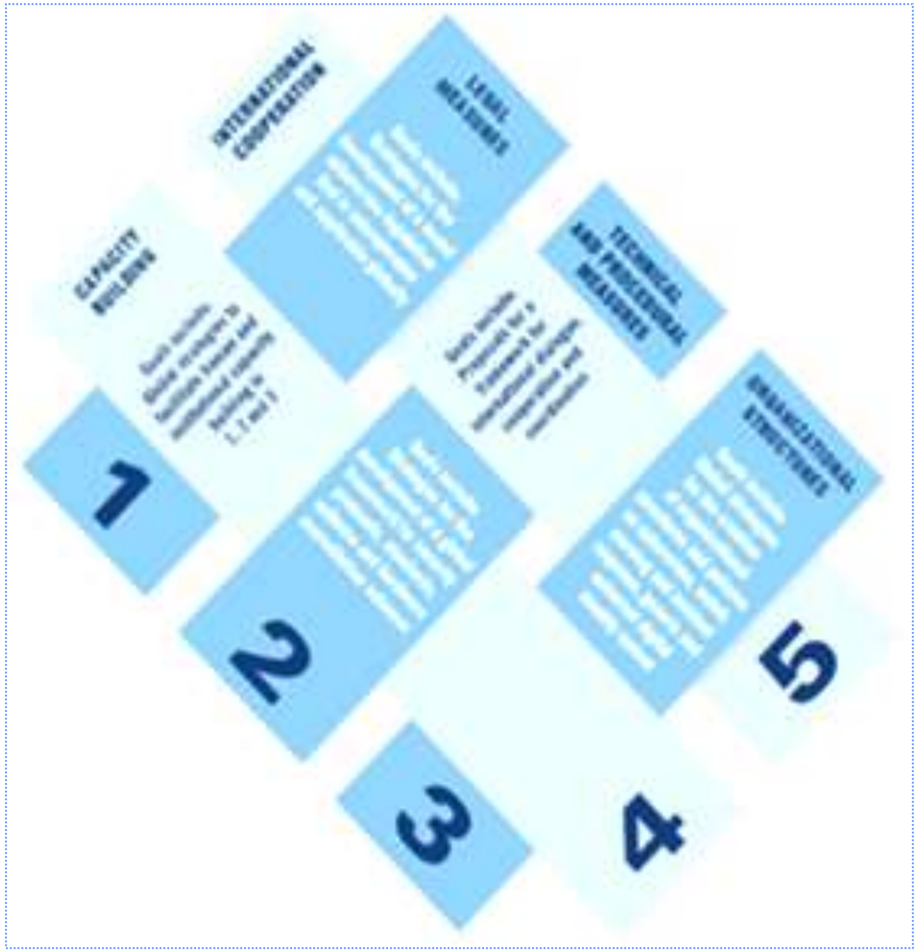
Critical Information Infrastructure Protection

