Critical Information Infrastructure Protection

Role of CIRTs and Cooperation at National Level

18 September 2017

Key Aspects of Cybersecurity in the Context of Internet of Things (IoT)
Tashkent, Uzbekistan, 18-19 September 2017

About ITU

ITU is the United Nations **specialized agency for information and communication technologies** (ICTs)

Founded in Paris in 1865 as the International Telegraph Union

More than 150 years of experience and innovation

ITU Sectors

What we do

'Committed to Connecting the World'

3
Sectors

ITU Radiocommunication

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

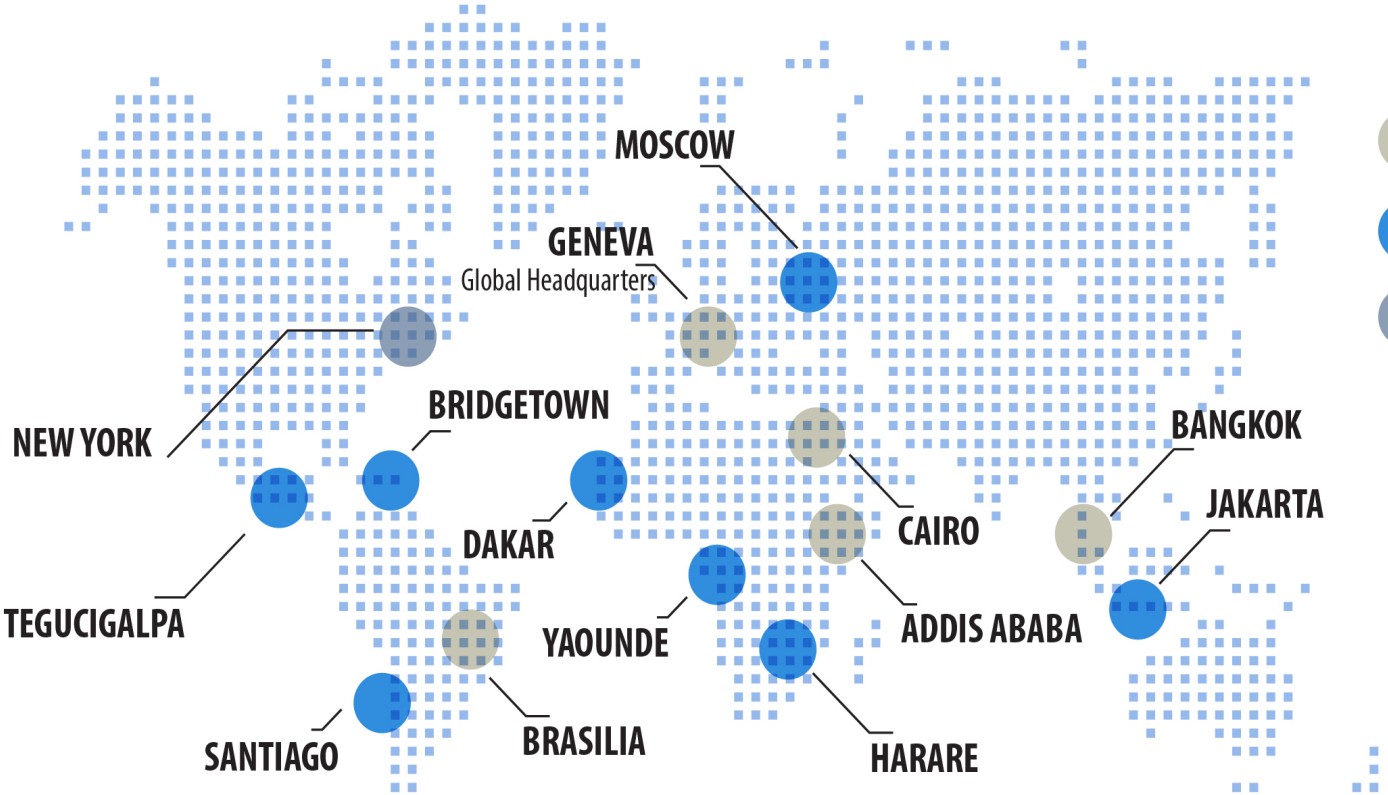
ITU Standardization

Establishing global standards

ITU Development

Bridging the digital divide

Global presence



5 regional offices

8 area offices

1 UN office

CELEBRATING 25 YEARS OF ACHIEVEMENTS

ITU members

ITUWTDC
BUENOS AIRES 2017
9-20 October

193

MEMBER STATES

+700

INDUSTRY & INTERNATIONAL ORGANIZATIONS

+150

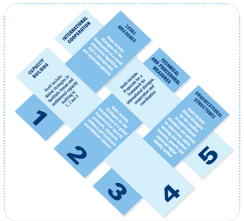
ACADEMIA MEMBERS

ITU-D 1992 2017
CELEBRATING 25 YEARS OF ACHIEVEMENTS

ITU Mandate on Cybersecurity

2003 – 2005
WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 - "**Building Confidence and Security in the use of ICTs**"

world summit on the information society
Geneva 2003 - Tunis 2005



2007
Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General
GCA is a **framework for international cooperation in cybersecurity**

2008 to date
ITU Membership endorsed the GCA as the ITU-wide strategy on international cooperation.

