Protecting Critical Infrastructure from Terrorists' Cyber-Attacks: Threat-Actor Focused Approach

12 May 2023 | Offline effects of Online Activities
Mexico City, Mexico

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

New and Emerging Technologies

Technology is evolving at a rapid pace that can be abused by terrorist actors, as well as, provide opportunities for Counter Terrorism Law Enforcement authorities

Illustrative

> "*Requests* the Office of Counter-Terrorism and other relevant Global Counter-Terrorism Coordination Compact Entities 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."

Artificial intelligence/Machine Learning

Blockchain Technology

Encryption

Internet

- **Internet of Things**
- **Darkweb**
- **Web 3.0**

Social Media

Drone Technology

Virtual Assets

Additive Manufacturing (3D Printing)

Biometrics

Augmented Reality

Examples of Abuse

Internet / Social Media

Training
Propaganda
Live-Streaming
Radicalization
Glorification
Incitement

Encryption, Anonymised Networks

Planning, strategic support and co-ordination of attacks, internal communication, Procurement of weapons/false identities, Money laundering, digital payments, virtual

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

Programme Achievements

The Cyber and New Technologies Programme efforts has resulted in notable achievements

More than **150 Member States** have benefited

Over 3000 officials acquired new skills and knowledge

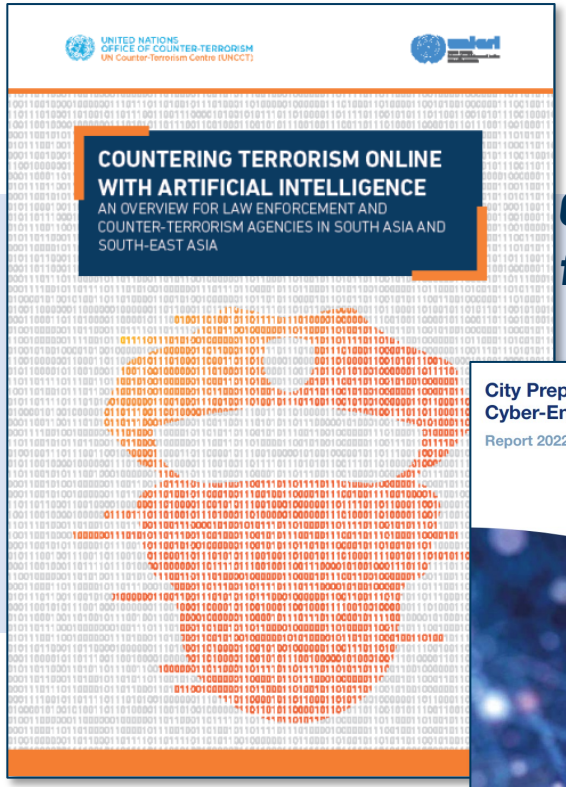
5 new Knowledge products have been published

32% Women and 68% Men Trained

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

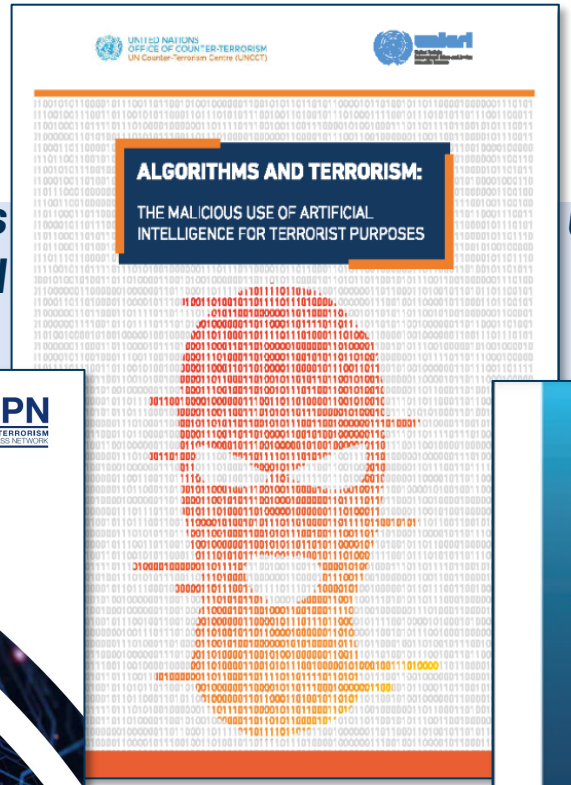
Knowledge Products

Examples of knowledge products developed under the Cyber & New Technology Programme