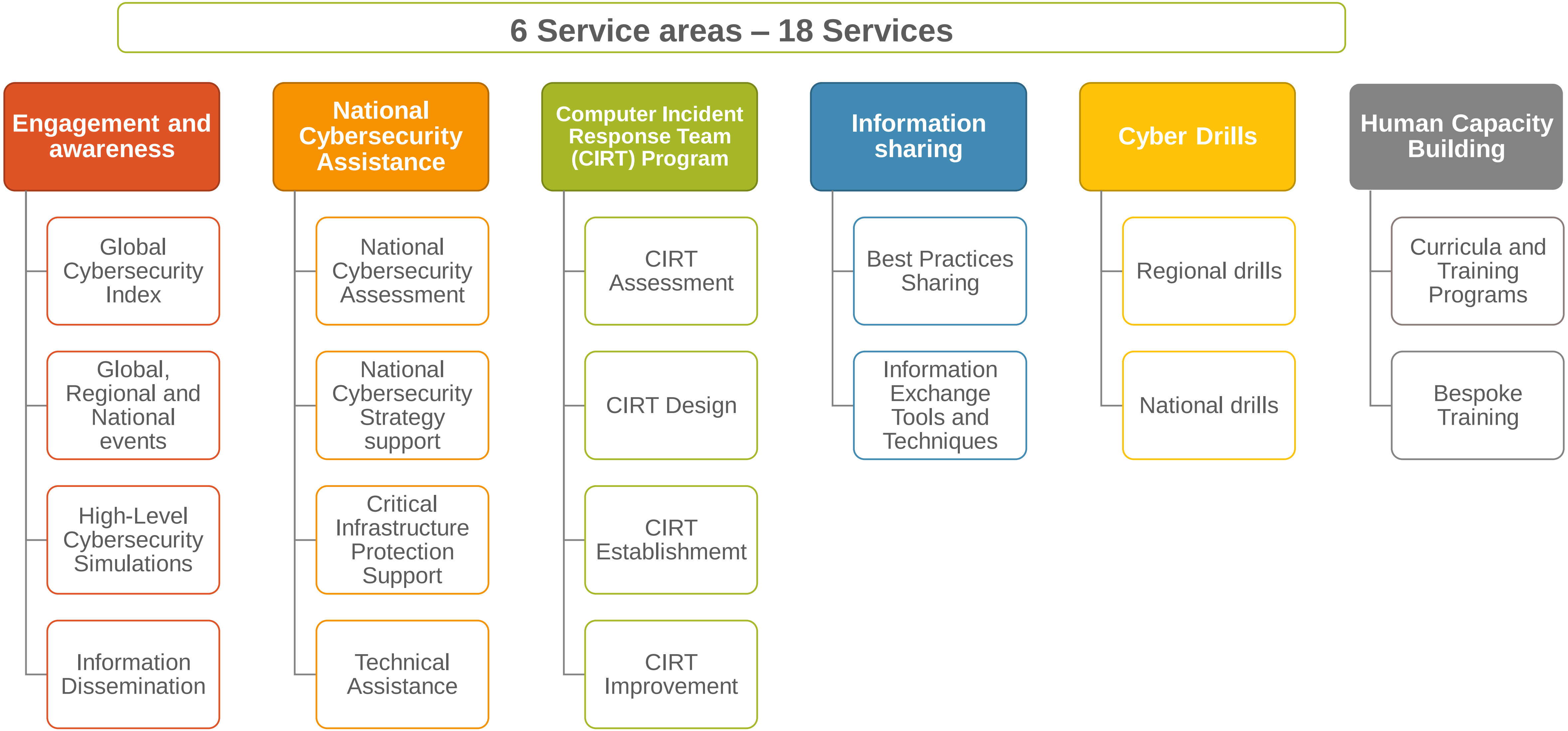
Role of CIRTs and Cooperation at National Level

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

BDT Cybersecurity Program



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's Standardization Sector

Economic Impact of Standardization

Adds 0.3% - 1% to the GDP

Source: European Commission

ITU-T Study Group 17 – Security

- **Over 300 standards** (ITU-T Recommendations) for security
  - **Rec. ITU-T X.509** for electronic authentication over public networks; a cornerstone in designing applications relating to PKI; used in a wide range of applications including providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system
  - **ITU-T X.1500-series** on cybersecurity information exchange
  - **ITU-T X.1600-series** cloud computing security
  - **ITU-T X.1140-X.1150-series**: access control/authentication
  - **ITU-T X.1080-series**: telebiometrics
- Key areas of current work:
  - Telecommunication/ICT Security
  - Cyberspace security
  - Application Security: Internet of Things, web services, cloud computing, Big Data, Intelligent Transport System
  - Identity management and authentication
  - Child Online Protection