GCA GLOBAL CYBERSECURITY AGENDA

Child Online Protection

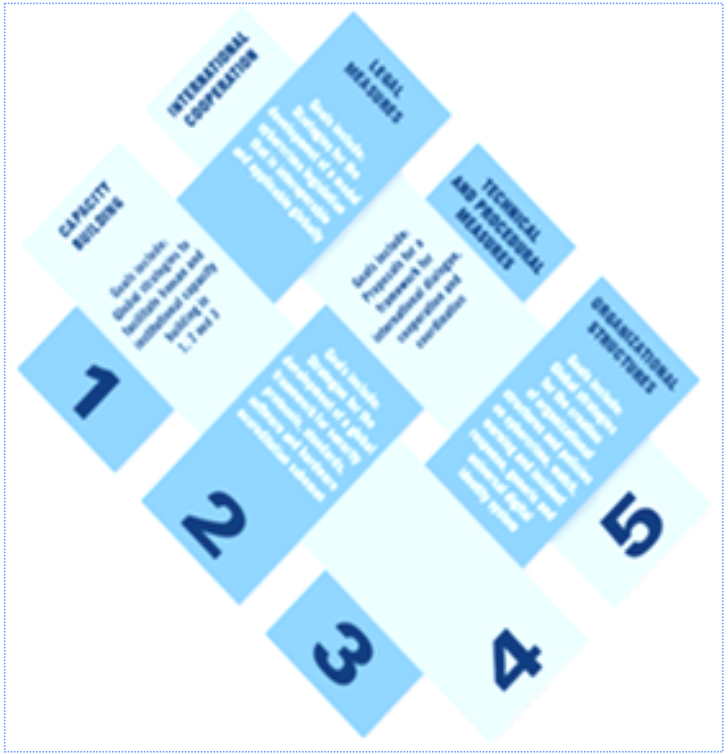
Building confidence and security in the use of ICTs is widely present in **PP and Conferences**' resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues, from legal to policy, to technical and organization measures.

ITUWTDC BUENOS AIRES 2017 9-20 October

ITU-D 1992 2017 CELEBRATING 25YEARS OF ACHIEVEMENTS

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.



BDT Cybersecurity Program

ITUWTDC
BUENOS AIRES 2017
9-20 October

6 Service areas – 18 Services

Engagement and awareness
- Global Cybersecurity Index
- Global, Regional and National events
- High-Level Cybersecurity Simulations
- Information Dissemination

National Cybersecurity Assistance
- National Cybersecurity Assessment
- National Cybersecurity Strategy support
- Critical Infrastructure Protection Support
- Technical Assistance

Computer Incident Response Team (CIRT) Program
- CIRT Assessment
- CIRT Design
- CIRT Establishmemt
- CIRT Improvement

Information sharing
- Best Practices Sharing
- Information Exchange Tools and Techniques

Cyber Drills
- Regional drills
- National drills

Human Capacity Building
- Curricula and Training Programs
- Bespoke Training

ITU-D 1992 2017
CELEBRATING 25YEARS OF ACHIEVEMENTS

Agenda

1. What Is National Critical Information Infrastructure?
2. Threats to National Critical Information Infrastructure
3. The Role of the national CIRT in the CIIP

Agenda

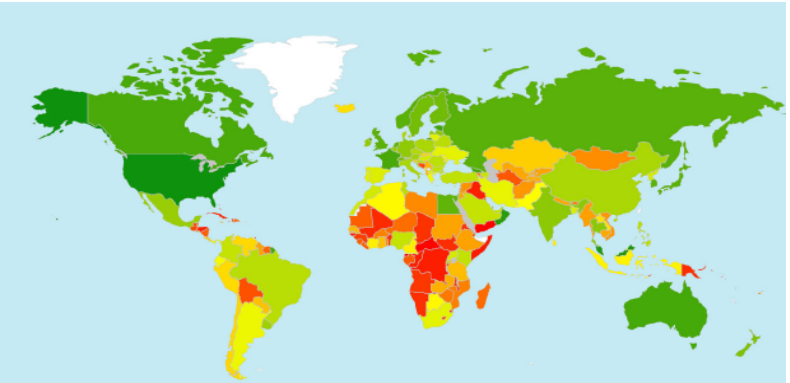
1. **What Is National Critical Information Infrastructure?**
2. Threats to National Critical Information Infrastructure
3. The Role of the national CIRT in the CIIP

What Is Critical National Infrastructure?

ITUWTDC
BUENOS AIRES 2017
9-20 October

Global Cybersecurity Index 2017
Top three ranked countries in the Word

Member State	Score	Global Rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3



Source : Global Cybersecurity Index (GCI) 2017
www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspxITU

ITU-D 1992 2017
CELEBRATING 25 YEARS OF ACHIEVEMENTS

What Is National Critical Information Infrastructure?

Singapore

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 -

sectors

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

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:

