CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

Rouda AlAmir Ali

Programme Officer

ITU Arab Regional Office

Meet us

ITU at a glance

What we do

‘Committed to Connecting the World’

3 Sectors

ITU Radiocommunication

Coordinating radio-frequency spectrum and **assigning** orbital slots for satellites

ITU Standardization

Establishing global standards

ITU Development

Bridging the digital divide

193

MEMBER STATES

+700

INDUSTRY & INTERNATIONAL ORGANIZATIONS

+150

ACADEMIA MEMBERS

MEMBERSHIP

Cybersecurity in ITU – A brief timeline

Geneva 2003 – Tunis 2005

WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 - **"Building Confidence and Security in the use of ICTs"**

INTERNATIONAL COOPERATION
LEGAL MEASURES
CAPACITY BUILDING
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

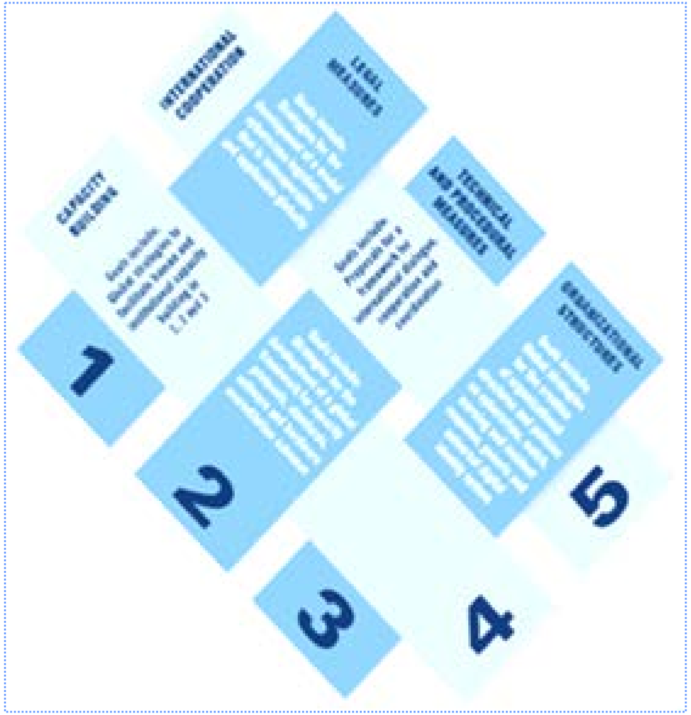
In 2007 **Global Cybersecurity Agenda (GCA)** was **launched** by the Secretary General of ITU. GCA is a **framework for development and international cooperation in cybersecurity**

In 2008 ITU Membership **endorsed** the **GCA** as the ITU-wide strategy on international cooperation & initiative on COP started.

Building confidence and security in the use of ICTs is widely embedded in ITU Governing **Conferences**' resolutions.

Global Cybersecurity Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.
- GCA builds upon five pillars:
    1. Legal Measures
    2. Technical and Procedural Measures
    3. Organizational Structure
    4. Capacity Building
    5. International Cooperation
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.


INTERNATIONAL COOPERATION
LEGAL MEASURES
CAPACITY BUILDING
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

ITU’s Role in Tackling Cyber Threats

To build confidence and security in the use of telecommunications/ICTs, develop and implement standards in cybersecurity on International Level

Assist Member States to strengthen cybersecurity capacity to effectively share information, find solutions, and respond to cyber threats, and to develop and implement national strategies and capabilities, including capacity building, encouraging national, regional and international cooperation towards enhanced engagement among Member States and relevant players

Develop products and services for building confidence and security in the use of telecommunications/ICTs, such as reports and publications, and for contributing to the implementation of national and global initiatives

