Cybersecurity Dimensions of the UN Security Council Resolution 2341 (2017)

UNOCT/UNCCT Capacity Building Efforts

ICAO Global Aviation Security Symposium 2019 (AVSEC19)

UNSCR 2341 and the Role of Civil Aviation in Protecting Critical Infrastructure from Terrorist Attacks

Fernando Puerto Mendoza, Programme Management Officer

20 September 2019 - Montreal, Canada

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

Overview:
Cybersecurity dimensions of UNSRC 2341 (2017)

- Critical Infrastructure and ICT
- Threat landscape, recent cyberattacks
- Mapping of the Resolution into the Cybersecurity dimension
  - Initial Considerations
  - Preamble
  - Operative Clauses
- UNOCT/UNCCT and Capacity Building work on New Tech

CI and ICT

- Almost all Critical Infrastructure (CI) relies on Information/Communication Technologies, Industrial Control Systems or Operational Technologies (PLCs, SCADA, DSC, …)
- In a connected world, inherent vulnerabilities of ICT expose CI to cyber threats
- Cyber-attacks against CI, as much traditional kinetic attacks, can have devastating outcomes
- Lower risk for the attacker:
  - They don’t require physical presence, travel, border controls, handling of illegal materials
  - Attribution of cyberattacks is very challenging
  - Capabilities to perform cyberattacks are becoming more accessible, less expensive (cyberattacks-as-a-service)

Critical Infrastructure as a target for cyber-attacks

Threat Actor

Adversary with malicious **intent** and **capability**

Opportunity

Malicious Act

Commits a **threat event** or malicious act (cyber-attack)

Which exploits a **security vulnerability**

Vulnerability

Computer-based Systems

Critical Infrastructure

Which violates the C-I-A of information or the system with physical consequence

Threat landscape, recent Cyber-attacks

20 July 2019:
NASA's Jet Propulsion Laboratory (JPL) attacked

Forbes

142,476 views | Jun 20, 2019, 10:58 am

Confirmed: NASA Has Been Hacked

Davey Winder Senior Contributor

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

The U.S. National Aeronautics and Space Administration (NASA) this week confirmed that its Jet Propulsion Laboratory (JPL) has been hacked. An audit document from the U.S. Office of the Inspector General was published by NASA this week. It reveals that an unauthorized Raspberry Pi computer connected to the JPL servers was targeted by hackers, who then moved laterally further into the NASA network. How much further? Well, the hackers apparently got as far as the Deep Space Network (DSN) array of radio telescopes and numerous other JPL

Recent Cyber-attacks - Ramsomware

July 25, 2019 (Reuters):
Power distribution company in South Africa.

WORLD NEWS JULY 25, 2019 / 5:36 AM / 2 MONTHS AGO

Johannesburg power body hit by ransomware attack

2 MIN READ

JOHANNESBURG (Reuters) - City Power, responsible for powering South Africa's financial capital Johannesburg, said on Thursday it had been hit by a ransomware virus that had encrypted all of its databases, applications and

CNBC SEARCH QUO

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV

TECH

Louisiana declares state of emergency after cybercriminals attack school districts

PUBLISHED FRI, JUL 26 2019 • 12:25 PM EDT

Kate Fazzini
@KATEFAZZINI

SHARE

KEY POINTS

- Louisiana's governor has declared a state of emergency over a cybersecurity issue after a series of attacks shut down phones and locked and encrypted data at three of the state's school districts.