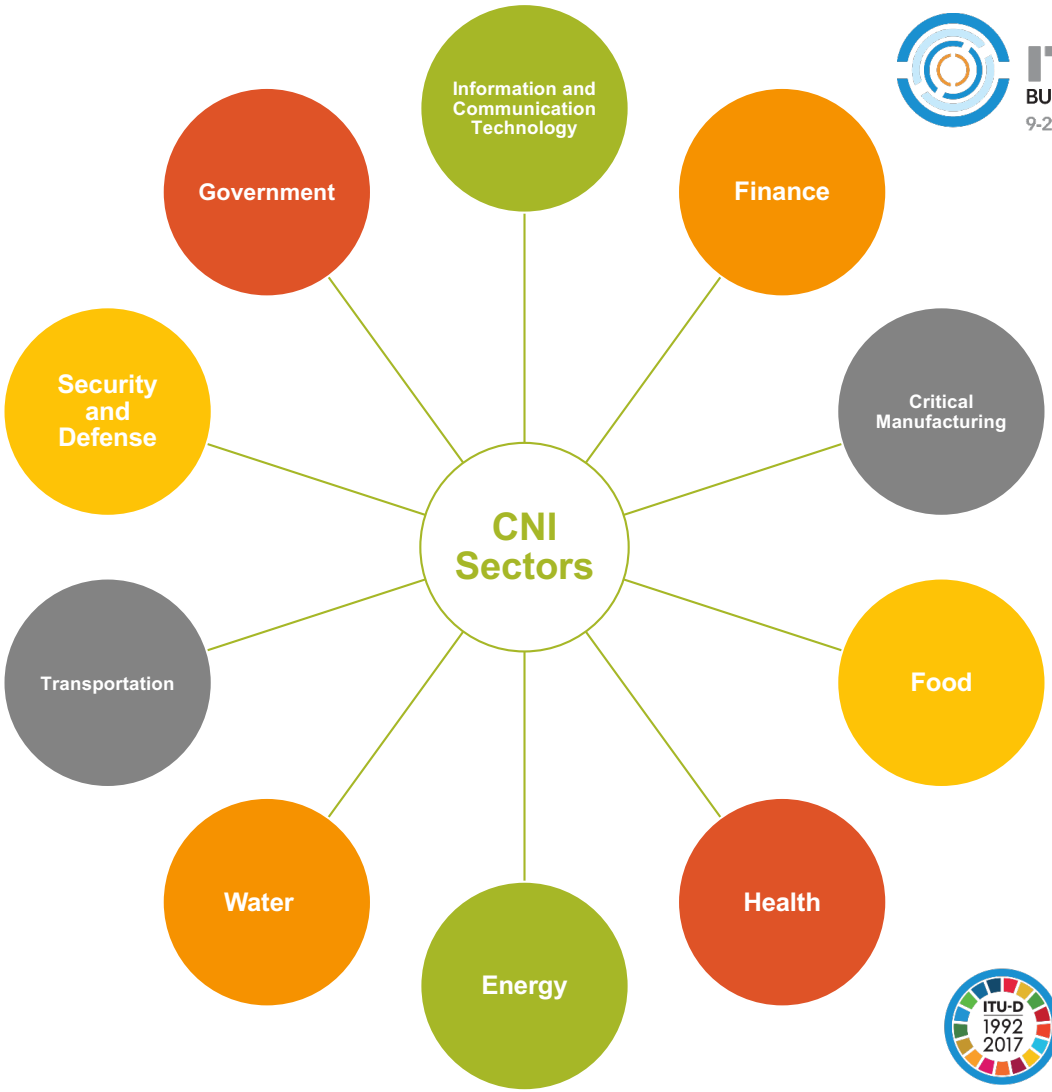
"Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on:

- 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."

CyberSecurity Malaysia - Malaysia -

sectors

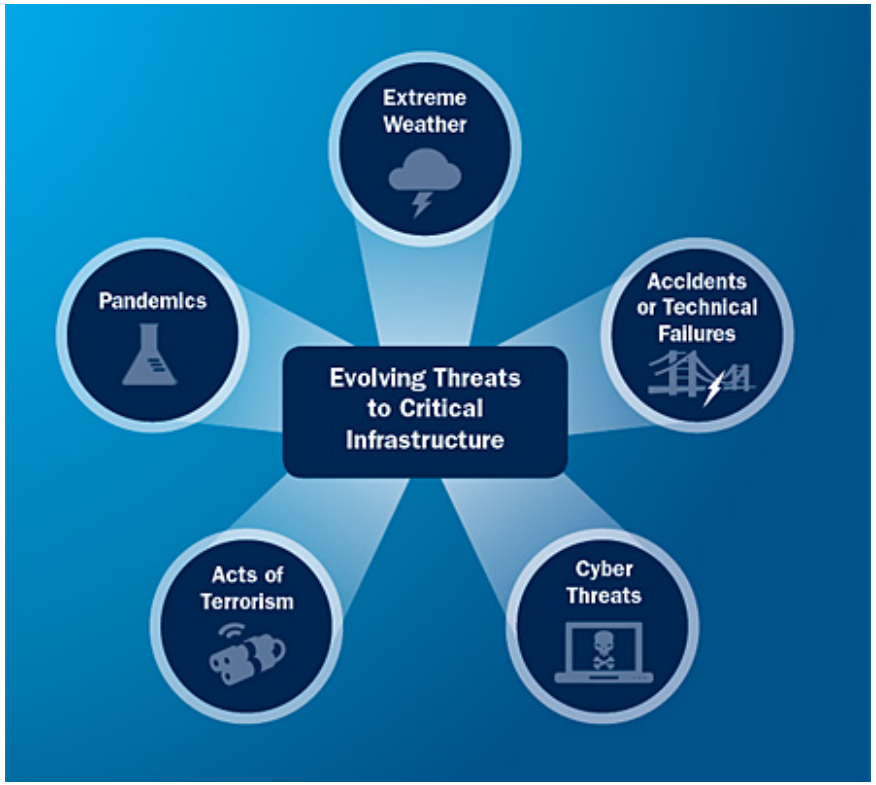
In General, we can identify 10 Critical National Infrastructure sectors :



Agenda

1. What Is National Critical Information Infrastructure?
2. **Threats to National Critical Information Infrastructure**
3. The Role of the national CIRT in the CIIP