Our Approach - Implementation Mechanisms

Project Implementations

Technical Assistance

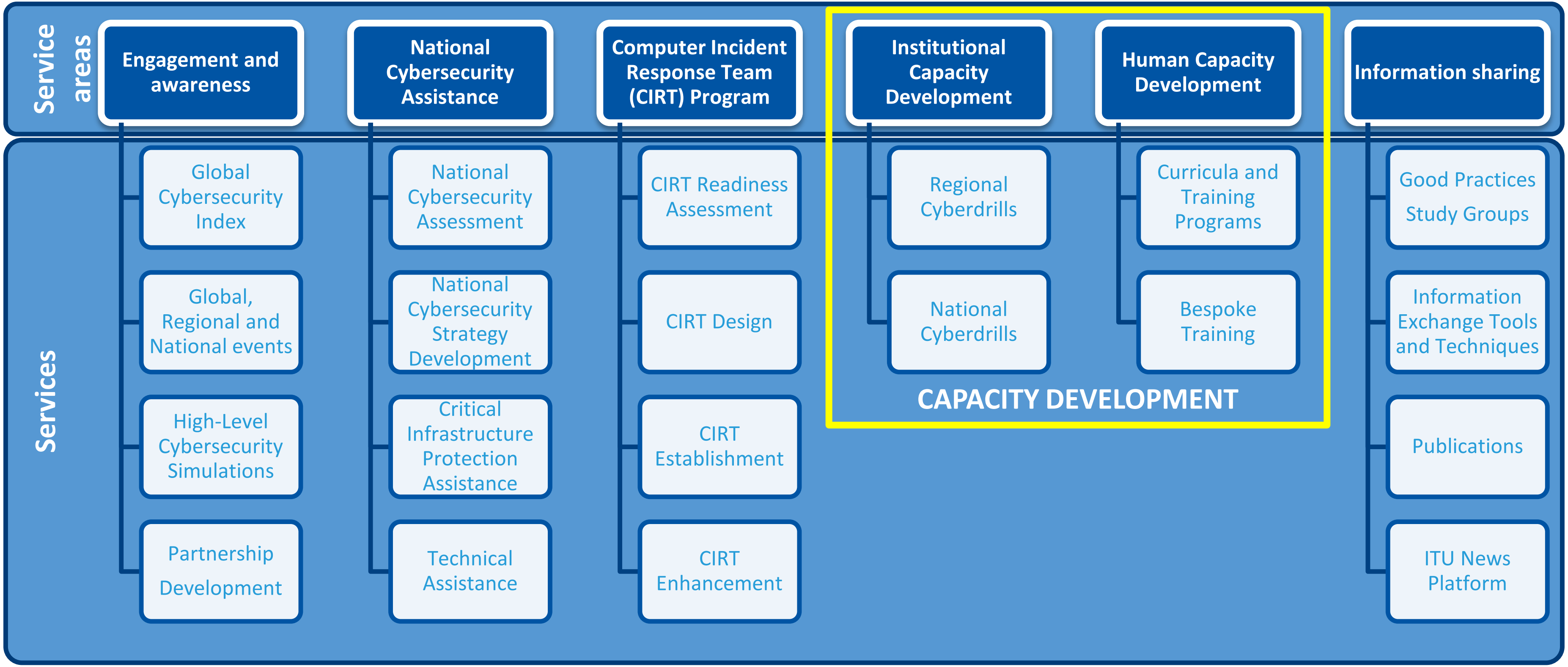
Information Sharing

Capacity Development

Partnership Development

Product Development

Cybersecurity Services Catalogue



Service areas

Services

Engagement and awareness
- Global Cybersecurity Index
- Global, Regional and National events
- High-Level Cybersecurity Simulations
- Partnership Development

National Cybersecurity Assistance
- National Cybersecurity Assessment
- National Cybersecurity Strategy Development
- Critical Infrastructure Protection Assistance
- Technical Assistance

Computer Incident Response Team (CIRT) Program
- CIRT Readiness Assessment
- CIRT Design
- CIRT Establishment
- CIRT Enhancement

Institutional Capacity Development
- Regional Cyberdrills
- National Cyberdrills

Human Capacity Development
- Curricula and Training Programs
- Bespoke Training

CAPACITY DEVELOPMENT

Information sharing
- Good Practices Study Groups
- Information Exchange Tools and Techniques
- Publications
- ITU News Platform

CIRT Framework for protecting critical information infrastructure

CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
CERT	Computer Emergency Response Team
CIRC	Computer Incident Response Capability
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

Why CIRT?

CIRT serves as a trusted central coordination point of contact for cybersecurity aims at identifying, defending, responding and managing cyber threats.

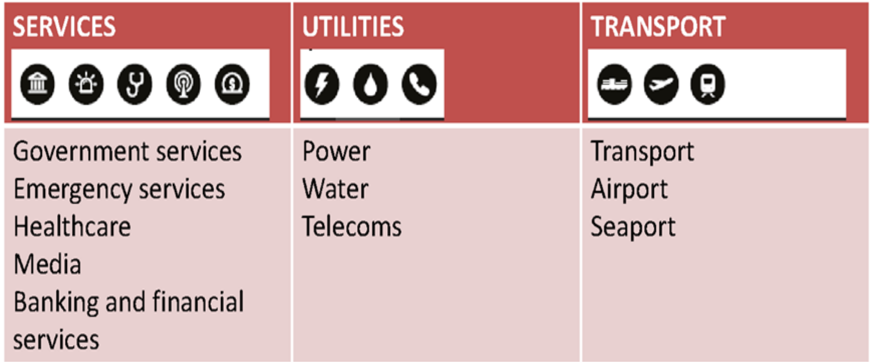
CIRT in charge of protecting critical information infrastructures should possess minimum set of capabilities in order to take part in and contribute to sustainable cross-border information sharing and cooperation.

CIRTs to strengthen the security and resilience of national (critical) information infrastructures.

What Is National Critical Information Infrastructure?

Singapore

sectors



SERVICES	UTILITIES	TRANSPORT
Government services Emergency services Healthcare Media Banking and financial services	Power Water Telecoms	Transport Airport Seaport

Definition of Critical National Infrastructure:

“CIIs are computers or computer systems that are necessary for the continuous delivery of essential services that Singapore relies on, the loss or compromise of which will lead to a debilitating impact on national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. Currently, essential services have been identified in 11 sectors, including utilities, banking and finance, media, info-communications, healthcare and transportation.”

The Cyber Security Agency of Singapore (CSA) - Singapore -

What Is Critical National Infrastructure?