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**

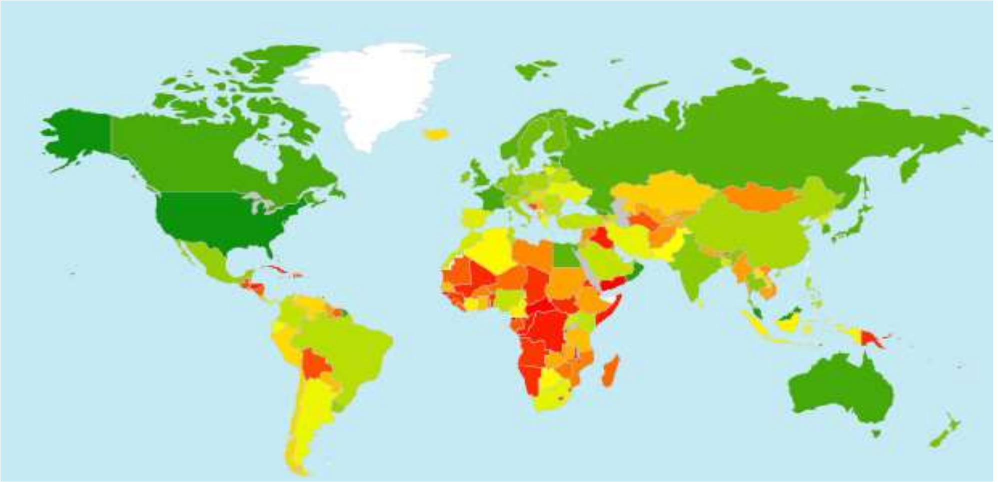
Agenda

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

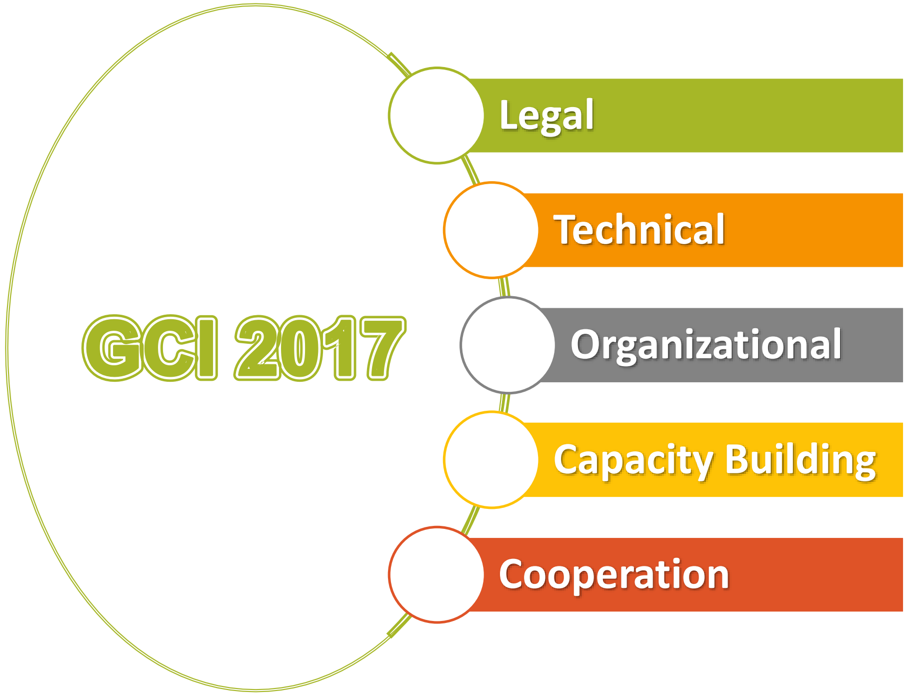
What Is Critical National Infrastructure?

