Dear esteemed delegates, distinguished participants, good morning. Thank you very much for inviting me to speak on behalf of the UN Counter-Terrorism Committee Executive Directorate (CTED). My name is Eunjung Irene Oh, and I’m an Associate Expert in the Information and Communications Technology Team in CTED. I’m here to present an overview of the work and initiatives of CTED in countering terrorist exploitation of new and emerging technologies, with a focus on its role as a first point of entry for capacity-building for Member States in the area of ICTs and terrorism.

CTED is a special political mission dedicated to supporting the Counter-Terrorism Committee and Member States in their implementation of Security Council resolutions on counter-terrorism. The three core functions of CTED are (1) assessments (we do these through country visits, ongoing dialogue with Member States, and desk reviews of strategies, legislation, and polices, and other materials shared by States), (2) research and analysis (we identify and analyse new trends and developments and produce trends alerts, analytical briefs, and other reports on counter-terrorism), and (3) facilitating technical assistance to Member States, in close cooperation with our partners.

As a special political mission in the Security Council, CTED is at the core of understanding, identifying, and facilitating various technical assistance and capacity-building needs in relation to new and emerging technologies and their use by terrorists. We do this through our active participation in the Global Counter-Terrorism Coordination Compact, co-leading five working groups, and through strong working relationships with entities providing capacity-building to Member States, as well as with partnerships with civil society, private sector, and academia. We also leverage various tools, such as recommendations adopted by the Committee and our counter-terrorism database, in the
development of capacity-building programmes and national action plans that are tailored to meet the unique need of individual Member States.

In the realm of ICT, CTED identified critical technical assistance gaps in combating terrorist and violent extremist activities online and made a number of recommendations for Member States to address those challenges. For instance, we identified that Member States face challenges in obtaining digital evidence stored by service providers in cross-border jurisdictions. To bridge this gap, we recommended comprehensive training programmes for law enforcement and criminal justice practitioners working with digital evidence, including how to extract and perform forensic analysis of evidence, methods for utilizing digital evidence in trials, and the processes surrounding the admissibility of digital evidence in court, as well as training in international and domestic human rights laws, especially with regard to privacy, freedom of expression, and data protection. We also co-developed Practical Guide for Requesting Electronic Evidence Across Borders with the United Nations Office on Drugs and Crime and the International Association of Prosecutors to enhance the capacity of investigators and prosecutors worldwide. We have also identified the need for technical assistance on how to identify and investigate terrorism-financing crimes committed online using virtual currencies, new payment methods, and cyber-based fundraising techniques, for example. Further information on our gaps analysis is available to our partner agencies, and we are happy to provide further details on the various areas we have identified.

CTED also promotes public-private partnerships as an essential element in countering terrorist use of ICTs and other new and emerging technologies. States benefit significantly from the technological expertise available in the tech sector; Member States’ sharing of threat information can also benefit the private sector by expanding its threat awareness and strengthening its technical capabilities to counter threats. Meanwhile, close cooperation with civil society actors can help to ensure that online investigations and content-moderation efforts are proportional, fully human rights-compliant, and gender-
sensitive. In addition, academic institutions and the evidence-based research that they produce play an important role in identifying emerging issues and helping to design effective capacity-building measures. CTED has been at the forefront of strengthening public-private partnerships, as evidenced by the launch of Tech Against Terrorism – a nongovernmental organization that supports the global tech industry in its efforts to tackle terrorist exploitation of their technologies – and the establishment of CTED’s Global Research Network – which brings together more than 100 leading research institutions from across the globe. CTED has also maintained a strong partnership with the Global Internet Forum to Counter Terrorism (GIFCT), an industry-led NGO designed to prevent terrorists and violent extremists from exploiting digital platforms.

With strong partnerships as well as technical and regional expertise in counter-terrorism, CTED will continue to play a critical role in identifying the technical assistance needs of Member States in counter-terrorism and support the capacity-building programmes of our partners, such as the United Nations Office of Counter-Terrorism, the United Nations Office on Drugs and Crime, INTERPOL, the European Union, and the Organization for Security and Cooperation in Europe. We will also continue to engage with our civil society and private sector partners to identify innovative and collaborative ways to tackle the abuse of ICTs in a holistic and inclusive manner. Thank you so much.