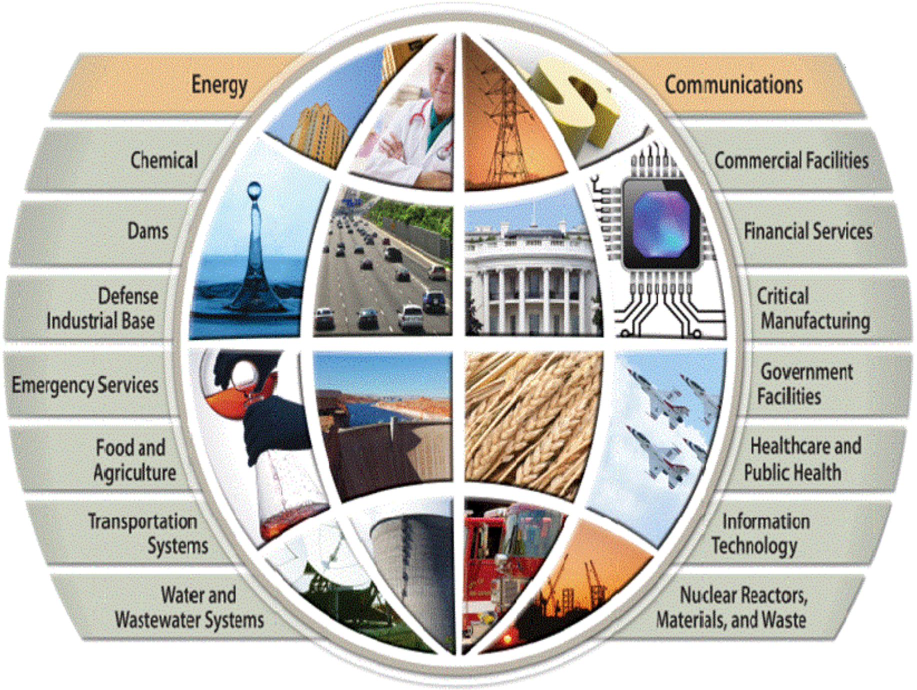
The United States of America

Definition of Critical National Infrastructure:

"Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

Department of Homeland Security -USA-

sectors



What Is Critical National Infrastructure?

Malaysia

Definition of Critical National Infrastructure:

“Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on:

- National economic strength; Confidence that the nation's key growth area can successfully compete in global market while maintaining favourable standards of living.
- National image; Projection of national image towards enhancing stature and sphere of influence.
- National defence and security; guarantee sovereignty and independence whilst maintaining internal security.
- Government capability to functions; maintain order to perform and deliver minimum essential public services.
- Public health and safety; delivering and managing optimal health care to the citizen.”

sectors

DEFENCE & SECURITY

TRANSPORTATION

BANKING & FINANCE

HEALTH SERVICES

EMERGENCY SERVICES

ENERGY

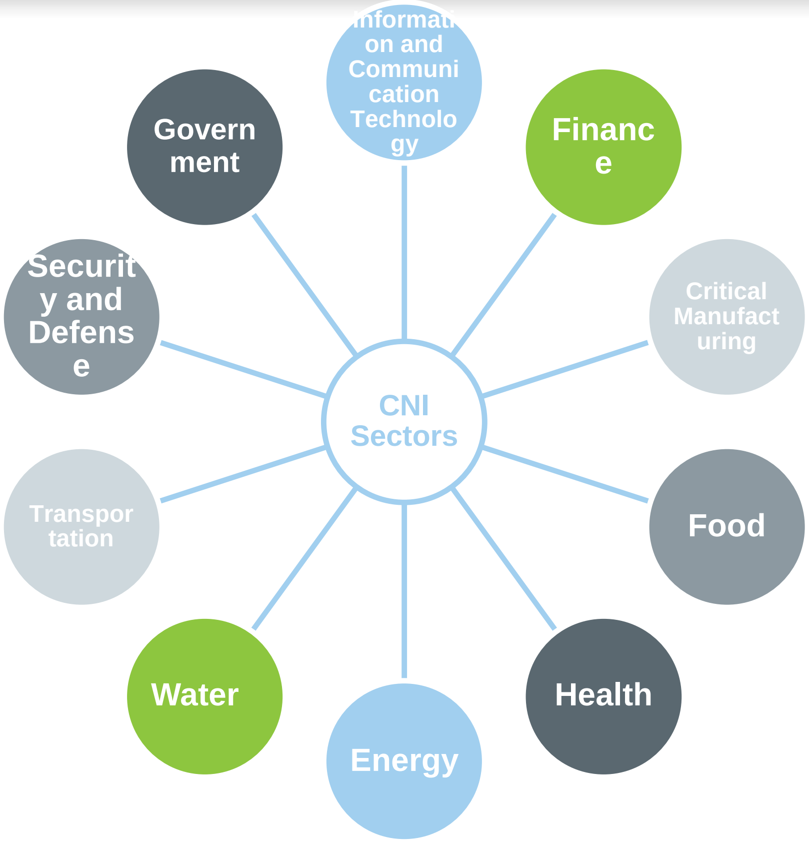
INFORMATION & COMMUNICATIONS

GOVERNMENT

FOOD & AGRICULTURE

WATER

In General, we can identify 10 Critical National Infrastructure sectors :