July 26, 2019 (CNBC):
Louisiana's school districts

Initial Considerations – UNSCR 2341

As a Security Council Resolution, 2341 is legally binding

UN Security Council

From the Resolution's preamble:

- Member States can decide what they consider Critical Infrastructure
- Cybersecurity is one of the "streams of efforts" for protection
- Vital role of promoting awareness of terrorist threats and vulnerabilities through regular national local dialog, training and outreach.
- The role of preparedness for terrorist attacks includes: 1) prevention, 2) protection, 3) mitigation, 4) response and 5) recovery

Preparedness vs. Cyber kill chain

1) Prevention	• Avoid attack • Awareness of threats • Good security hygiene
2) Protection	• Physical controls • Logical controls • Legal or admin controls
3) Mitigation	• Risk management • Minimize damage
4) Response	• Procedures in case of attack
5) Recovery	• Bringing operation back to normal

Reconnaissance & Plotting	• Forming the attack strategy
Scan	• Search for vulnerabilities
Attack	• Circumvention of controls • Exploiting vulnerabilities
Command & Control	• Escalation • Hiding traces
Actions on targets	• Inflict damage/exfiltration of information

Cyber dimensions of 2341 - **Preamble**

- Interdependencies: Cross-border and cross-sector [Everything is connected]

- Protection requires cooperation domestically and cross borders with governmental authorities, foreign partners and private sector: Knowledge sharing, best practices, lessons learned.

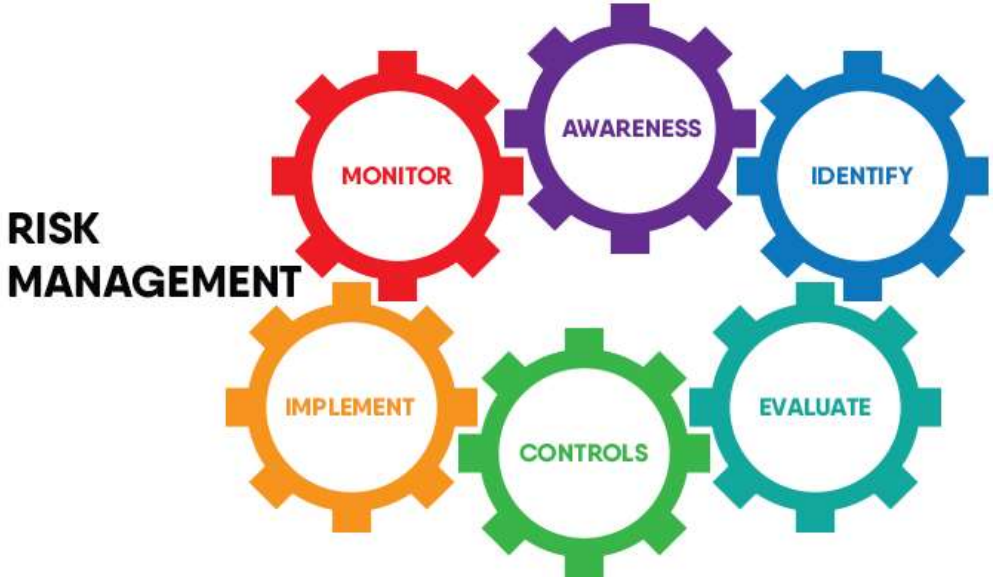
Cyber dimensions of 2341 – **Operative Clauses**

- (1) Coordinated efforts to raise awareness, expand knowledge and understanding of the challenges.., in order to improve preparedness
- (2) Strategies for risk reduction
- (3) Ensure criminal responsibility for terrorist attacks intending to disable/destroy CI, as well as the planning/training/financing/logistical support for such attacks.
- (4) Exchange relevant information/cooperation
- (5) National/international partnerships with private/public stakeholders to share information[…], including through joint training
- (11) CTC, CTED and CTITF [now the Compact] to continue facilitating bilateral/ multilateral technical assistance/capacity building

(2) Strategies for Risk Reduction

Approaches to Risk Management:

- Identifying/preparing for terrorist threats
- Reduce vulnerability of CI
- Preventing and disrupting terrorist plots against CI
- Minimizing impacts and recovery time in the event damage from attacks
- Identifying the cause of damage or the source of attack
- Preserving evidence of an attack
- Holding those responsible for an attack accountable

