Improving Co-operation between National CSIRTs and Law Enforcement

21 November 2022 | ITU 10th Cyber Drill for Americas
Tegucigalpa, Honduras

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

Impact of new technologies to countering terrorism

OPEN WEB

- Propaganda
- Radicalization
- Incitement
- Glorification
- Live-streaming
- Training

ENCRYPTION, ANONYMISED NETWORKS

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

GCTS Pillar II: "*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."

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

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

Programme Donors

- European Union
- Germany
- Japan
- Kingdom of Saudi Arabia
- Republic of Korea
- United Arab Emirates

Programme achievements

Achievements

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

SC Resolution 2341 (2017) on protection of critical infrastructure against terrorist threats

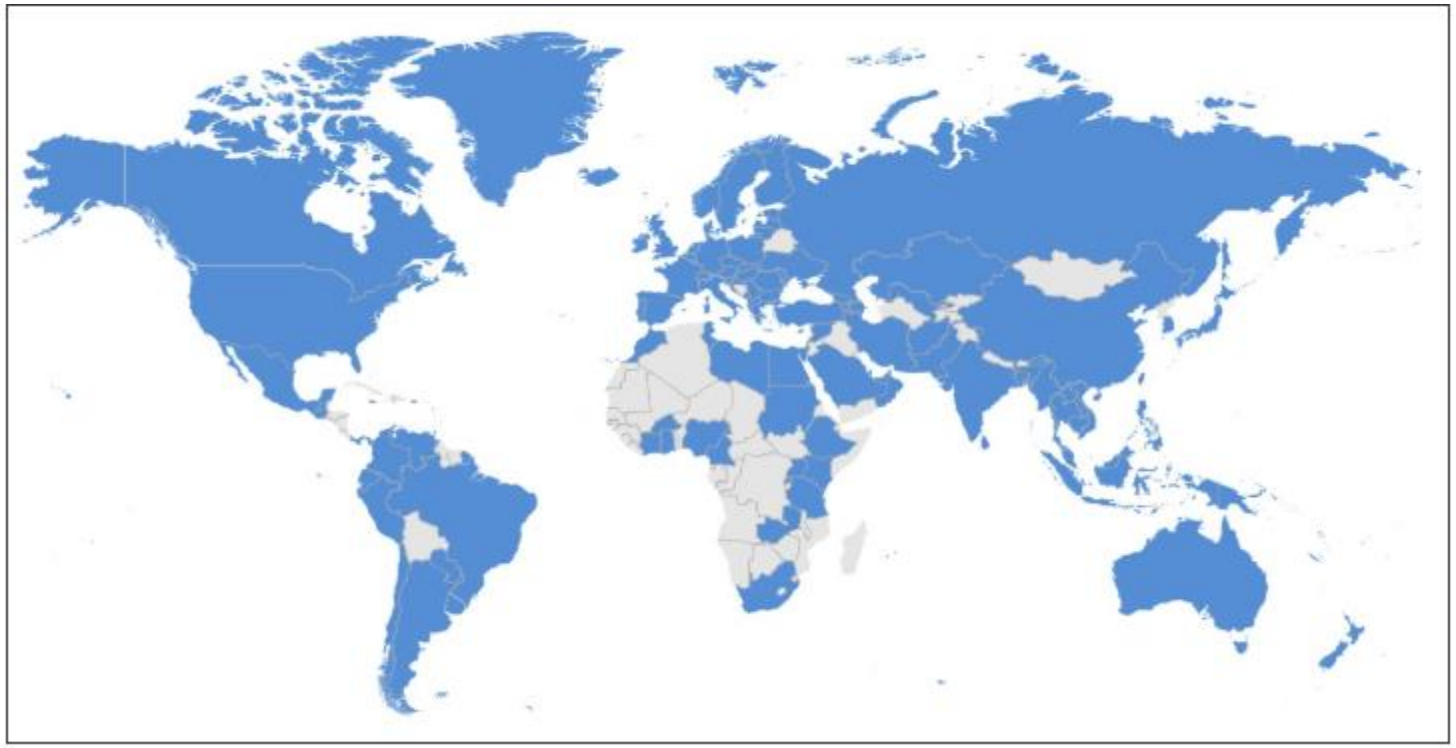
- Protection efforts entail multiple streams of efforts, such as planning; public information and warning; operational coordination; intelligence and information sharing; interdiction and disruption; screening, search and detection; access control and identity verification**; cybersecurity**; physical 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**;