CNI Sectors

Information and Communication Technology

Finance

Critical Manufacturing

Food

Health

Energy

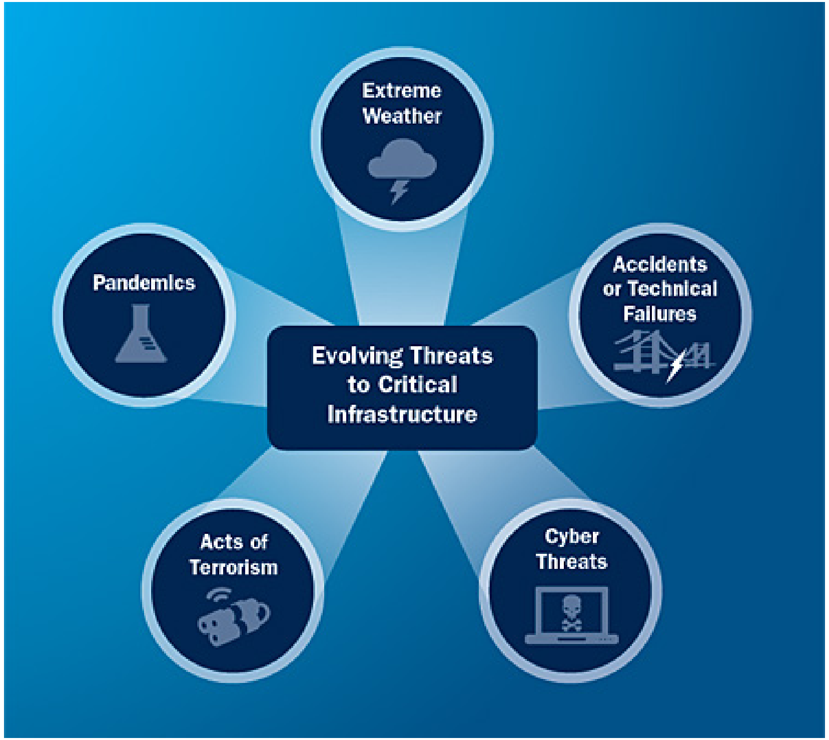
Water

Transportation

Security and Defense

Government

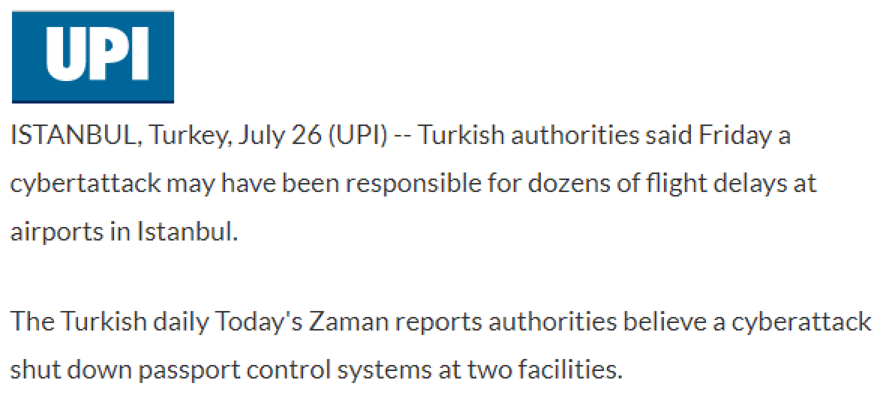
Threats to Critical National Infrastructure


Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

Source : https://emilms.fema.gov

Threats to Critical National Infrastructure

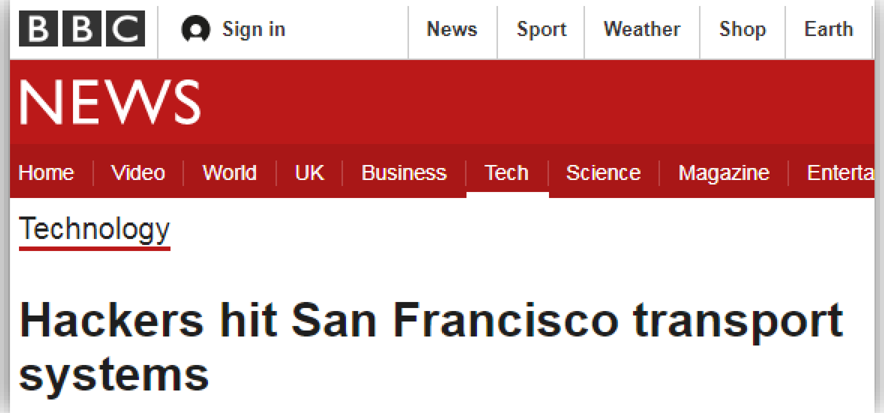
Istanbul Airports
July 2016


UPI

ISTANBUL, Turkey, July 26 (UPI) -- Turkish authorities said Friday a cybertattack may have been responsible for dozens of flight delays at airports in Istanbul.

The Turkish daily Today's Zaman reports authorities believe a cyberattack shut down passport control systems at two facilities.

San Francisco train system
November 2016



Technology

Hackers hit San Francisco transport systems

Type of Incident Response Team

- **National Incident Response Team**
- **Organizational Incident Response Team**

  Governmental CIRT
- **Multi-Organizational Incident Response Team**

  UN-CSIRT , CERT-EU
- **Sectorial Incident Response Team**

  Financial Institutions CIRT , CII CIRT
- **Regional Incident Response Team**

  AfricaCERT, APCERT , OIC-CERT

The Role of the national CIRT in the CIIP

What is a National CIRT?

enisa

A national / governmental CERT typically handles incidents at a national level, identifies incidents that could affect critical infrastructures, warns critical stakeholders about computer security threats, and helps to build effective incident response across its constituency in both, public and private sectors.

CERT

A National CSIRT coordinates incident management and facilitates an understanding of cyber security issues for the national community. A National CSIRT provides the specific technical competence to respond to cyber incidents that are of national interest.

