International Digital Security Forum – Vienna
Security in times of pandemic and major global events

Adapting to the COVID-19 era: United Nations capacity-building work in the fields of counter-terrorism, cybersecurity and new technologies.

Fernando Puerto Mendoza
Programme Management Officer
Cybersecurity and New Technologies Unit

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

UN Office of Counter-Terrorism (UNOCT)

The United Nations Office of Counter-Terrorism was established through the adoption of General Assembly resolution 71/291 on 15 June 2017.

UNOCT is led by USG

Mr. Vladimir Voronkov

Secretary-General of the United Nations Mr. António Guterres (right) and Mr. Vladimir Voronkov (left), Under-Secretary-General of the United Nations Counter-Terrorism Office.

UN GCTS – 4 Pillars

PILLAR I

address the conditions conducive to the spread of terrorism

PILLAR II

prevent and combat terrorism

PILLAR III

build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard

PILLAR IV

ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism

Latest GCTS review (A/RES/72/284)
[The GA] "Expresses *concern at the increasing use, by terrorists and their supporters, of information and communications technologies, in particular the Internet and other media, and the use of such technologies to commit, incite, recruit for, fund or plan terrorist acts*."

Malicious uses of cyberspace by terrorists

Public activities (usually in the open web)

- Propaganda / Radicalization / Incitement / Glorification / Live-streaming / Fearmongering
- Training: dissemination of manuals / guides / video instructions to perpetrate attacks

Undercover activities (facilitated by encryption and the Darkweb):

- Planning, strategic support and coordination of attacks / Internal communications
- Procurement of weapons / false identities / illegal services (crime as a service)
- Financing: Online businesses / money laundering / digital payments / crypto assets
- Cyberattacks: Espionage / Data leaks / Defacements / Social media attacks / Sabotage of critical infrastructure
  - **Potentially, in combination with kinetic attacks**

UN Security Council Resolution 2341 (2017)

1. Each State determines what constitutes its CI and how to protect it from terrorist attacks.

2. States are encouraged to:

•raise awareness, expand knowledge and understanding of the challenges posed by terrorist attacks against CI

•develop of strategies for reducing risks to CI from terrorist attacks

•establish criminal responsibility for terrorist attacks against CI

•strengthen national, regional and international partnerships, both public and private

•ensure domestic interagency cooperation

•enhance international cooperation, including in sharing of information and good practices

Understanding the challenge: Cybercrime vs CT

- Terrorist Motivations
- Terrorism as a distinctive threat to CI
- Human rights-compliant approach to countering terrorism, also in cyberspace

Global Counter-Terrorism Programme on Cybersecurity & New Technologies

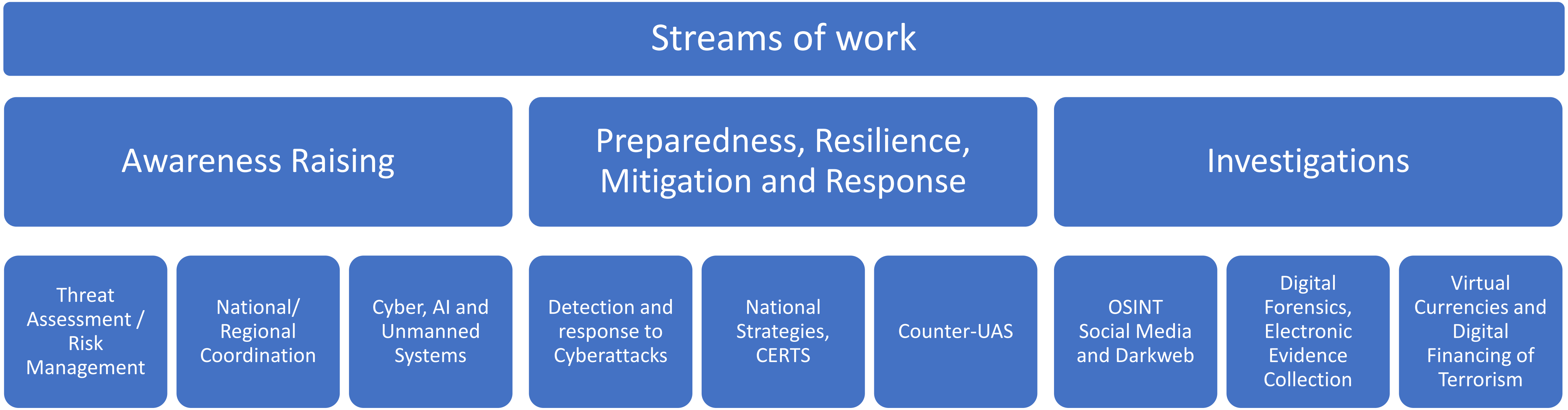
The programme aims to support MS, international and regional organisations and UN entities in:

