



2023 Counter-Terrorism Week SIDE EVENTS

19–23 JUNE 2023

UNITED NATIONS HEADQUARTERS • NEW YORK



PERMANENT MISSION OF THE
UNITED ARAB EMIRATES
TO THE UNITED NATIONS
NEW YORK

Preventing and Countering the Use of New and Emerging Technologies for Terrorist Purposes: Way Forward for a Holistic Multilateral Response

22 June 2023; 13:15-14:30 EST; ECOSOC Chamber; (In-Person)

Concept Note

Introduction

New and emerging technologies —particularly information and communications technologies (ICT) such as the Internet, including social media platforms and online financial tools— are primarily used for social communications, digital commerce, and informational purposes by the general population. Additionally, the digital transformation has exponential benefits as a development accelerator for countries. However, in recent times, they have also been exploited by terrorists and terrorist groups such as Da’esh, Al-Qaida, their affiliated groups, undertakings, and entities; and other terrorist organizations for organizing a wide range of terrorist activities, including incitement to terrorism, radicalization, recruitment, training, acquiring weapons and their components, fund-raising, and planning and conducting terrorist attacks. The development of appropriate solutions must be considered as the use of new and emerging technologies for terrorist purposes has become a pervasive challenge and poses a transnational and global threat.

2. The issue of the use of new and emerging technologies for terrorist purposes requires greater attention of the Member States, the United Nations Counter-Terrorism entities, and other relevant stakeholders. Not only is there a need to evaluate, and understand the extent and gravity of the threat; but also to explore ways to strengthen the resilience and capacity of Member States to address and

2023 COUNTER-TERRORISM WEEK

www.un.org/counterterrorism/CTweek2023-SE
[@UN_OCT](https://twitter.com/UN_OCT) | [#CTWeek](https://twitter.com/CTWeek) | [#UNiteToCounterTerrorism](https://twitter.com/UNiteToCounterTerrorism)

mitigate this threat. To this end, in the past year, several initiatives have been taken by the United Nations system, among these the Special Meeting of the Counter-Terrorism Committee (CTC) of the Security Council on ‘Countering the use of new and emerging technologies for terrorist purposes’ held in Mumbai and New Delhi, India from 28-29 October 2022. In advance of the Special Meeting, the Counter-Terrorism Committee Executive Directorate (CTED) had organized a series of technical meetings in September and October 2022 on issues relating to Information and Communication Technologies (ICT), countering the financing of terrorism (CFT), and the global misuse of unmanned aerial systems (UAS) by terrorists to gather a broad range of views and good practices to inform the proceedings of the Special Meeting. The members of the Committee formally adopted the “Delhi Declaration” as the primary output of the Special Meeting.¹

3. The Delhi Declaration recognizes a number of key concerns and tenets unanimously agreed by the Committee and provides guidance to Member States and stakeholders in countering the use of new and emerging technologies for terrorist purposes. It also sets forth areas of future work for the CTC and CTED, including the development of recommendations on the three themes as well as a set of non-binding guiding principles to assist Member States to implement the Delhi Declaration in a holistic manner. Importantly, these documents will also contain good practices on the opportunities offered by the same set of technologies to counter this threat, consistent with applicable obligations under international law, including international human rights law, international humanitarian law, and international refugee law.

4. The digital transformation is exemplified by governments transferring its functions to the cyberspace. For example, the long-term vision of the United Arab Emirates (UAE) in that regard includes the evolution from e-government to cloud and smart government and finally, to Artificial Intelligence (AI)based government, while being protected by an implementation plan utilizing new and emerging technologies.

5. Against this backdrop, the Permanent Missions of India and the UAE to the UN, are organizing a sideevent on these aspects of the counter-terrorism agenda on the margins of the Counter Terrorism Week 2023. India chaired the CTC in 2022, and the UAE is the current Chair. The participants of the event— which include Member States, the UN system, the private sector, and civil society—will raise awareness about the continued urgency to address these threats, including through the implementation of the Delhi Declaration. The side event will further explore how Member States can promote safe and secure technological advancements, including the digital transformation, through strategic outreach to and voluntary cooperation with the private sector and civil society, while preventing and countering the acquisition and use of such technology by terrorist groups and individual terrorist actors, including through possible regulatory measures.

¹ The text of the Delhi Declaration in all six official UN languages can be found [here](#).

Background and Context

6. The growing exploitation of ICT by terrorists and terrorist groups to spread their propaganda has left Governments and the tech industry struggling to effectively address this challenge. The diversity of platforms and communication channels available, the use of terrorist-owned websites, and the range of circumvention techniques that terrorists and their supporters use to avoid content moderation and the development of counter-narratives even more complex. Exponential leaps in the development of AI raise new risks for how terrorists could exploit ICTs to advance their ability to operate and avoid detection. Advancements in augmented and virtual reality technologies are likely to pose further threats in this regard.