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

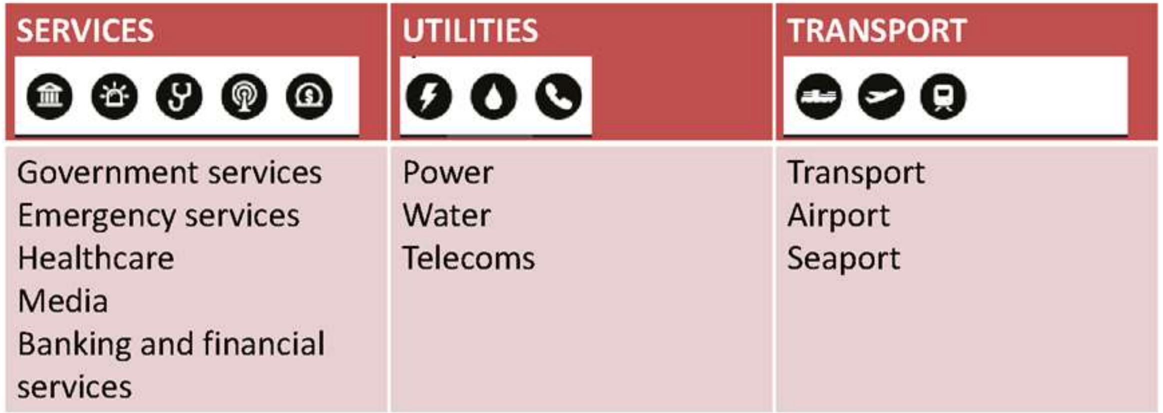


What Is National Critical Information Infrastructure?

Singapore

sectors

Definition of Critical National Infrastructure:

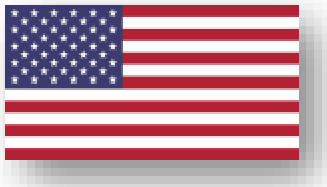


SERVICES	UTILITIES	TRANSPORT
Government services	Power	Transport
Emergency services	Water	Airport
Healthcare	Telecoms	Seaport
Media		
Banking and financial services		

"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."

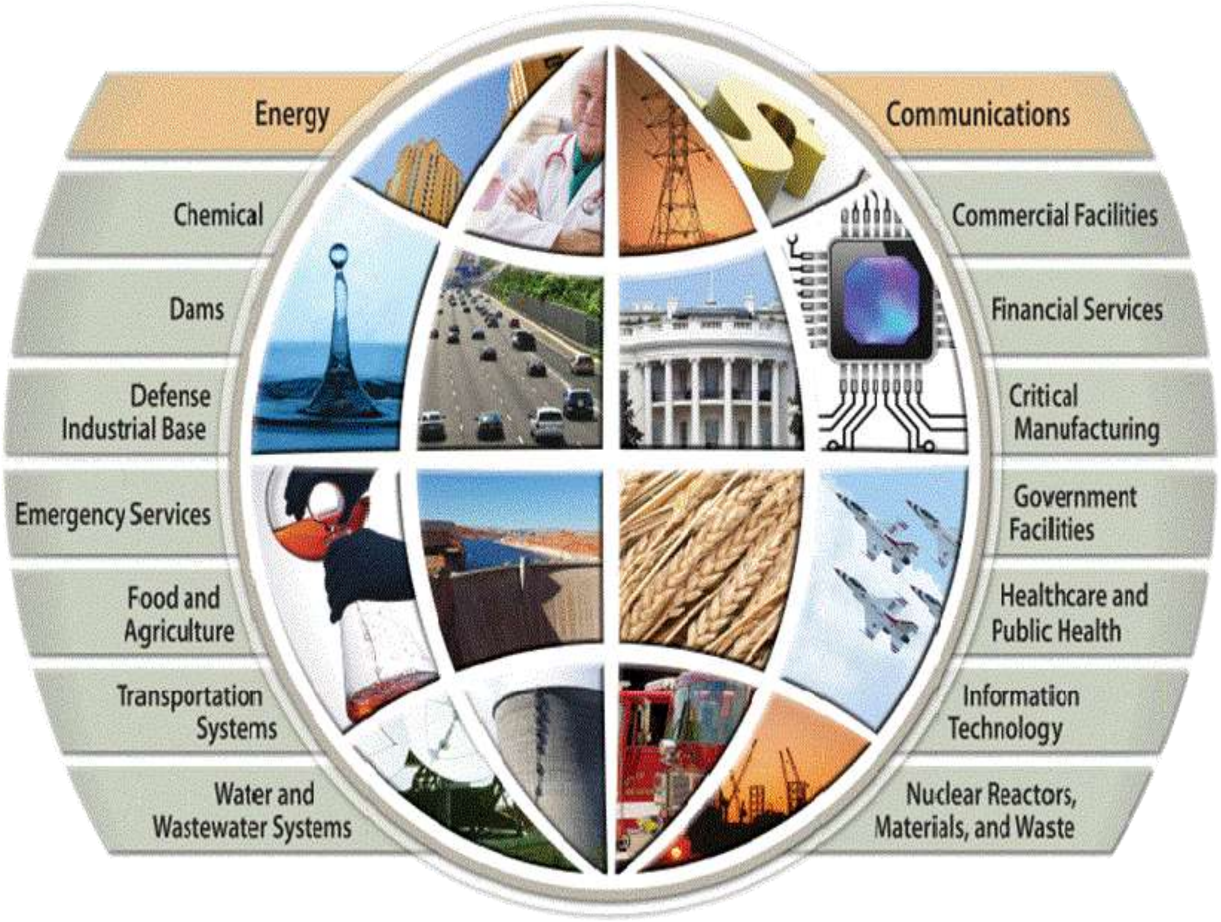
The Cyber Security Agency of Singapore (CSA) - Singapore -