Raising awareness of the threat of terrorist use of new technologies

Enhancing technical capacities and cooperation among Member States in the areas of

1) prevention, mitigation and response against the threat of terrorist and violent extremist groups misusing new technologies to perform attacks on critical infrastructure

2) countering and investigating terrorist activities by gathering digital forensic evidence and through the use of new technologies



Streams of work

Awareness Raising

Preparedness, Resilience, Mitigation and Response

Investigations

Threat Assessment / Risk Management

National/ Regional Coordination

Cyber, AI and Unmanned Systems

Detection and response to Cyberattacks

National Strategies, CERTS

Counter-UAS

OSINT Social Media and Darkweb

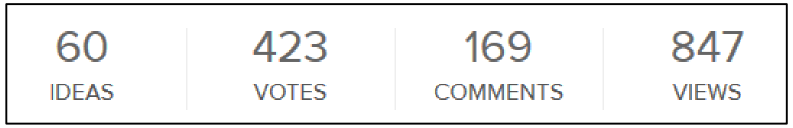
Digital Forensics, Electronic Evidence Collection

Virtual Currencies and Digital Financing of Terrorism

2019 Global Cybersecurity Challenge

- In collaboration with OICT and the Austrian Institute of Technology
- Global competition in two phases: 1) Online activity 2) On-site event in Vienna
  - Raise awareness among the youth of the threats of terrorist use of Internet
  - Identify ideas for future programmes

AUSTRIAN INSTITUTE OF TECHNOLOGY



60	423	169	847
IDEAS	VOTES	COMMENTS	VIEWS

CYBERSECURITY CHALLENGE
Countering Digital Terrorism
#CyberChallenge
# UNitetoCounterTerrorism
UNITED NATIONS OFFICE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
UNITED NATIONS OFFICE OF COUNTER-TERRORISM UN Counter-Terrorism Centre (UNCCT)
UNTIL
AIT

CYBERSECURITY CHALLENGE
Countering Digital Terrorism
COMBAT THE SPREAD OF TERRORIST CONTENT

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

COVID-19 effects

"The pandemic has also highlighted vulnerabilities to new and emerging forms of terrorism, such as misuse of digital technology, cyberattacks and bioterrorism."
UN Secretary General, Antonio Guterres, 6 July 2020[1]

Some well-known threats have recurrently increased as a result of the pandemic:

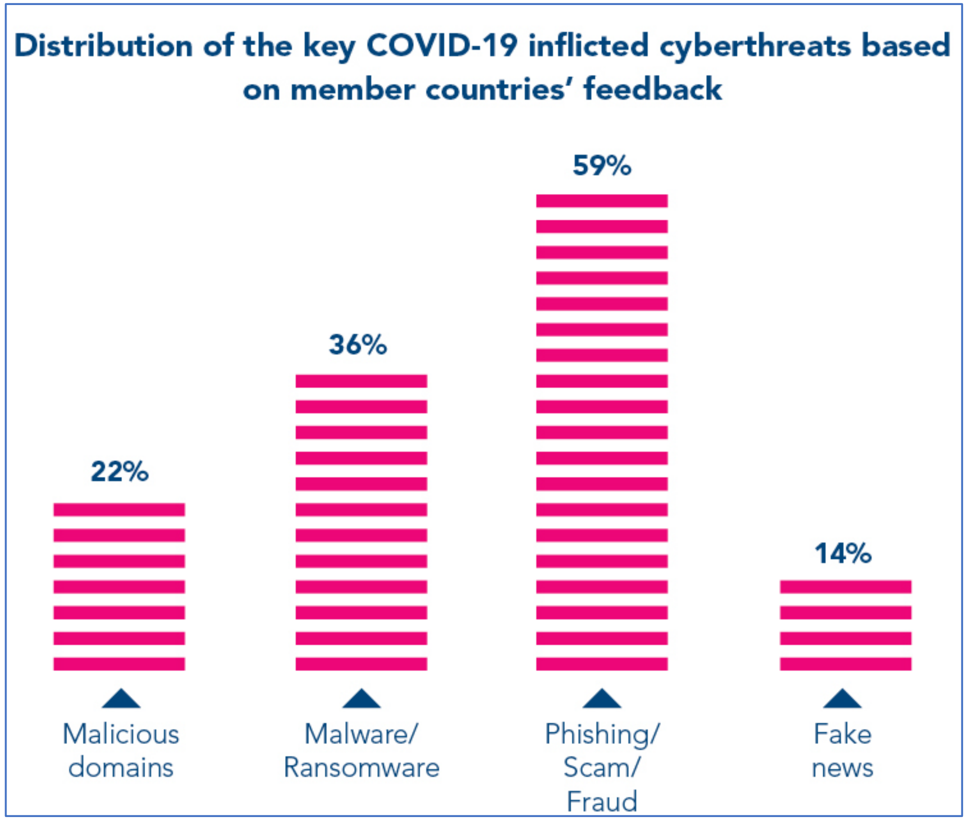
- In April 2020, WHO reported 5x increase in cyberattacks to hospitals[2]
- New perception of what constitutes critical infrastructure