FIRST

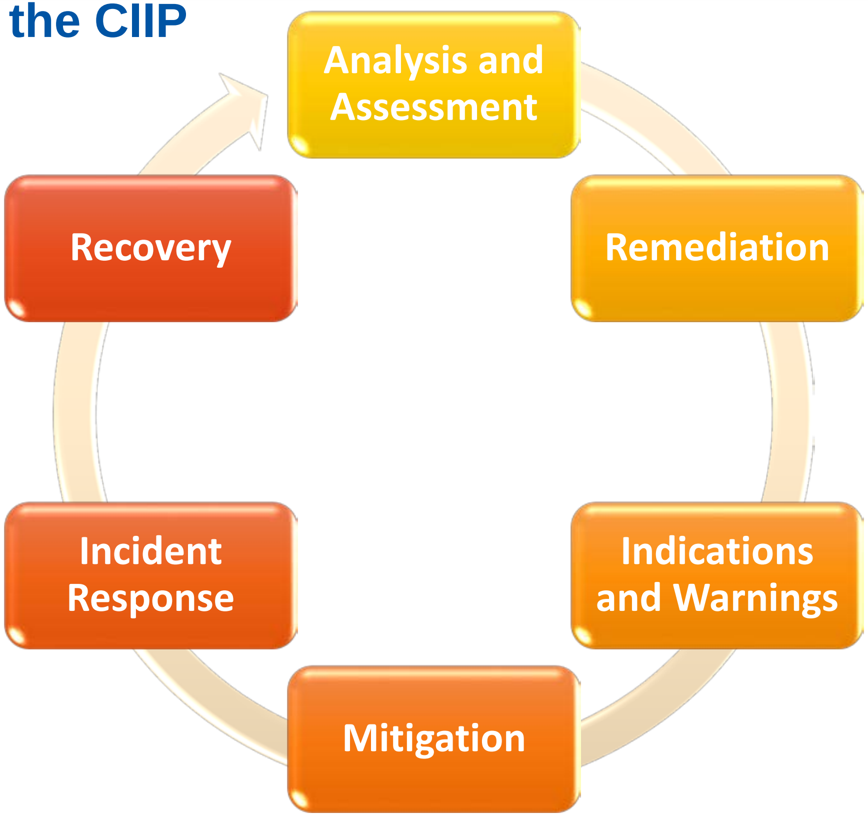
A national CSIRT refers to an entity which has the sole mandate to provide national-level coordination of cybersecurity incidents. Its constituency generally include all government departments/agencies, law enforcement, private sector, academia, and civil society. It also generally is the authority to interact with the national CSIRTs of other countries, as well as with regional and international players.

Role of CIRT within the CIIP

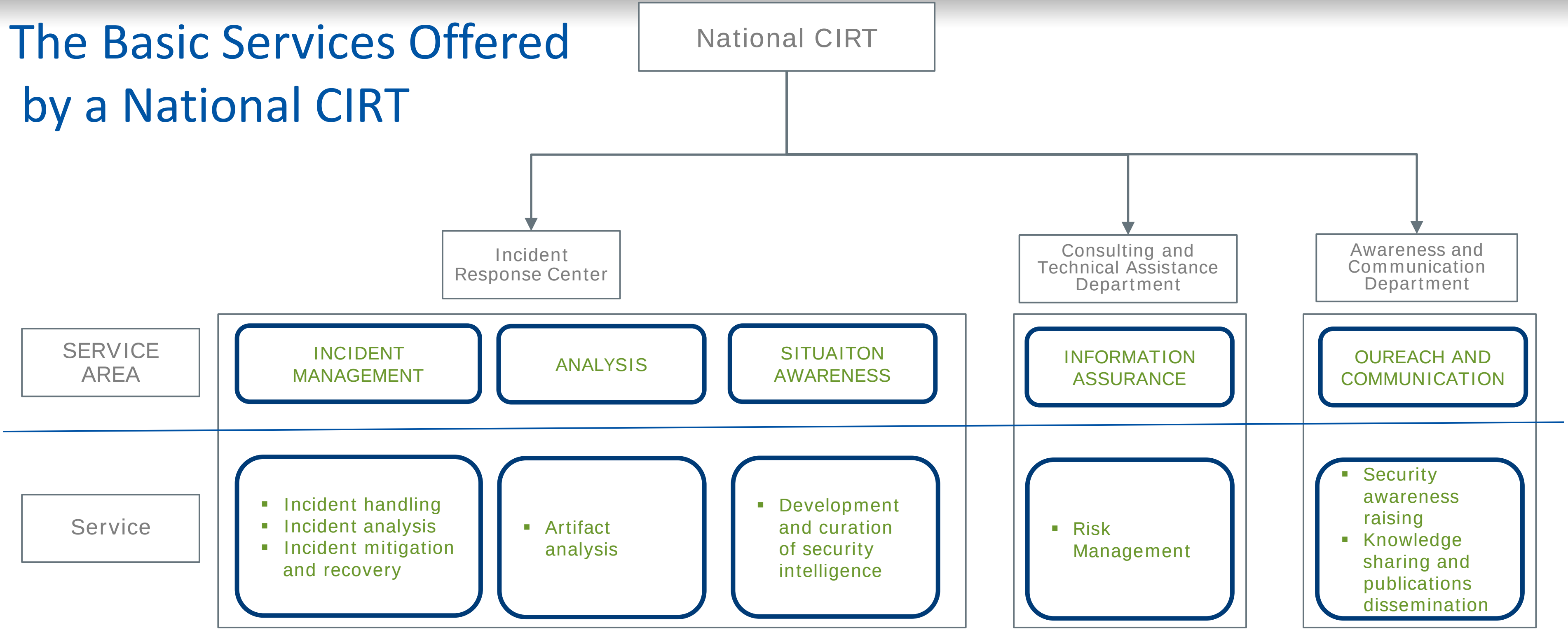
- Facilitate the development of a national CIIP strategy (CIIP)
- Assisting owners & operators of CII to mitigate their information risk
- Establish a trusted communication channel between all the stakeholders
- Provide early warning
- Coordination of incidents response at the National level
- Help CII to develop their own incident management capabilities.
- Testing and measuring CIIP maturity over time and guiding strategy based on measurement
- Promote National Culture of Cybersecurity

The Role of the national CIRT in the CIIP

The Six Phases of Critical information Infrastructure Protection (CIIP)