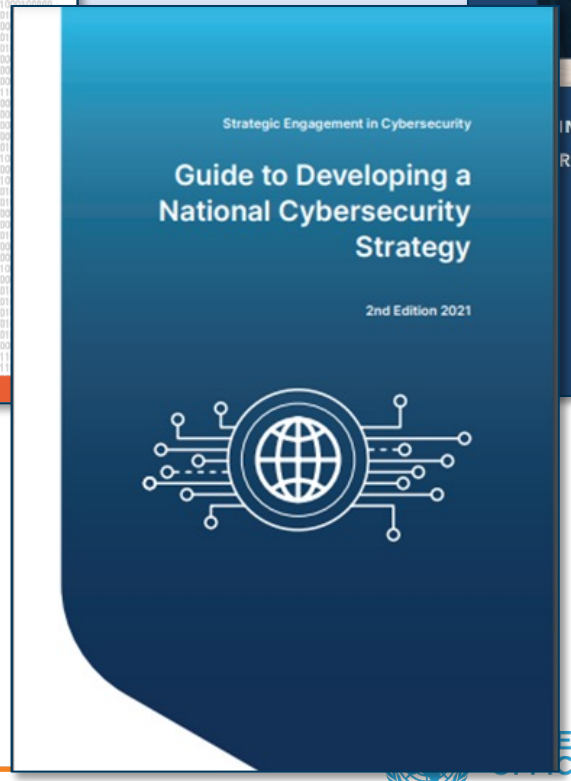
Countering Terrorism Online with Artificial Intelligence

City Preparedness for Cyber-Enabled Terrorism



Malicious Use of Artificial Intelligence for Terrorist Purposes

Guide for National Cybersecurity Strategy



OSINT for Counter-Terrorism Investigations

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;***

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

7th Review of the UN Global Counterterrorism Strategy (GCTS)

Critical Infrastructure Protection – 7th review of the GCTS

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...*

National Computer Security Incident Response Teams (CSIRT)

National CSIRTs are the national point of contact for domestic incident-response stakeholders and for other national CSIRTs around the world

Worldwide there are currently 118 National CSIRTs

Source(s): ITU

Law enforcement role in cybersecurity

Law enforcement agencies – reduce the number of threat actors by prosecuting culprits for criminal acts

Illustrative

Investigations

Collection

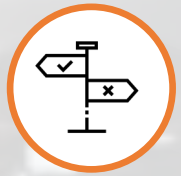
Processing

Analysis

Executive Action

Arrest / Disruption

Decision



Prosecution

Criminal Case Development

Legal Proceedings

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

Cybersecurity – Roles and Responsibilities

National CSIRTs and Law Enforcement Authorities play a central role with regards to cybersecurity and cyber incidents

National CSIRTs

- **Cyber-incidents**
- **Priority to recovering system and making them less vulnerable to future attacks (“technical mentality”)**
- **Securing and rebuilding compromised system**
- **Protection and hardening of systems to reduce the risk of incident**
- **Deterring attacks through protection and hardening of systems**

Law Enforcement Authorities

- **Cyber crimes**
- **Priority to attributing the attack and prosecuting the culprit**
- **Attributing the attack and collecting evidence**
- **No role in protection and hardening of systems, exploitation of vulnerabilities**
- **Deterring attacks through prosecution of criminals**

Cybersecurity Responsibility Matrix

Duties: Prior to incident/crime

High-Level

Prior to Incident / Crime	During Incident / Crime		Post Incident / Crime	
	CSIRT	*Law Enforcement*	*Judges / Magistrate*	*Prosecutors*
Collecting cyber-threat intelligence	✓	✓		✓
Analysis of vulnerabilities and threats	✓	✓		✓
Issuing recommendations for new vulnerabilities and threats	✓			
Advising potential victims on preventive measures against cyber-crime	✓			

Cybersecurity Responsibility Matrix

Duties: During the incident/crime

High-Level

Prior to Incident / Crime | **During Incident / Crime** | **Post Incident / Crime**

	CSIRT	*Law Enforcement*	*Judges / Magistrate*	*Prosecutors*
Discovery of the cyber-incident/crime	✓	✓		
Classification of the cyber-incident/crime	✓	✓		✓
Identification of the type & severity of a compromise	✓	✓		✓
Evidence collection	✓	✓		✓
Preserving the evidence	✓	✓		✓
Mitigation of an incident	✓	✓		✓
Conducting criminal investigation		✓		✓
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓		✓

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

Cybersecurity Responsibility Matrix

Duties: Post incident/crime

High-Level

Prior to Incident / Crime	During Incident / Crime	Post Incident / Crime			
	CSIRT	Law Enforcement	Judges / Magistrate	Prosecutors
Systems recovery	✓			
Protecting the constituency	✓			
Analysis and interpretation of collected evidence		✓	✓	✓
Requesting testimonies from CSIRT and LE			✓	✓
Admitting and assessing the evidence			✓	✓
Judging who committed a crime			✓	
Assessing incident damage and cost	✓	✓	✓	✓
Reviewing the response and updating policies and procedures	✓			