Threats to Critical National Infrastructure



Source : https://emilms.fema.gov

Threats to Critical National Infrastructure

ITUWTDC BUENOS AIRES 2017 9-20 October

Mirai Botnet (未来)

September and October 2016

Octave Klaba
@olesovhcom
Follow

Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the
simultaneous DDoS are close to 1Tbps !

```
log /home/vac/logs/vac.log-last | egrep "pps\|.........
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

10:37 PM - 21 Sep 2016

705 Retweets **586** Likes

The Telegraph

Unprecedented cyber attack takes Liberia's entire internet down

share

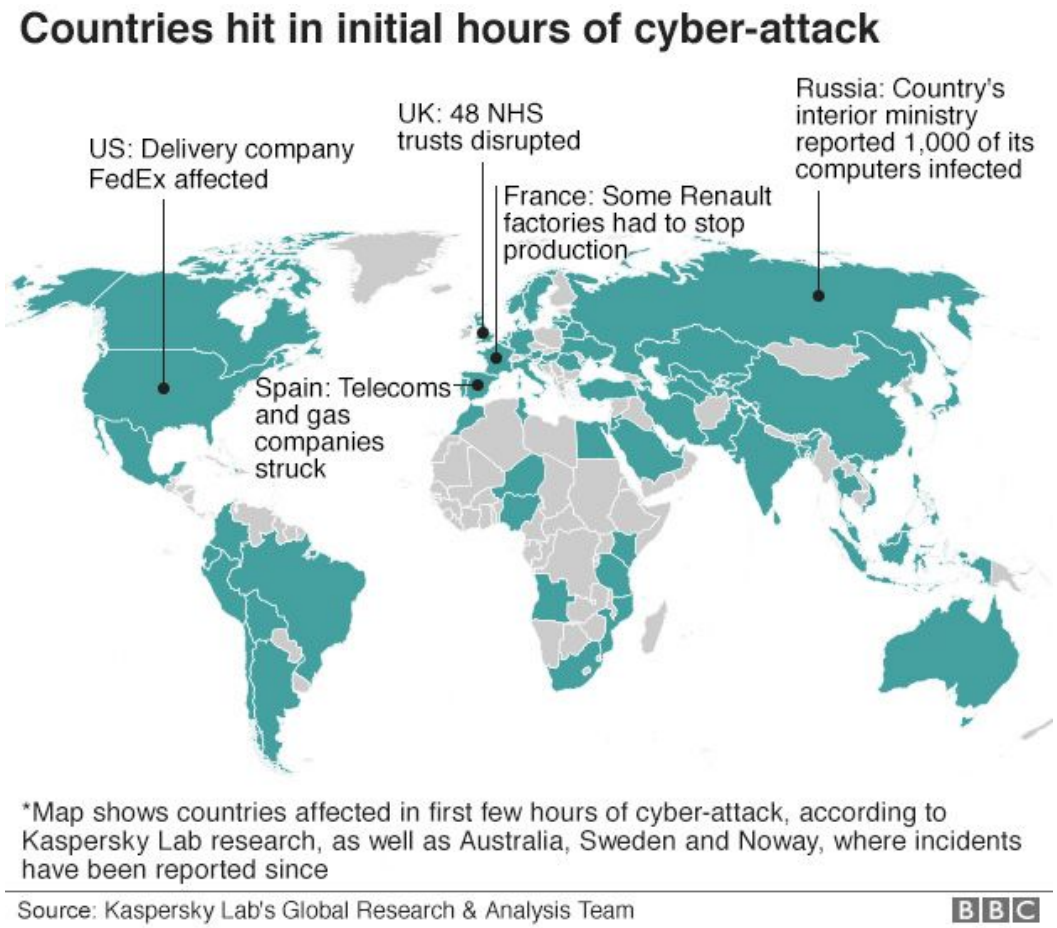
An unprecedented cyber attack has knocked Liberia's internet offline, as hackers targeted the nation's infrastructure using the same method that shut down hundreds of the world's most popular websites at the end of last month.

The attack, which is the same used to shut off sites including Netflix, eBay and Reddit, fuels fears that cyber criminals are practicing ways to sabotage the US' internet when the country heads to the polls on November 8.

Multiple attacks against Liberia's rudimentary internet infrastructure have have intermittently taken the country's websites offline over the course of a week. Although it isn't clear who was behind either attack, experts said the method used was simple enough to have been launched by a lone actor and that it appeared to have come from the same source.

Threats to Critical National Infrastructure

WannaCry ransomware
May 2017



Threats to Critical National Infrastructure

ITUWTDC BUENOS AIRES 2017 9-20 October

WannaCry ransomware

May 2017

East and North Hertfordshire NHS
NHS Trust

Patients & Visitors | GPs & Professionals | Member Area | Our Hospitals | About The Trust | Get Involved | News & Media

You are here: SEARCH

Our Hospitals
- Hertford County
- Lister
- Mount Vernon Cancer Centre