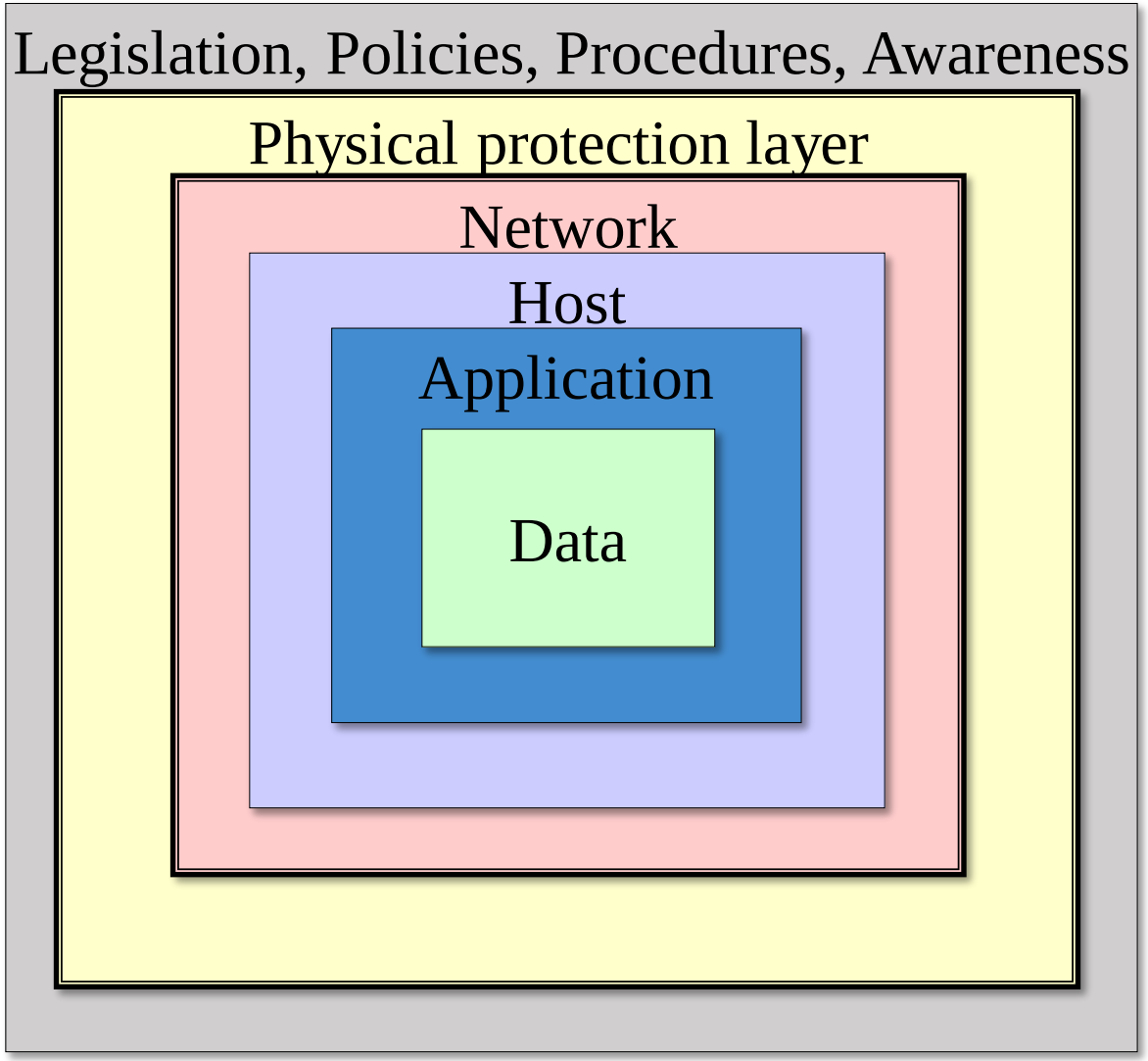


Reduce vulnerability of CI: Defense-in-Depth

Defense-in-depth is a security principle.

