Counter-Terrorism Committee Executive Directorate (CTED)

Special Meeting of the Counter-Terrorism Committee on countering the use of new and emerging technologies for terrorist purposes

Mumbai and New Delhi, India, 28-29 October 2022

Concept Note

A. Introduction

1. With the growing prevalence of technology and the rapid rise in digitization, addressing the use of new and emerging technologies for both terrorist purposes and for countering terrorism is an issue of increasing concern for Member States, policymakers and researchers. The Security Council has given focus to this issue in a number of counter-terrorism related resolutions, most recently its resolution 2617 (2021), which specifically refers to "emerging technologies".

2. Mindful of the increasing threat posed by misuse of new and emerging technologies, as well as the many positive uses of technologies for countering terrorism, the Counter-Terrorism Committee proposes to hold a Special Meeting open to all Member States and including the participation of relevant operational partners, including United Nations organizations, international and regional organizations, civil society organizations (CSOs), private-sector entities, and members of the Global Research Network (GRN) of the Counter-Terrorism Committee Executive Directorate (CTED).

3. The Special Meeting would focus specifically on three significant areas in which emerging technologies are experiencing rapid development, growing use by Member States (including for security and counter-terrorism purposes), and an increasing threat of abuse for terrorism purposes: (i) use of the Internet and social media; (ii) new payment technologies and fundraising methods; and (iii) unmanned aerial systems (UAS).

4. The objectives of the proposed Special Meeting would be: (i) to provide an overview of the ways in which Member States are deploying new and emerging technological developments to prevent and counter terrorist narratives and acts and to bring terrorists to justice, consistent with their human rights obligations; (ii) to update Member States on recent developments and the latest evidence-based research regarding the threats posed by terrorist use of new and emerging technologies; (iii) to identify continuing challenges; and (iv) to share existing good practices in legislative, policy, and regulatory responses, industry activities, public-private partnerships, and compliance with international human rights law.

5. The proposed Special Meeting would also provide an opportunity to reflect on the work of the Committee, CTED, and their operational partners on countering the use of new and emerging technologies for terrorist purposes while respecting human rights and fundamental freedoms, taking into account Member State compliance with applicable obligations under international law, and taking into consideration specific gender aspects relating to digitalization and technology. It would also facilitate the review of steps taken by Member States to institute appropriate legal, policy, and operational measures and efforts to develop and utilize public-private partnerships;

self-regulation, good "safety-by-design" practices, and other measures implemented by the private sector; and initiatives taken by civil society and other relevant actors. The discussions would additionally focus on ways in which States and other relevant actors can strengthen their engagement and cooperation in countering the use of new and emerging technologies by terrorists and their financiers.

B. Background

6. New and emerging technologies – particularly information and communications technologies (ICT) such as the Internet, social media platforms, and financial technologies – are mostly used for social communications, digital commerce, and informational purposes by the general population. They have also 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 terrorism and violent extremism conducive to terrorism, recruitment, training, planning, networking, securing logistical support, acquiring weapons and their components, fundraising, and conducting terrorist operations.

7. As terrorist use of the Internet and social media platforms 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.

8. Increasingly, financial services used by terrorists take place online and are facilitated by communication technologies. Terrorists move or store funds through the use of digital marketplaces and wallets, online payment platforms and applications, mobile-payments or virtual currencies. There is also an increased risk of the abuse of the Internet by terrorist organizations for fundraising through crowdfunding, merchandise sales, donation appeals through social media platforms, and other methods. At the same time, innovations in financial technologies, products and services offer significant economic opportunities and provide effective tools to respond to emerging threats.

9. Further issues of concern are the potential use of dual use technologies by terrorists and the exploitation of emerging technologies (including 3-D printing, robotics, artificial intelligence (AI) and machine learning, UAS, and synthetic biology) for various terrorist purposes. As critical infrastructures become increasingly reliant on ICT, access to advanced malicious software by terrorist groups could lead to new kinds of cyberattacks. Terrorists have already demonstrated the ability to use 3-D printing to make firearms and have also acquired the capacity to weaponize UAS to execute attacks. They are capable of constructing sophisticated devices from scratch and modifying commercial UAS for malicious purposes, as highlighted in CTED's Trends Alert of

May 2019. Developments in these and other new technologies could be utilized by terrorists to expand the range and lethality of their attacks.

10. The Security Council has focused attention on countering the exploitation of ICT and related technologies for terrorist purposes for over 20 years and has adopted 15 counter-terrorism related resolutions, including 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). The Council has also adopted 4 policy documents on the matter, consisting of the Madrid Guiding Principles (S/2015/939), 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). Issues relating to new and emerging technologies, including ICT, are also addressed in the Counter-Terrorism Committee's updated Global Survey of the implementation of Security Council resolution 1373 (2001) and other relevant resolutions by Member States (S/2021/972) and the "Technical Guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions" (S/2019/998).