Need for strengthening resilience of critical infrastructure and CERT-CERT cooperation

Global call for additional coordination and information sharing

[1] https://www.un.org/sg/en/content/sg/statement/2020-07-06/secretary-generals-remarks-the-opening-of-the-virtual-counter-terrorism-week-united-nations-delivered
[2] https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

COVID-19 effects (Cont.)



- Pandemic-related cyberthreats: Malicious domains, ransomware, phishing and fraud, and Fake news

- Increased propaganda, violent and extremist narratives and disinformation related to COVID-19

- Terrorist / radical groups are moving away from "traditional" social media platforms and turning instead to encrypted platforms, cloud storage services, filesharing services, pastebins, web archiving, gaming platforms…

These threats require global responses through communications strategies, law enforcement online investigations, and respecting universal human rights, with particular emphasis in freedom of expression and right to privacy.

https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Adapting UN work to the “new normal”

- “Virtualizing” training and other capacity building activities

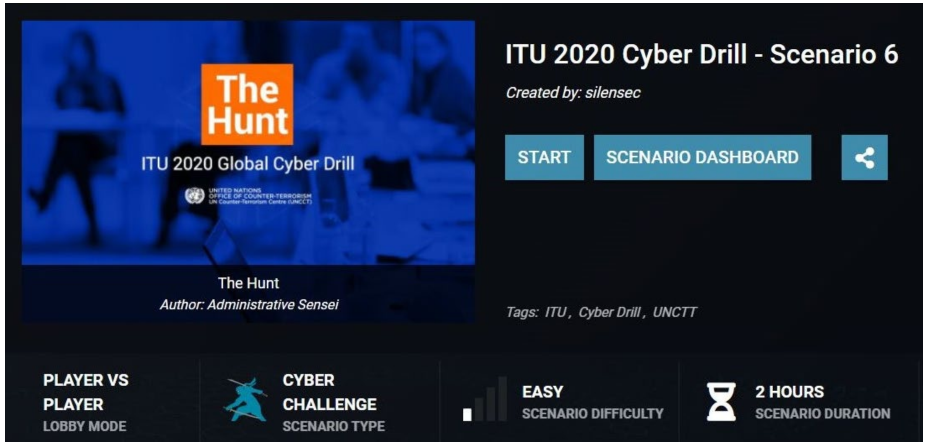
- Keeping up with the evolving cyber threats

- Engaging stakeholders remotely

- Focusing on the development of written outputs:
  - Research report on the potential use of AI by terrorists and violent extremists
  - Revised Global Guide to Developing a National Cyber Security Strategy, in collaboration with ITU
  - Handbook on internet counter-terrorism investigations, in collaboration with INTERPOL
  - Regional trends reports

- Developing of scenario-based training

- Leaning on UN regional presence to deliver UNOCT’s mandate



ITU 2020 Cyber Drill - Scenario 6

Created by: silensec

The Hunt

Author: Administrative Sensei

Tags: ITU, Cyber Drill, UNCTT

PLAYER VS PLAYER — LOBBY MODE

CYBER CHALLENGE — SCENARIO TYPE

EASY — SCENARIO DIFFICULTY

2 HOURS — SCENARIO DURATION

The Hunt
ITU 2020 Global Cyber Drill
UNITED NATIONS OFFICE OF COUNTER-TERRORISM UN Counter-Terrorism Centre (UNCCT)
START
SCENARIO DASHBOARD

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

un.org/counterterrorism | @UN_OCT | #UniteToCounterTerorrism

For a Future Without Terrorism