The Basic Services Offered by a National CIRT



National CIRT

Incident Response Center

Consulting and Technical Assistance Department

Awareness and Communication Department

SERVICE AREA

INCIDENT MANAGEMENT

ANALYSIS

SITUAITON AWARENESS

INFORMATION ASSURANCE

OUREACH AND COMMUNICATION

Service

- Incident handling
- Incident analysis
- Incident mitigation and recovery

- Artifact analysis

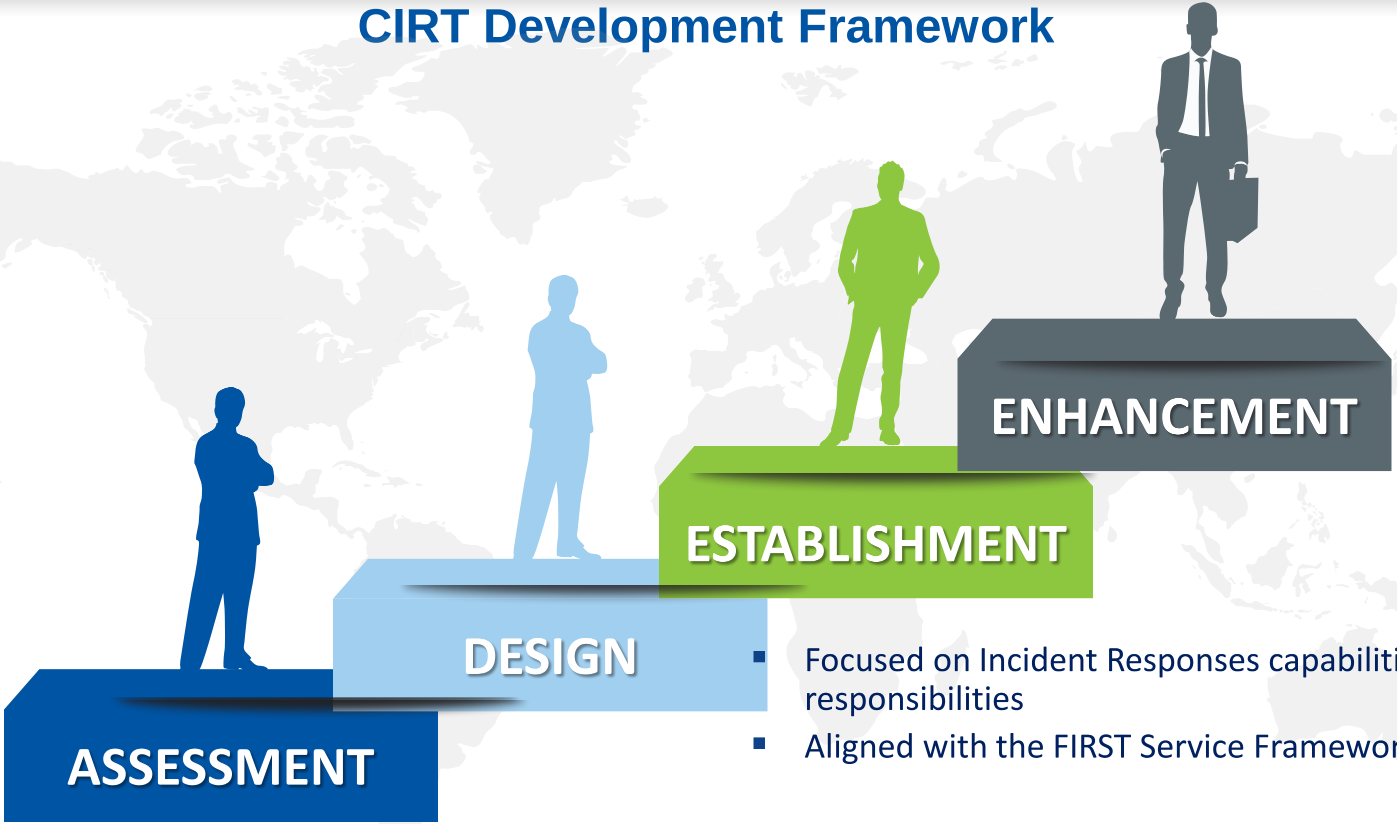
- Development and curation of security intelligence