- New QEII

Care Quality Commission

East and North Hertfordshire NHS Trust

CQC overall rating

Requires improvement

5 April 2016

See the report ›

Quick Links
- A&E / Emergency department
- Visiting times
- Cancel/change your appointment
- Maternity services liaison committee
- Work for us

We're currently experiencing significant problems with our IT and telephone network

Which we're trying to resolve as soon as possible

This means that people will have difficulty phoning us for the time being – please bear with us. Apologies for any inconvenience.

Our Services

Our staff work hard to deliver the best quality of care to all our patients in the wide range of services we offer.
- A-Z of services
- Blood tests
- Maternity
- Outpatient appointments
- Radiology

Work for us

Our Trust has an exciting future. Be part of something special - join our team.

Find out more about working for us or view our latest vacancies.

We also have a dedicated page just for our nursing and midwifery vacancies.

Why Choose Us?

We provide good quality healthcare to our local community and beyond.
- Good transport links
- Improving patient experience

Belfast Telegraph DIGITAL

HOME | NEWS | SPORT | BUSINESS | ENTERTAINMENT | LIFE | CARS | OPINION | TRA

Northern Ireland | UK & World | Brexit | Technology | Jobs | Food, Drink and Hospitality | Agri

Home › Business › Technology

NHS cyber attack: Ransomware hackers force hospitals across England to divert emergency patients as incident spreads to Scotland

ITU-D 1992 2017 CELEBRATING 25 YEARS OF ACHIEVEMENTS

Threats to Critical National Infrastructure

WannaCry ransomware
May 2017

How it works

In most cases of infection, attackers send spam emails disguised as being work-related, with a link pointing to a malicious site. Unsuspecting victims click on the link.

As the link loads, the malicious site hosting the exploit kit starts to communicate with the victim's computer.