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

Cooperation

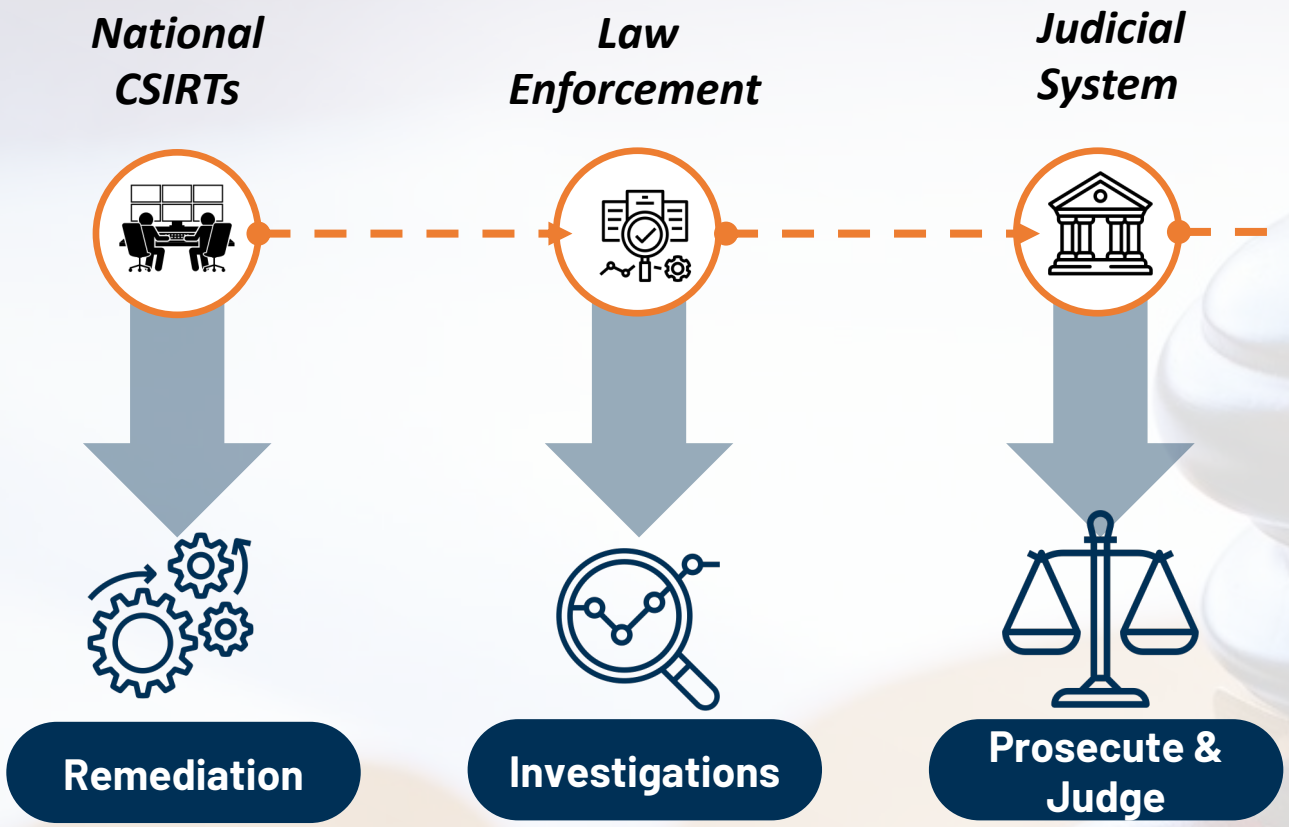
Why co-operation is important?

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

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

Cooperation between CSIRT and Law Enforcement

How LE-CSIRT cooperation can be improved?



- **Legal frameworks establishing formal rules for co-operation**
- **Internal policies**

Capacity Building

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

Threat-Scenario Exercise

- **Collaboration with the OAS:**
  - **TTX later today**
- **Collaboration with the ITU:**
  - **Global and regional cyber drills to foster co-operation between CSIRTs and law enforcement**
- **Collaboration with the Counter-Terrorism Preparedness Network:**
  - **Development of knowledge to increase cities' preparedness to terrorist cyber-attacks**
  - **Table-top exercise for cities**

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

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

Cybersecurity and **New Technologies**

Akvile Giniotiene,
Head, Cyber and New Technologies Unit
akvile.giniotiene@un.org