UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

Cybersecurity and New Technologies

Global Counter-Terrorism Programme on Cybersecurity and New Technologies

March 2020 – December 2024

The Cybersecurity and New Technologies Programme provides capacity building support to Member States, international and regional organizations for developing and implementing effective responses to challenges and opportunities that the Internet and other Information and Communications Technologies provide in countering terrorism.

The programme is funded by the European Union, Germany, Japan, the Republic of Korea, the Kingdom of Saudi Arabia, and the United Arab Emirates.

Objectives

- Develop knowledge and raise awareness of challenges and opportunities related to new technologies in countering terrorism.
- Enhance skills and capacities required to develop and implement effective national counter-terrorism policy responses to the challenges and opportunities of new technologies.
- Enhance skills and capacities required to protect critical infrastructures against terrorist cyber-attacks
- Enhance criminal justice capacities to counter and investigate terrorist use of new technologies

Achievements

150+ Member States benefited

4000+ officials acquired new skills and knowledge on:

12 new knowledge products

artificial intelligence, cybersecurity, online investigations, dark web investigations, cryptocurrencies investigations and digital forensics.

Human Rights and Gender Mainstreaming

Human rights and gender mainstreaming is reinforced through all programme outcomes and outputs. Each outcome has a human rights and gender mainstreaming compliance monitoring plan to assess and measure mainstreaming effectiveness. All capacity building activities integrate human rights focused training, ensuring that the human rights framework is applied to digital space, and make a significant contribution to gender equality, empowerment of women and addressing their specific needs.

Focal Point

Ms. Akvile Giniotiene, Programme Manager: akvile.giniotiene@un.org

Why

During the eighth review of the of the United Nations Global Counter-Terrorism Strategy Member States expressed their deep concern "by the use of the Internet and other information and communications technologies, including social media platforms, for terrorist purposes, including the continued spread of terrorist content," and encouraged Member States "to work together and with other relevant stakeholders, including academia, the private sector and civil society, to ensure that terrorists do not find safe haven online, while promoting an open, interoperable, reliable and secure Internet that fosters efficiency, innovation, communication and economic prosperity, while respecting international law, including international human rights law, including the right to freedom of expression." The Office of Counter-Terrorism and other relevant Global Counter-Terrorism Coordination Compact entities were requested to "jointly support innovative measures and approaches to build the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism.

Geographical scope

Global

Substantive programme partners

UNICRI, INTERPOL, OSCE, CTED, DOS, DPO, DPPA, ICAO, OICT, UNODC, ITU