- Risk Management

- Security awareness raising
- Knowledge sharing and publications dissemination

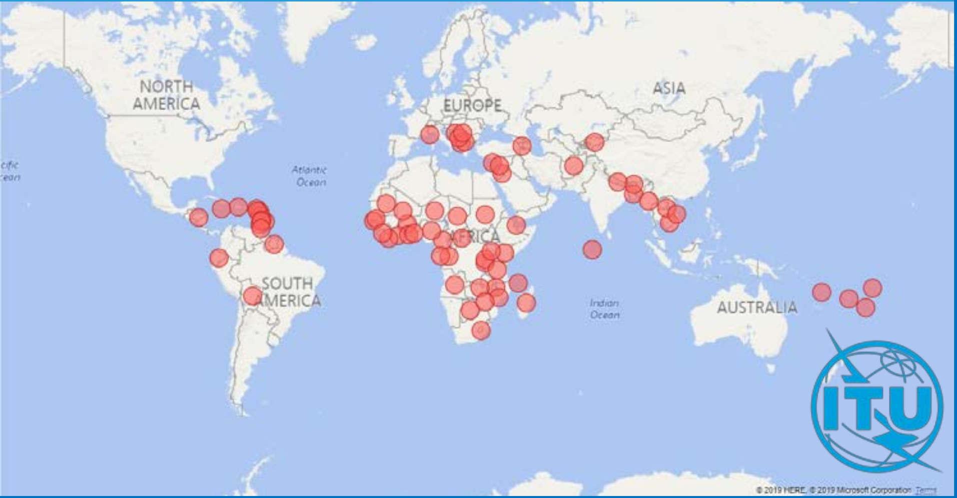
ITU CIRT Framework Activities

CIRT Development Framework

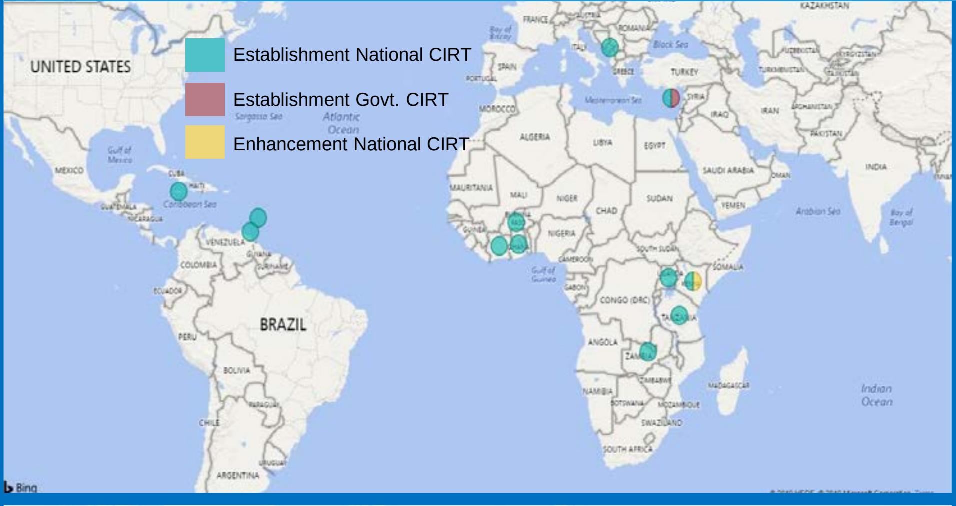


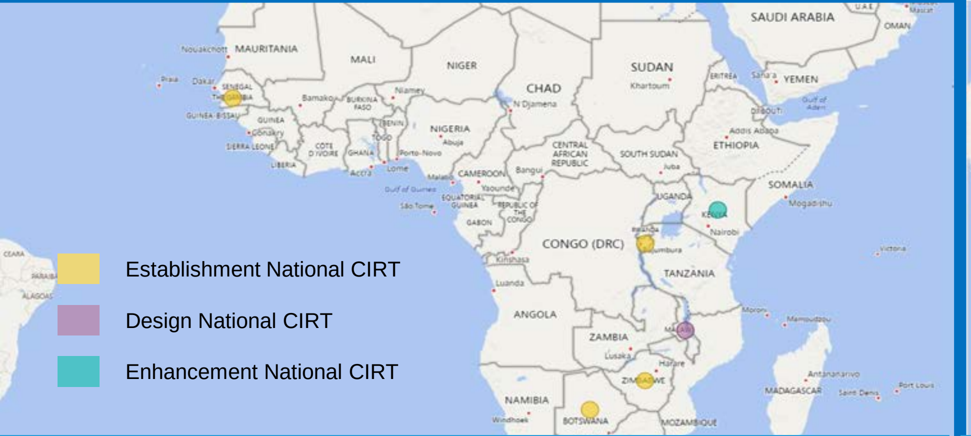
- Focused on Incident Responses capabilities with National responsibilities
- Aligned with the FIRST Service Framework

75 CIRT READINESS ASSESSMENTS

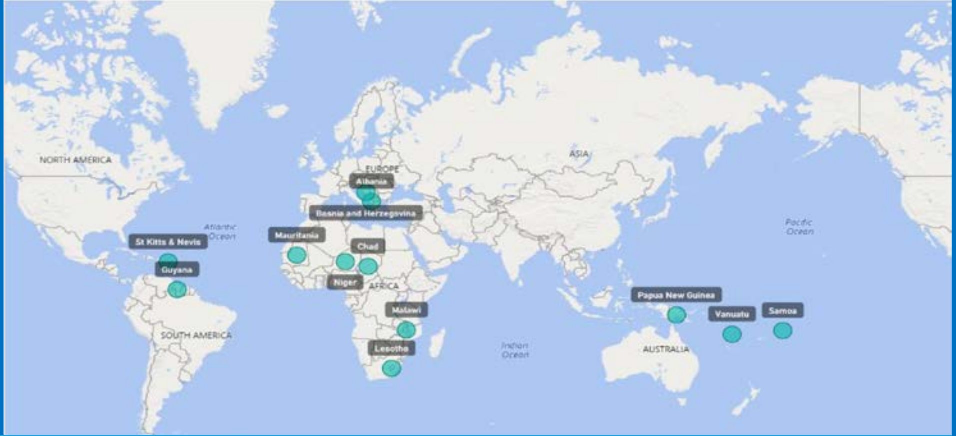


13 CIRT ESTABLISHMENT + 1 ENHANCEMENT





CIRT ESTBLISHMENT IN 2019

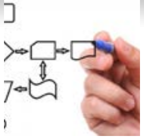


CIRT ESTABLISHMENT– INTERESTS

The Role of the Government in Tackling Cyber Threats

Establishment of sound policies, strategies and legislations and ensure their implementations

Establish organizational structures and define their roles



Develop and implement technical and procedural understandings and measures

Establish capacity development and awareness creation programs - from basics to advanced levels

Nurture Multi-stakeholder Cooperation on National, Regional and International levels