When the exploit kit finds a vulnerability in the victim's computer, it pushes down a malicious .exe file.

Once installed, the ransomware deletes existing backup system files, limiting the victims' ability to perform any system recovery.

It creates copies of the malware in three folders including AppData, Start menu and root directory to make sure the malware restarts upon reboot.

Then it searches for files with specific extensions and starts to encrypt these files. It is able to encrypt more than 100 types of files.

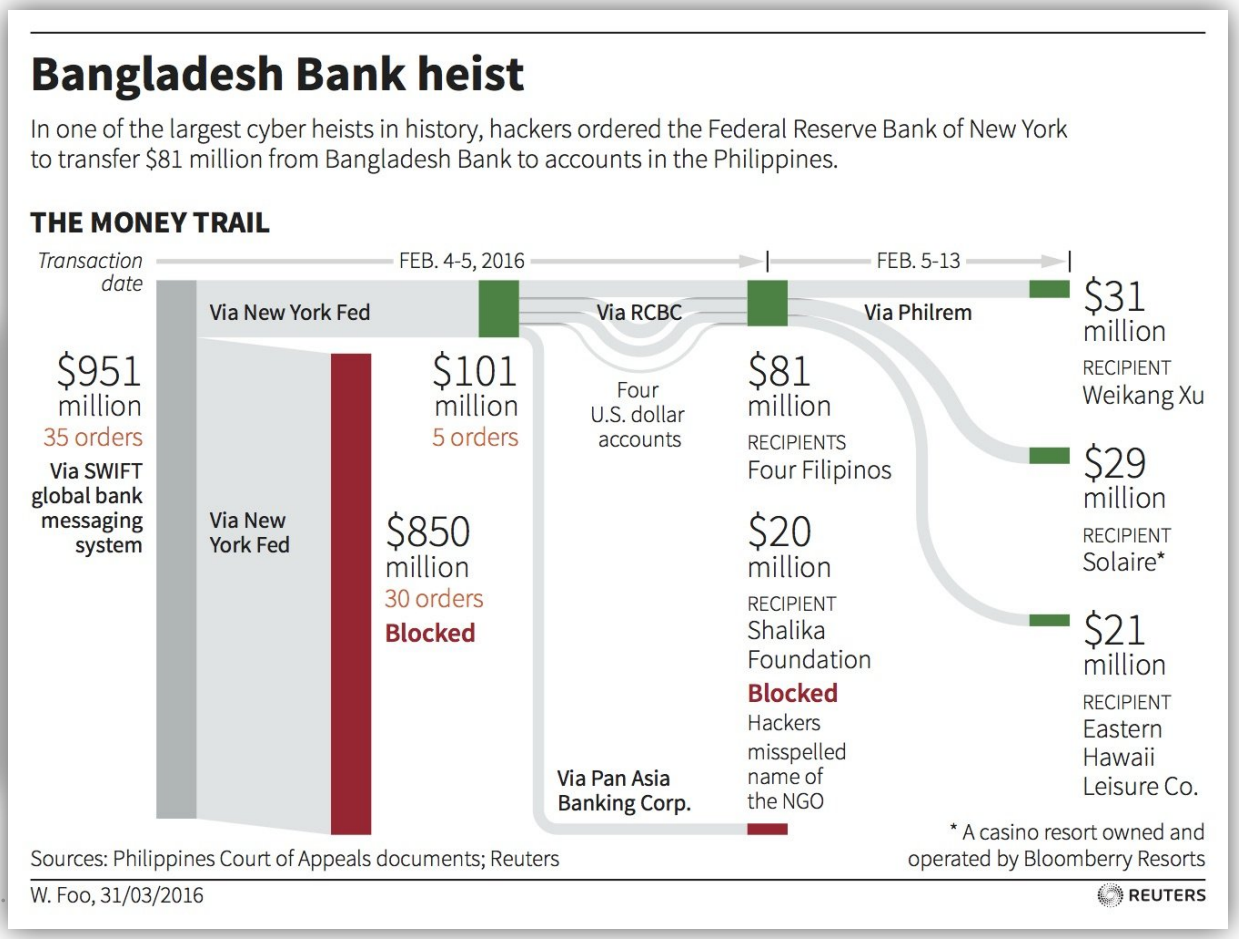
After encryption is finished, the malware sends the encryption key and other infomation to the malicious site.

The victim then gets a ransom message demanding payment in untrackable bitcoins. The note also indicates the amount will be doubled after three days.

Threats to Critical National Infrastructure

Bangladesh Bank

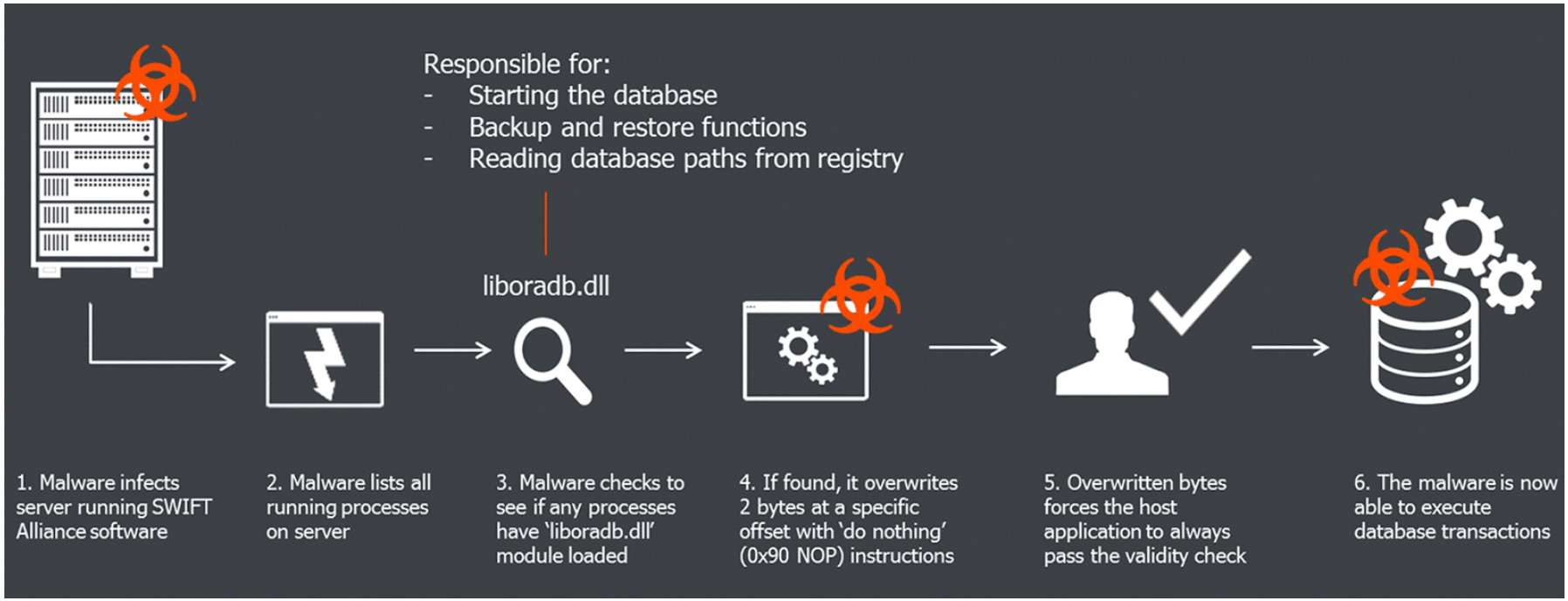
4 February 2016



Threats to Critical National Infrastructure

Bangladesh Bank

4 February 2016



Source : BAE Systems

Threats to Critical National Infrastructure

ITUWTDC
BUENOS AIRES 2017
9-20 October

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

BBC | Sign in | News | Sport | Weather | Shop | Earth

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Enterta

Technology

Hackers hit San Francisco transport systems

ITU-D 1992 2017
CELEBRATING 25 YEARS OF ACHIEVEMENTS

Threats to Critical National Infrastructure

Kiev's power grid
December 2016

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Ar

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 | Technology

Share

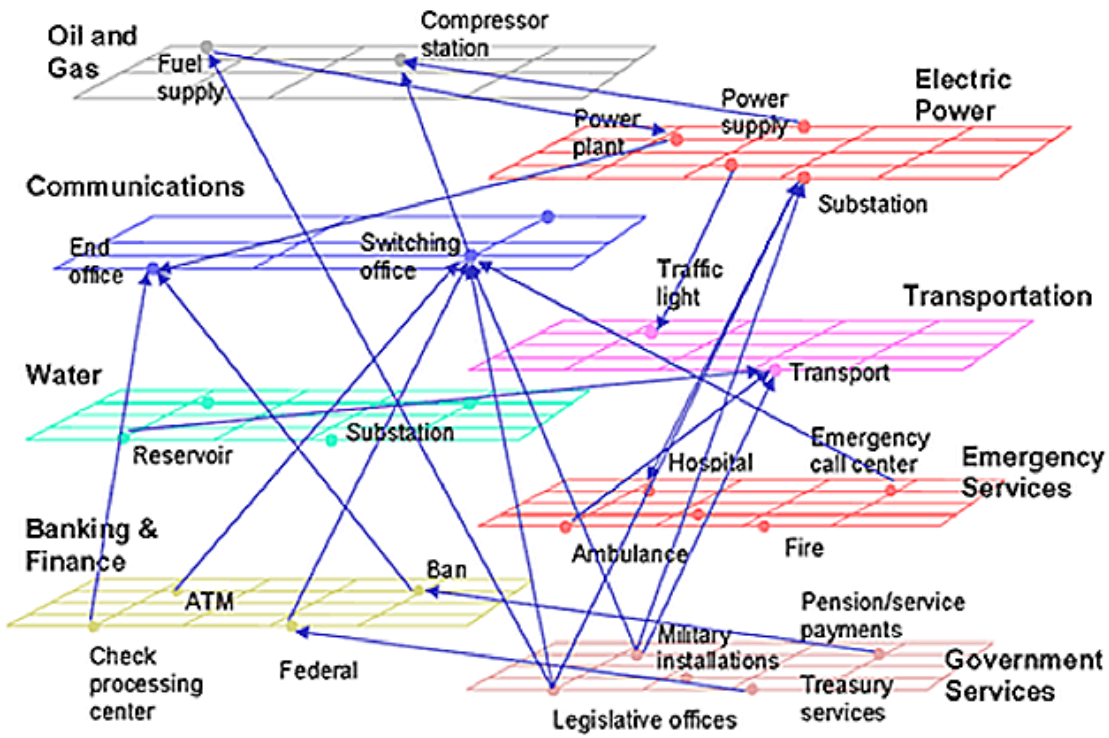
REUTERS

Ukraine's energy grid has been attacked twice by hackers

A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

Threats to Critical National Infrastructure



Cascade effect