"Concept of multiple layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by adversaries in order to achieve their objectives."

Defense-in-Depth: Layered Measures



Layers of defence are implemented at multiple levels of the system architecture and combined with the technical and administrative measures

About UNOCT

Established through General Assembly resolution 71/291 (15 June 2017)

Led by USG Mr. Vladimir Voronkov

Five main functions:

- **LEADERSHIP**
- **COORDINATION**
- **CAPACITY BUILDING**
- **IMPROVING VISIBILITY**
- **ADVOCACY**

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.

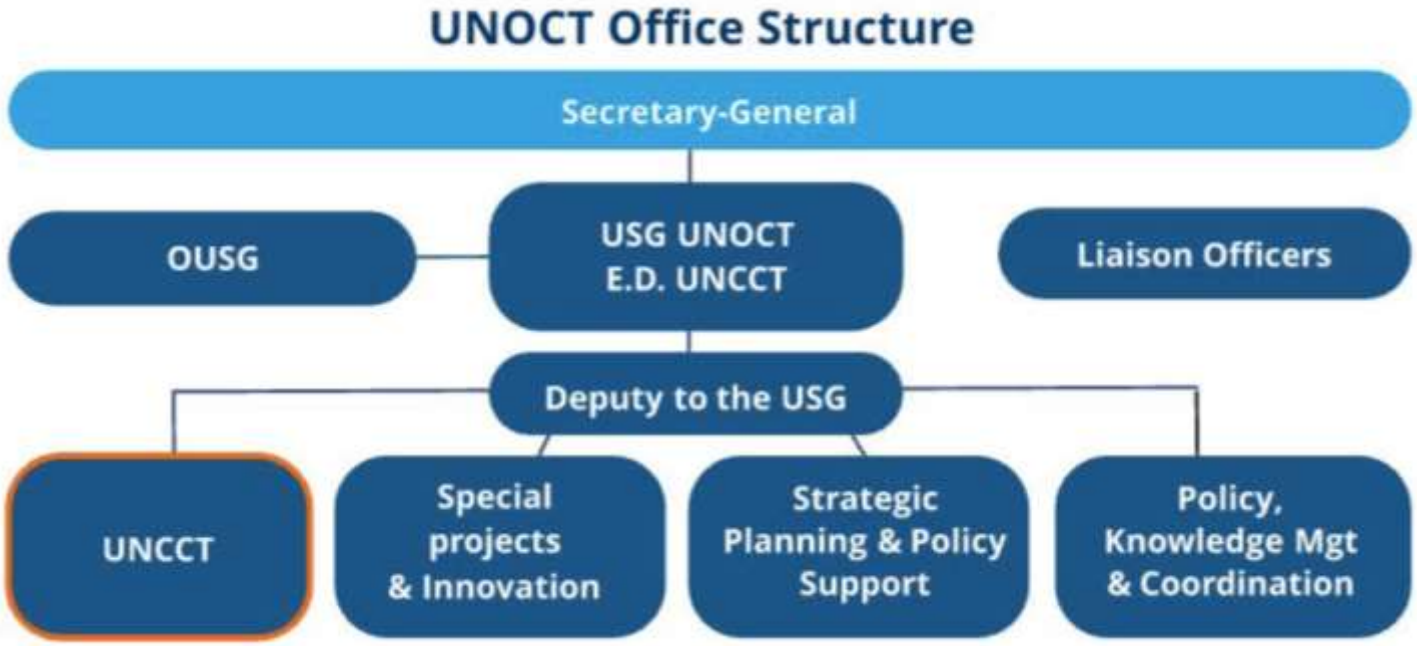
#UNiteToCounterTerrorism

About UNCCT

The UN Counter-Terrorism Center was established in 2011 to promote international counter-terrorism cooperation and support Member States in the implementation of the Global Counter-Terrorism Strategy

Provide global good practice to help Member States address and counter the threat of terrorism and violent extremism

Centre of Excellence in providing Member States capacity-building to implement the Global Counter-Terrorism Strategy in a balanced manner.