Ensure Sound Policy, Strategy and Legislative Measures

- Update the measures to meet the current and future changes.
- Ensure the policy makers follow and upgrade their knowledge with the trends.
- Update the laws to encompass changes in the area of cyber-crime and other related crimes.
- Follow the trends in law development in the region and on the international level

Establishment of Organizational Structures

Establish national organizations that will improve the posture of cybersecurity, such as National CIRT, GovCIRT and Sectoral CIRTs

- Conduct regular multi-stakeholder cybersecurity exercises targeting National Critical Infrastructures

Ensure checks and balances are in place and clear separation of duties established among organizations on cybersecurity

Establish clear definitions of roles and responsibilities

Develop and implement technical and procedural understandings and measures

Develop sound competency on technical and operating procedural measures

Maintain and update operating procedures to address current and future challenges

Use, develop and implement best practices related to various areas of expertise

Establish capacity development and awareness creation programs - from basics to advanced levels

Establish and implement a comprehensive awareness creation program for citizens, businesses and the government

Design a capacity development framework to develop national cybersecurity skills required for the future of the country

Ensure educational institutions establish educational programs on cyber crime laws, cybersecurity technical and policy skills – to drive human capacity development

Nurture Multi-stakeholder Cooperation on National, Regional and International levels

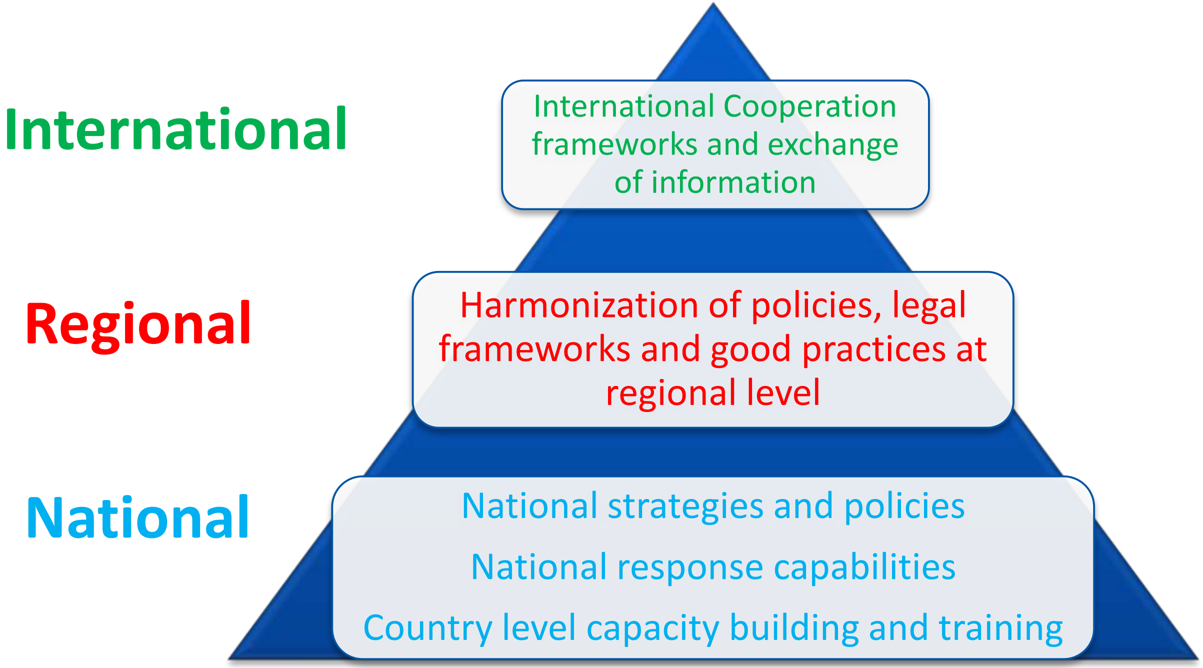
Develop an inclusive approach, invite all stake-holders to contribute through an open and inclusive discussion

Join multilateral or bilateral agreements to promote cooperation in the areas of cybersecurity, cyber-crime and capacity building

Ensure information sharing and cooperation at different levels

Conclusion: Coordinated Response

Need for a multi-level response to the cybersecurity challenges



International

International Cooperation frameworks and exchange of information

Regional

Harmonization of policies, legal frameworks and good practices at regional level

National

National strategies and policies

National response capabilities

Country level capacity building and training

Conclusion

- Emerging technologies create new vectors of potential risks and liabilities, including new threats to public safety, physical harm and catastrophic systemic attacks on shared public infrastructure.
- Cyberattacks on critical infrastructure may generate cascading effects resulting in economic loss, disruption of service provision and, in some cases, human casualties. When applied to civil aviation industry, the impact can be catastrophic.
- There is a need for establishing, adoption and catalyzing of appropriate security and risk mitigation frameworks and strategies that enable the safe, secure and continuous digital transformation of the critical sectors.
- Collaboration between the relevant stakeholders is a must to build the required levels of cyber-resilience understanding and governance.

Conclusion

- Building human capabilities and raising awareness are the key elements for building a culture of cybersecurity
- Enabling robust eco-system that is resilient to cyber threats is imperative in the digital age.
- Effective mechanisms and institutional structures at the national level are necessary to reliably deal with cyber threats and incidents.
- The absence of such institutions and lack of national capacities poses a genuine problem in adequately and effectively responding to cyber attacks. CIRT play an important role in the solution.
- ITU is working with Member States to build capacity at national and regional levels, deploy capabilities, and assist in establishing and enhancing CIRTs.

CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO

Thank You