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

29, October 2022, 9.00 a.m. EDT

#### Opening remarks of

### Mr. Weixiong Chen, Acting Executive Director, CTED

Your Excellency Mr./Ms. xxxx [Gov. of India official], Excellencies, distinguished participants,

I wish to sincerely thank the Government of India for hosting th special meeting.

I also wish to commend India for its leadership role and significant contribution as a member of the Security Council and as Chair of the Counter-Terrorism Committee.

The special meeting comes at the right time and for the right topics.

Twenty years ago, the Security Council decided that all States should deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe haven.

However, we have witnessed a shift in the nature of terrorist attacks over the years.

Today, terrorists consider the digital sphere as a safe haven.

Terrorists are skilled at using new platforms and systems for many purposes, including to incite, recruit, finance, plan and execute terrorist attacks.

Terrorists are also increasingly exploiting chat, gaming, and audio-visual platforms.

They understand cyber security and take measures to shield their illegal activities.

The dark web serves as a marketplace for materials, weapons and fake documents.

In this context, how we develop and deploy technology will determine how effectively we shall be able to tackle new and emerging threats to international peace and security caused by terrorist acts.

Member States are increasingly deploying technological developments in areas such as artificial intelligence (AI) and big data to prevent terrorist acts and to bring terrorists to justice.

Both public and private sectors are experimenting with new technologies to improve the traceability of financial transactions.

And small and large technology companies are investing in, and deploying, AI to detect terrorist content on their platforms.

The CTED-led initiative Tech against Terrorism has also identified over 200 platforms actively used by terrorist groups.

Unmanned aircraft systems are one of those technologies.

As the UAS industry continues to innovate, it is lowering into the aerial sphere.

How could the international community respond most effectively?

First, our understanding, capabilities and responses must keep pace with the identified threats.

CTED remains committed to stay ahead of the technology curve. We have and will continue to:

-Support the Security Council and the Counter-Terrorism Committee in addressing emerging ICT challenges in the context of maintaining international peace and security and in counter-terrorism;

-Strengthen our own assessment work, analysis and technical expertise and guidance.

The Launch of the CTED-UNODC

in 2019 is one such example.

-Enhance partnership with other UN entities and international and regional organizations and arrangements in raising the awareness of the threat by the misuse of ICT for terrorism purposes, and facilitate the delivery of technical assistance to States in need;

-Contribute to the innovative initiatives such as the Global Internet Forum to Counter Terrorism (GIFCT) and Tech Against Terrorism, as well as the work the Global Counter-Terrorism Forum (GCTF),

Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems.

Second, regulations and innovation are complementary and mutually reinforcing.

As social media, UAS and new payment technologies continue their rapid development, our legislation and regulations will need to keep pace.

*Third*, we must continue to identify, share and build expertise and technical resources and capacity.

Law enforcement agencies have made great strides in their ability to investigate, detect and disrupt the use of new and emerging technologies for terrorist purposes.

Further targeted training and capacity-building will be required to ensure that criminal justice officials can effectively investigate, and, as appropriate, prosecute, and adjudicate technology-related terrorist crimes.

Fourth, a multi