Critical Infrastructure Protection – 7th review of the GCTS

- *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

CSIRTs role in a national cybersecurity eco-system

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



Source: ITU

Law enforcement role in cybersecurity

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

Different approaches to cybersecurity

National CSIRT

- 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 Agencies

- 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

Duties: Prior to incident/crime

Activities	CSIRT	LE	Judges	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	√	√		

Duties: During the incident/crime

Activities	CSIRT	LE	Judges	Prosecutors
Discovery of the cyber-incident/crime	√	√		
Classification of the cyber-incident/crime	√	√		√
Identification of the type and 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	√	√		√

Duties: Post incident/crime

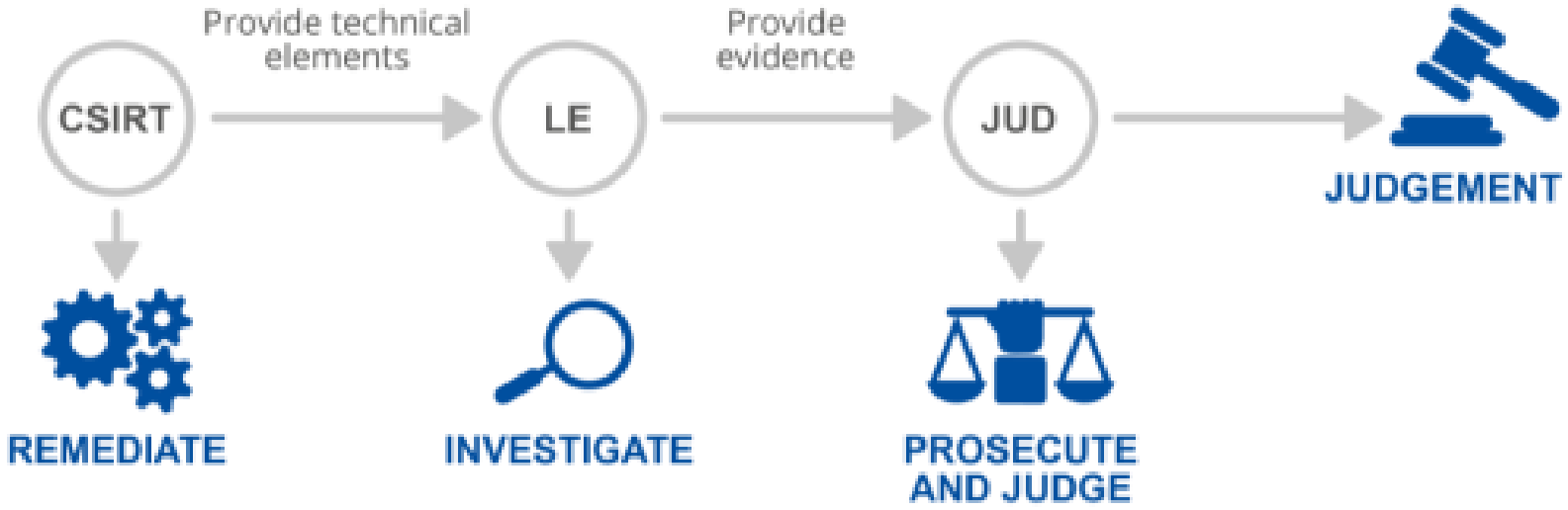
Activities	CSIRT	LE	Judges	Prosecutors
Systems recovery	√			
Protecting the constituency	√			
Analysis and interpretation of collected evidence		√	√	√
Requesting testimonies from CSIRT and LE			√	√
Admitting and assessing the evidence			√	√
Judging who committed a crime			√	
Assessing incident damage and cost	√	√	√	√
Reviewing the response and updating policies and procedures	√			

Why co-operation is important?

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

How LE-CSIRT cooperation can be improved?

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



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