Source : NSA

Interconnected Nature of Critical Infrastructure

CNN Money International + Markets Economy Companies Tech Autos India Video

Natural disasters caused $175 billion in damage in 2016

by Charles Riley @CRrileyCNN

January 4, 2017: 7:45 AM ET

Cybercrime costs the global economy $450 billion: CEO

Luke Graham | @LukeWGraham

Published 10:00 AM ET Tue, 7 Feb 2017

CNBC

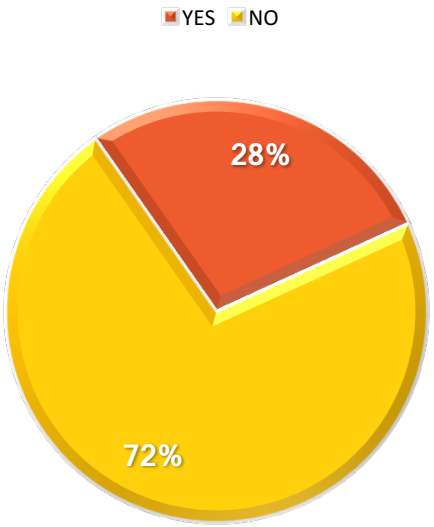
In 2016 "cybercrime cost the global economy over $450 billion, over 2 billion personal records were stolen and in the U.S. alone over 100 million Americans had their medical records stolen," said Steve Langan, chief executive at Hiscox Insurance, told CNBC.

Agenda

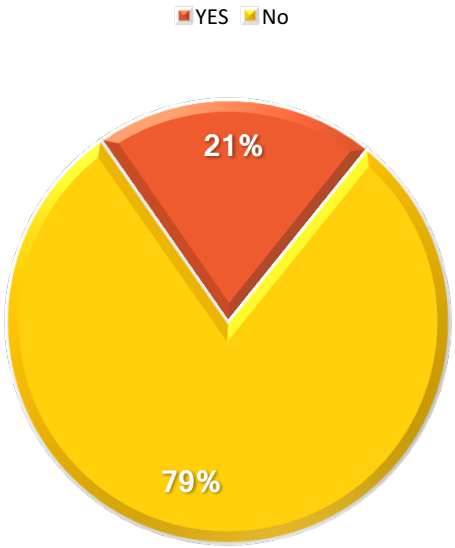
1. What Is National Critical Information Infrastructure?
2. Threats to National Critical Information Infrastructure
3. **The Role of the national CIRT in the CIIP**

CIRT The Role of the national CIRT in the CIIP

Key findings of GCI 2017 on CIIP
(LEGAL)



Does the legislation or regulation impose the implementation of cybersecurity measures on the critical infrastructure operators?

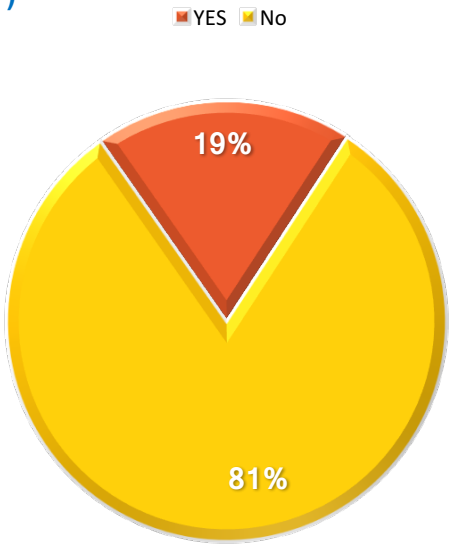


Does the legislation or regulation impose cybersecurity audits on the critical infrastructure operators ?

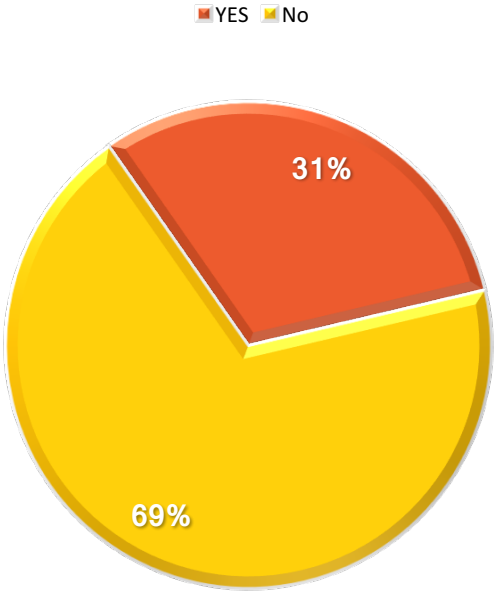
Source : Global Cybersecurity Index (GCI) 2017
www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspxITU

CIRT The Role of the national CIRT in the CIIP

Key findings of GCI 2017 on CIIP
(ORGANIZATIONAL)



Does national cybersecurity strategy include a national resilience plan ?

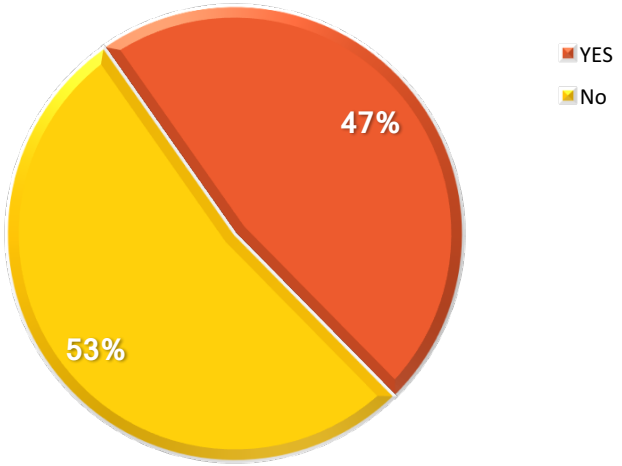


In the national strategy for cybersecurity , Is there a section on the protection of critical information infrastructure?

Source : Global Cybersecurity Index (GCI) 2017
www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspxITU

CIRT The Role of the national CIRT in the CIIP