UN Global CT Strategy – 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

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

Source: https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy

UNOCT – Two approaches regarding New Technologies

1) Countering terrorist misuse of technology:

- Terrorist financing using digital platforms and cryptocurrencies
- Recruitment and spread of terrorist narratives online
- Cyberattacks against CI
- UAVs threats
- Dark web communications

2) Use of technology to counter terrorism

- OSINT techniques
- Digital evidence collection and forensic investigations/ prosecution
- API-PNR / GoTravel project

Belarus High-Level Conference, 3-4 September 2019
Countering Terrorism Through Innovative Approaches and the use of New and Emerging Technologies

UNCCT's Cyber-Security Project (I)

"Enhancing the Capacity of Member States to Prevent and Investigate Cyber-attacks Perpetrated by Terrorist Actors and Mitigate their Impact"

***Funded** by the Governments of Japan and The Kingdom of Saudi Arabia*

***Goal**: Enhance capacities to prevent cyber-terrorist attacks against critical infrastructure, mitigate their impact, recover and restore the targeted structures, should these occur.*

***Outcome 1**: Enhanced Member States' awareness of the threats*

***Outcome 2**: Enhanced Member States' knowledge of the solutions to increase IT Security and resiliency of critical infrastructures*

UNCCT's Cyber-Security Project (II) *Phase I - 2019*

Participant Member States:

South East Asia and Bangladesh (11 Member States)

Completed Activities:

July 2019 - Regional Workshop for Awareness raising and scope the need

September 2019 – Pilot in-depth training for Bangladesh, Brunei, Lao PDR, Philippines, and Thailand

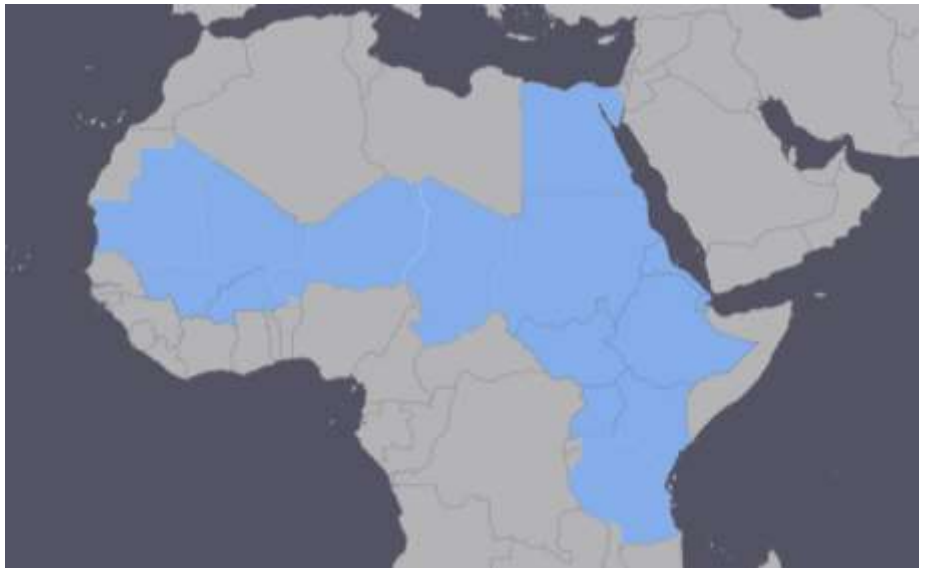
UNCCT's Cyber-Security Project (III) *Phase I - 2020*

3 Participant Regions:

Sahel (5 Member States)

East Africa (3 Member States)

Horn of Africa (6 Member States)



Activities per Region:

Regional Workshop for Awareness raising

Pilot in-depth training for selected countries

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

un.org/counterterrorism | @UN_OCT | #UniteToCounterTerorrism

For a Future Without Terrorism