

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, 28-30 October 2022

Remarks by Marco Teixeira, UNODC Regional Representative for South Asia

Excellencies, Distinguished Delegates

On behalf of UNODC, thank you for the invitation to participate in this important meeting which focuses on an issue of critical importance to addressing modern terrorism. As we have heard from our expert panellists, new technologies are increasingly exploited by terrorist groups to fund, plan, and even engage in terrorist attacks. Terrorists are utilizing the Internet for radicalization, recruitment, financing, and planning using new methods and platforms to hide their activity. It is therefore essential that the international community works together to respond to these evolving threats.

National governments need the technical tools and data sources to effectively assess national risks, respond to evolving threats, and allocate resources using a risk-based approach. This requires identifying and resolving blockages in sharing information at the national and international levels, putting in place monitoring measures, and harnessing the potential of new technologies to compare bulk datasets.

There is a risk however that these new technologies could be abused, infringing on the rights to privacy and freedom of speech. We must therefore ensure that robust oversight mechanisms and legal frameworks are carefully conceived and implemented.

We must benefit from lessons learned in our efforts to address terrorism - that human rights violations committed as part of terrorism responses are counter-productive, further fuelling violent extremism. We must continue to support space for legitimate expression of opinions as part of non-violent dissent and to protect the right to privacy as a key element in building and maintaining trust in a society.

When States put in place measures to deal with this content including electronic evidence and data collection, any infringement on the right to privacy must comply with the principles of necessity, proportionality, and non-discrimination, as detailed under the International Covenant on Civil and Political Rights.

While the responsibility for countering the terrorist use of these new technologies ultimately lies with Member States, the United Nations, Civil Society Organizations, and the private sector can play a key role in these efforts.

The establishment of public-private partnerships would be beneficial to break down communication barriers and facilitate joint training programmes, building understanding and supporting the development of harmonized practices. The United Nations is able to play an important role in facilitating these exchanges.

The UN can support States by developing operational solutions, guidance materials and tools to help countries navigate these complex issues, to work across various legal systems, and foster inter-operability. UNODC has already been working closely with CTED and other UN partners to support law enforcement and judicial authorities with the use and handling of electronic evidence across borders, the adoption of passenger data frameworks, including Advanced Passenger Information (API) and Passenger Name Record (PNR), and data protection guidance. However, as technologies evolve there continues to be a need to develop new guidance which keeps pace with these changes.

Furthermore, the United Nations can provide technical and capacity building support to Member States in adapting this guidance to their specific needs legal framework and context ensuring that:

- legislation and policies take into account human rights considerations and put in place oversight mechanisms;
- intelligence and criminal justice officials have the knowledge, skills, and equipment to counter terrorist misuse of these technologies;
- countries can work together across borders to share information and evidence; and
- governments and private sectors entities have strengthened coordination to detect and prevent terrorism acts.

UNODC, as a technical assistance provider, is already working with States to help put in place these measures but given the complexity and quickly evolving nature of terrorist use of new technologies, much more needs to be done.

UNODC looks forward to continuing and expanding its work to support Member States to stay one step ahead of this complex and evolving threat – by better responding to the new ways in which terrorists are using the online space and supporting criminal justice officials to utilize new technologies to detect and counter terrorist activity while respecting human rights.