Key findings of GCI 2017 on CIIP
(ORGANIZATIONAL)



Do you have an responsible agency responsible for critical information infrastructure protection?

- **Governments** are responsible for the country's overall security, public safety, the effective functioning of the economy, and the continuity of government services in case of an emergency or crisis

➔ **Government has responsibility to lead**

- **Private Sector** Most of the critical infrastructures are administered by the private sector operators

- The CIIP is the **SHARED** responsibility of both public and private organisations who develop, own, provide, manage and/or use this critical infrastructure.

Source : Global Cybersecurity Index (GCI) 2017
www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspxITU

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

CIRT The Role of the national CIRT in the CIIP

What is a National CIRT?

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.

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.

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.

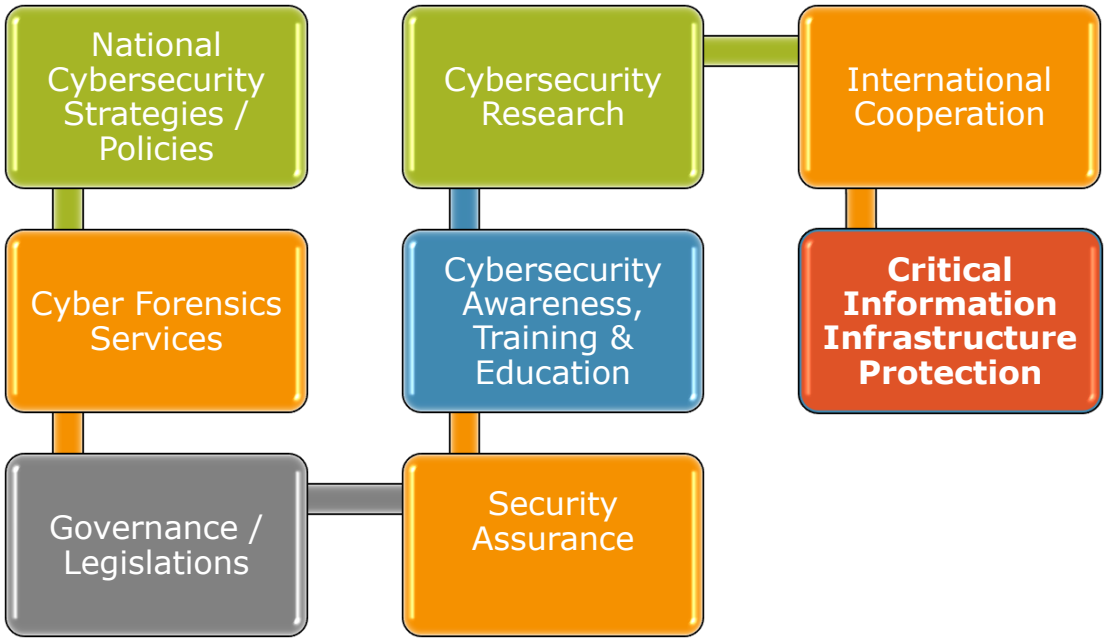
CIRT The Role of the national CIRT in the CIIP

Basic Services of a National CIRT

Incident Management	ANALYSIS	SITUATIONAL AWARENESS	INFORMATION ASSURANCE	Outreach/Communications
• Incident Handling • Incident Analysis • Incident Mitigation And Recovery	• ARTIFACT ANALYSIS	• DEVELOPMENT AND CURATION OF SECURITY INTELLIGENCE	• Risk Management • Technical Security Support	Security Awareness Raising Knowledge Sharing and Publications Dissemination

CIRT The Role of the national CIRT in the CIIP

National CIRT as enabler



CIRT The Role of the national CIRT in the CIIP

The Six Phases of Critical information Infrastructure Protection (CIIP)

CIRT The Role of the national CIRT in the CIIP

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

THANK YOU