds to spread terrorist propaganda. The development of virtual reality technologies and the metaverse may yet pose further challenges.

Terrorists and violent extremists are additionally becoming highly adaptive in their efforts to avoid content moderation and are decentralizing their activities across a range of less-known and less-monitored platforms, to include turning to self-operated websites. They are also making use of tools such as anonymizers and virtual private networks (VPNs) to hide their identities, IP addresses, and locations. The profusion of methods and applications used by terrorists to ensure that their propaganda remains visible and

activities in the cyber domain, to include potential normative and policy solutions, operational actions, and guidance relating to respect for, and compliance with, international human rights law, fundamental freedoms, and gender considerations.

Format

The two technical sessions on 30 September and 3 October are open to Member States and other relevant operational partners to include United Nations organizations, international and regional organizations, the private technology sector, academia, and civil society organizations. The meetings will be conducted in English and held in virtual format only (via Microsoft Teams).

The duration of each technical session is three and a half hours, including time for moderated presentations by invited speakers, panel discussions, statements by registered participants (by prior-request during registration), and moderated Q&A with attending registered participants.

Invited speakers are requested to submit presentations and statements in writing within four business days in advance of the relevant session(s). Participants requesting to make statements during the technical sessions (time permitting) are likewise requested