11. Acting in accordance with the relevant Council resolutions, the Counter-Terrorism Committee and CTED continue to support Member States in their efforts to counter and prevent the use of new technologies for terrorist purposes through enhancing their legislative frameworks, and adopting relevant law enforcement, security, and financial measures, among other steps. The Counter-Terrorism Committee and CTED promote the development of public-private partnerships and actively facilitate the provision of technical assistance to address the use of new and emerging technologies to commit terrorist acts. The Security Council has repeatedly called on States to ensure that any measures taken to combat terrorism comply with all their obligations under international law, including international human rights law, international humanitarian law, and refugee law, as applicable. It is also essential that the gendered impacts of new technologies in the fight against terrorism are recognized and taken into consideration in order to avoid bias and ensure gender-responsiveness.

12. The Counter-Terrorism Committee and CTED also support Member States in their efforts to harness the vast potential of new and emerging technologies for good. Many innovative technologies such as artificial intelligence, advanced analytics, facial recognition, and UAS are being used by Member States, United Nations entities, international and regional organizations, CSOs, and other relevant actors to gather, use and share information necessary to detect and prevent acts of terrorism, bring perpetrators to justice, and to support victims of terrorism.

13. Although much has been accomplished in the areas of preventing and countering the use of emerging technologies for terrorist purposes, significant shortfalls remain. CTED's assessments show that States continue to face challenges in a number of relevant areas, including countering terrorist narratives; moderating online content; tracing and identifying terrorist crimes planned and/or committed online, to include terrorism financing and the procurement of weapons, UAS, and their components through online means. Many also still lack sufficient legal and regulatory frameworks, data management and processing protocols, risk and impact assessment practices, and rigorous access controls and records for technology-based systems, including those based on AI.

C. Format of Special Meeting

14. It is proposed that the Special Meeting and associated events take place over two days in Mumbai and New Delhi, India, as in-person events, with virtual participation by speakers, as necessary, in accordance with the prevailing arrangements for United Nations conferences. From the CTC member states, the Permanent Representatives and experts will be invited to participate in-person. It is further proposed that:

- Day 1 – 28 October 2022 – in Mumbai – consist of a "soft" opening of the Special Meeting and related events.
- Day 2 – 29 October 2022 – in New Delhi – consist of the Special Meeting of the Counter-Terrorism Committee, open to all Member States.

15. The opening plenary session of the Special Meeting of the Counter-Terrorism Committee on 29 October 2022 in New Delhi, India, is proposed to begin with a minute's silence in memory and honour of the victims of terrorism, their families, and survivors of terrorism. This would be followed by addresses by the Secretary-General of the United Nations *[TBC]*, the Minister of External Affairs of India *[TBC]*, the Chair of the Counter-Terrorism Committee, the Under-Secretary-General of the UN Office of Counter-Terrorism (UNOCT), and the Executive Director of CTED, as well as other possible speakers. The meeting would continue with thematic briefings and discussions on the three topics of the meeting, interventions and questions from CTC members, and the adoption of an outcome document before closing the Special Meeting. Non-Committee Member States will be requested to submit their statements in writing. The Vice-Chair(s) of the Committee would serve as moderator(s) during the Special Meeting *[TBC]*.

16. Detailed agendas for the Special Meeting and associated events spanning 28-29 October in Mumbai and New Delhi will be provided in due course.

17. The Special Meeting will be preceded by a series of virtual and/or in-person CTED-led technical meetings *[format, location, and timing TBC]* on the three themes involving, as appropriate, subject matter experts from Member States, United Nations offices and international and regional organization, tech industry and other private-sector entities, civil society organizations, and members of the GRN. The outcomes of these meetings would inform the presentations to be delivered and the discussions to be held during the Special Meeting.

18. The Special Meeting would be conducted in the six official languages of the United Nations (pursuant to the rules for interpretation and availability at the time of the Special Meeting).

E. Participants

19. The Special Meeting on 28 October 2022 in Mumbai, India and on 29 October 2022 in New Delhi, India, would be open to the wider United Nations membership and other relevant stakeholders (including partner United Nations counter-terrorism bodies; representatives of international, regional and subregional organizations; members of the GRN; CSOs; private-sector entities, and the media.

F. Outcome

20. The Committee would issue an outcome document or "Delhi Declaration on addressing the threat of use of new and emerging technologies for terrorist purposes" at the conclusion of the Special Meeting. It is proposed that this takes the form of a negotiated outcome document with annexes as derived from discussions held during the CTED-led technical meetings *[TBC]*, highlighting progress achieved in implementing Security Council resolutions, remaining gaps and ways to address them, reaffirming the commitment of Committee members to the fight against terrorism, and setting out a broad vision for the future actions and orientation of the Committee and CTED. Upon adoption, this outcome document would be made publicly available.

G. Communications

21. A page on the Committee's website would be dedicated to the event, in accordance with the usual procedure. CTED would circulate an annotated agenda, meeting documentation, and other logistical information, which would also be posted on the Committee's website. The Committee may also wish to consider issuing, inter alia, a Chair's statement or press release and/or holding a press conference in advance of and/or following the Special Meeting.

22. It is proposed that an option be provided for the Special Meeting on 28-29 October 2022 to be broadcasted live and/or recorded in order that participants may observe the proceedings online.