United Nations
Interregional Crime and Justice
Research Institute

Statement of the Director of the United Nations Interregional Crime and Justice Research Institute (UNICRI)

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

Thematic Briefings I:
Countering Terrorist Exploitation of Information and Communication Technologies (ICTs)

Mumbai, India
28 October 2022

Excellencies, Ladies and Gentlemen,

It is a pleasure to join you today on behalf of the United Nations Interregional Crime and Justice Research Institute (UNICRI). I would like to express my appreciation to H.E. Ms. Ruchira Kamboj, Permanent Representative of India to the United Nations and Chair of the Counter-Terrorism Committee (CTC), for convening this session, and to the Counter-Terrorism Executive Directorate (CTED) for supporting it. I also extend my deep appreciation to our gracious Host – the Government of India – for the wonderful welcome in Mumbai and here in New Delhi.

Ladies and gentlemen,

As the United Nations research and training institute for criminal justice and crime prevention, UNICRI closely follows criminal justice trends and developments. Related to information and communication technologies (ICT), UNICRI's work focuses on identifying and analyzing the impact of technological changes on trends and patterns in crime, including terrorism, and exploring the potential opportunities technology presents for law enforcement and counter-terrorism actors.

In 2015, we established our Centre for Artificial Intelligence (AI) in The Hague, which strives to analyze precisely these challenges and opportunities in the context of AI. Together with the United Nations Office of Counter-Terrorism (UNOCT), we have looked extensively at trends and developments in cybercrime, extrapolating potential malicious uses of AI for terrorist purposes – from the use of AI to enhance cyber-attack capabilities to targeted drone swarm attacks employing facial recognition technology.

In our report, *Algorithms and Terrorism*, we observe that terrorist organizations have tended to use various forms of 'low-tech terrorism', such as firearms and vehicles, but terrorists' use of emerging technologies such as AI must not be discounted. We also identify an important distinction between the 'use' and 'abuse' of AI: 'abuse' concerns attacks directed to the functionality of AI. As AI is increasingly integrated into how our world works, we must remain conscious of potential new threat scenarios in which AI systems themselves become targets. Our report concludes that the current capability of

groups such as Da'esh to effectively deploy AI is unlikely, but as AI becomes more widespread and the barriers to entry lower, the risks increase.

In this context, the crime-as-a-service model, through which terrorist groups and individuals seek services offered by adept cyber criminals on the dark web, is relevant. This model may enable terrorists to launch more technologically advanced cyber-attacks. I am pleased to share that UNICRI is launching an exercise to analyze examples of the crime-as-a-service model in the context of cyber-enabled terrorism, with a view to developing case studies that can support cybercrime investigators.

UNICRI has also been monitoring the impact of technology in the area of Weapons of Mass Destruction (WMD) terrorism. In 2021, in cooperation with UNOCT, UNICRI published the report *"Advances in Science and Technology to Combat Weapons of Mass Destruction Terrorism"*. This report elaborates possible risks associated with the malicious use of science and technology to develop and deploy WMD. It also identifies scientific and technological solutions to prevent and combat WMD terrorism.

Another area of growing interest for UNICRI is virtual reality, social gaming platforms, and the concept popularly referred to as the 'metaverse'. UNICRI is launching new research on this important cutting-edge topic, which aims to elaborate a model for what crime looks like in the virtual environment of the metaverse. One key focus will be the potential misuse of the metaverse by terrorists to spread propaganda, communicate and fund terrorist operations, and coordinate attacks both on- and off- line.

The misuse of ICT to generate and spread conspiracy theories and disinformation is another priority area because these acts are often linked to hatred and racism, xenophobia, islamophobia, and anti-Semitism. In the early months of the COVID-19 pandemic, UNICRI conducted a study, *"Stop the Virus of Disinformation"*, on the malicious use of social media. We identified examples by both Da'esh and Al Qaida. Disinformation and conspiracy theories persist and are increasingly problematic in many domains. For example, we will be releasing soon a new handbook for practitioners of chemical, biological, radiological and nuclear risk mitigation to debunk maliciously generated false information by non-State actors, including terrorists.

Ladies and gentlemen,

We live in the technological age and the possible use of new and emerging technologies for terrorist purposes must be accepted as a reality. While many of the technologies we are discussing during this Special Session are still ‘new and emerging’, it is vital that we strive to stay ahead of the curve. We already need to understand the potential misuses of these technologies and identify the gaps in legal frameworks or governance systems, so that we can better facilitate investigations and prosecutions to hold criminals and terrorists accountable for malicious use of these technologies.

At UNICRI we stand ready to share our expertise and to support the CTC to build such knowledge and understanding of the misuse of technology for terrorist purposes.

Thank you.