Capacity building under the UNOCT/UNCCT Global Counter-Terrorism Programme on Cybersecurity and New Technologies

23 May 2023 | OEWG Informal Roundtable Discussion on Capacity Building
New York
UNOCT: Mandate and Objectives

5 main Functions

- Improve visibility, advocacy, and resource mobilization for UN counter-terrorism efforts
- Provide leadership on the General Assembly counter-terrorism mandates entrusted to the SG from across the UN system
- Enhance coordination and coherence across the 45 Global Compact entities to ensure balanced implementation of the four pillars of the Strategy
- Strengthen the delivery of UN counter-terrorism capacity-building assistance to Member States
- Ensure that due priority is given to counter-terrorism across the UN system and that the important work on PVE is firmly rooted in the strategy
- Improve visibility, advocacy, and resource mobilization for UN counter-terrorism efforts
Global Counter-Terrorism Programme on Cybersecurity and New Technologies

Strategic United Nations commitment to the world without terrorism

Member States have primary responsibility for combatting terrorism

UNCCT/UNOCT Global Programme on Cybersecurity and New Technologies

- Knowledge development and awareness raising
- Capacity building for policy development
- Capacity building for preparedness, resilience, mitigation and response
- Capacity building for investigations
Funding Partners

- European Union
- Germany
- Kingdom of Saudi Arabia
- Republic of Korea
- Japan
- United Arab Emirates
The efforts of the Cyber and New Technologies Programme is supported by a wide range substantive partners.
Programme Achievements

The Cyber and New Technologies Programme efforts have resulted in notable achievements:

- More than **150 Member States** have benefited.
- **5 new Knowledge products** have been published.
- **Over 3000 officials** acquired new skills and knowledge.
- **32% Women** and **68% Men** Trained.
Security Council Resolution
SC Resolution 2341 (2017) on protection of critical infrastructure against terrorist threats

Protection efforts entail multiple streams of efforts, such as planning; public information and warning; operational coordination; intelligence and information sharing; interdiction and disruption; screening, search and detection; access control and identity verification; cybersecurity; physical protective measures; risk management for protection programmes and activities; and supply chain integrity and security.

Calls upon MS to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks.

Recalls that all States shall establish terrorist acts as serious criminal offences in domestic laws and regulations, and calls upon all Member States to ensure that they have established criminal responsibility for terrorist attacks intended to destroy or disable critical infrastructure, as well as the planning of, training for, and financing of and logistical support for such attacks.

Urges all States to ensure that all their relevant domestic departments, agencies and other entities work closely and effectively together on matters of protection of critical infrastructure against terrorist attacks;
7th Review of UN Global CT Strategy

...Urges all MS to take all necessary measures to prevent such attacks and to counter such terrorist acts, including the prosecution of perpetrators

Encourages MS to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks

Further calls upon MS States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect against, mitigate, investigate, respond to and recover from terrorist attacks...
Cooperation between CSIRTs and Law Enforcement

Why co-operation is important?

1. Better mitigation of cyber-incidents as well as cybercrime investigations
2. Better quality of electronic evidence
3. Greater availability of expertise and specialized technical tools
4. Improved availability of information about vulnerabilities and threats
5. Increased ability to respond to the large-scale attacks on national infrastructure
6. Greater security in society
Capacity Building

Threat-actor focused cybersecurity capacity building to foster cooperation between CSIRTs and Law Enforcement Authorities

Knowledge products

Raise awareness and support the adoption of guidelines into practice

OSINT

Use and application of open-source information for investigations and analysis of cyber-attacks

Darkweb

Investigations on darkweb to include collection, preservation and use of digital evidence in prosecution

Table-top exercises and Cyber Drills

To inform preparedness and response to terrorist cyber-attacks and foster collaboration and information sharing