7. The continued increase in the use of virtual assets and new methods for moving money can be abused for terrorism-financing purposes. These risks are compounded by the increase in the number and types of virtual asset service providers.

8. Further issues of concern are the potential misuse of dual use technologies by terrorist groups to expand the range and lethality of their attacks. AI and machine-learning capabilities are growing at an unprecedented rate and their malicious use could pose threats to digital and physical security. And, as critical infrastructures become increasingly reliant on ICT, access to advanced malicious software by terrorist groups can lead to new kinds of cyberattacks risking the security of entire populations and systems. In recent years, government databases have been hacked and there has been a rise in blackmail threatening sensitive data of individuals stored online, and attempts to disrupt the financial and health sectors. Avenues to address this threat include strengthening public-private partnerships, intelligence sharing, and investing in capacity-building of relevant state institutions.

9. Another example is the possibilities of modifications of UAS to expand the range and lethality of attacks as well as intelligence, surveillance, and reconnaissance conducted by terrorist groups. They 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.

10. The UN System has paid attention to address some of the issues. The Security Council over the past 20 years has adopted fifteen counter-terrorism related resolutions, including resolutions 2462 (2019) and 2617 (2021)² as well as Presidential Statements and other policy documents.³ It also addressed new

² Additionally, these include 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), and 2396 (2017).

³ These consist of the Madrid Guiding Principles (S/2015/939), the 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 (S/2018/1177).

technologies in a number of counter-terrorism resolutions focused on law enforcement and border control, aviation security, and the protection of critical infrastructure and “soft” targets, including specific references to the threats posed by terrorist use of UAS in resolutions 2370 (2017) and 2617 (2021). The Office of Counter-Terrorism (UNOCT) initiated global capacity-building programmes such as “Detecting, Preventing and Countering the Financing of Terrorism (CFT Programme)” in 2020; the Global Counterterrorism Programme on Cybersecurity and New Technologies also in 2020, and the Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (the AROS Programme) in 2021.

Objectives

11.11.

- a) Discuss how to effectively implement the Delhi Declaration, including in the context of the ongoing work of the CTC and CTED on countering the use of new and emerging technologies for terrorist purposes;
- b) Highlight steps taken by Member States, the private sector, civil society, and other key partners to prevent and counter terrorist and related threats while respecting applicable international law, including international human rights law, international humanitarian law, and international refugee law;
- c) Explore how Member States can promote safe and secure technological advancements, including the digital transformation, through strategic outreach to and voluntary cooperation with the private sector and civil society, while preventing and countering the acquisition and use of such technology by terrorist groups and individual terrorist actors, including through possible regulatory measures;
- d) Discuss capacity building needs and opportunities for One UN global and regional programming solutions, including a whole-of-society approach.

Agenda

Duration: 75 minutes	Date: 22.06.2023 Time: 13:15-14:30 EST Location: ECOSOC Chamber
6 minutes	Welcome remarks by Amb. Ms Ruchira Kamboj, the Permanent Representative of India to the UN
6 minutes	Welcome remarks by H.E. Dr. Mohamed Al Kuwaiti, Head of Cybersecurity, UAE
5 minutes	Special Remarks by Raffi Gregorian, Director and Deputy to the Under-Secretary-General, United Nations Office of Counter-Terrorism (UNOCT)
5 Minutes	Special Remarks by Mr. David Scharia, Director, Chief of Branch, CTED
	Panel Discussion
6 minutes	Presentation by CTED (expert)
6 minutes	Presentation by Mr Sameer Patil, Senior Fellow, Observer Research Foundation, India
6 minutes	Presentation by H.E. Ahmed AlQasimi, Executive Director - Hedayah (International Center of Excellence for Countering extremism and Violent extremism)
6 minutes	Presentation by Mr Priyank Mathur, Founder and CEO of Mythos Labs
6 minutes	Presentation by Karthik Nandakumar, Associate Professor, Computer Vision, Mohamed Bin Zayed University of AI, Abu Dhabi, UAE
6 minutes	Presentation by Adam Hadley, Tech Against Terrorism
15 minutes	Q&A (from the floor)
2 minutes	Concluding Remarks by the Permanent Mission of India (On behalf of India and UAE)

For any questions regarding this event, kindly contact Mr. Rajesh Parihar, Counsellor, Permanent Mission of India to the UN, polad.newyorkpmi@mea.gov.in, Ahmed AlMahmoud, Counsellor, Permanent Mission of the UAE, ct@uaeun.org and Mr. David Scharia, Chief of Branch, CTED, scharia@un.org.