What Is Critical National Infrastructure?



The United States of America

sectors

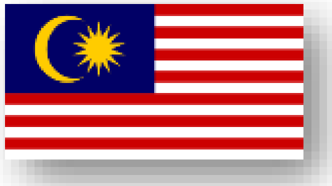


Definition of Critical National Infrastructure:

“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.”

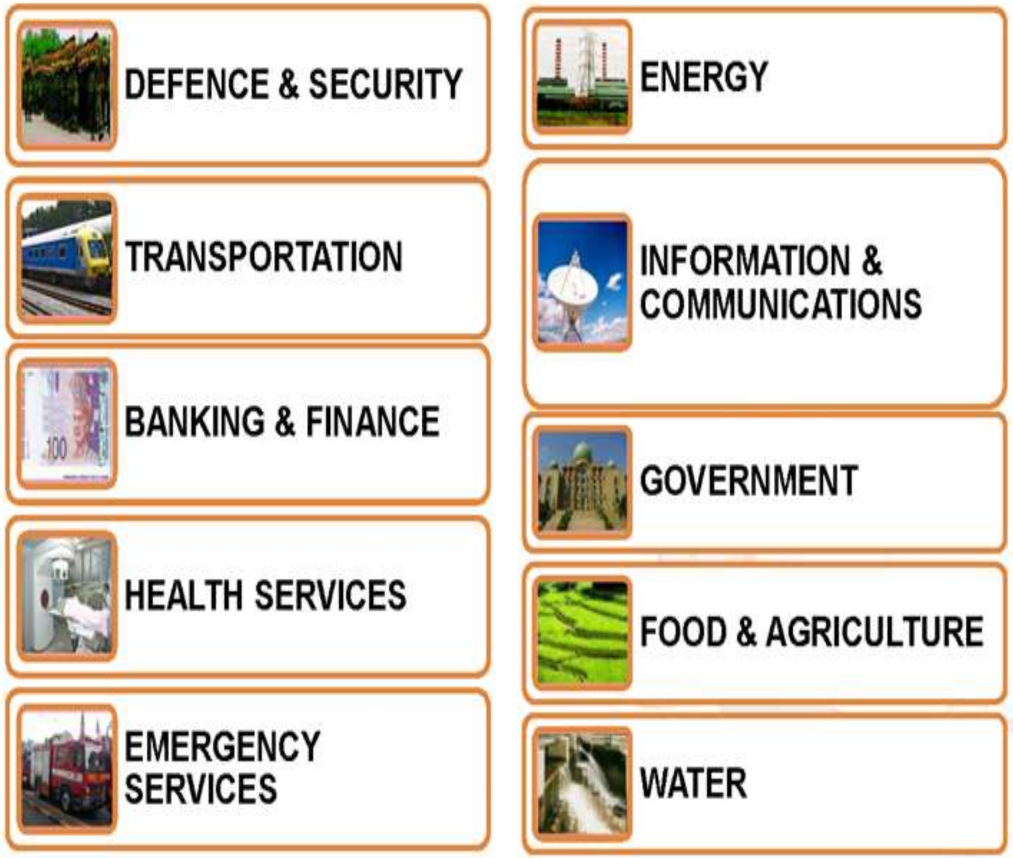
Department of Homeland Security -USA-

What Is Critical National Infrastructure?



Malaysia

sectors



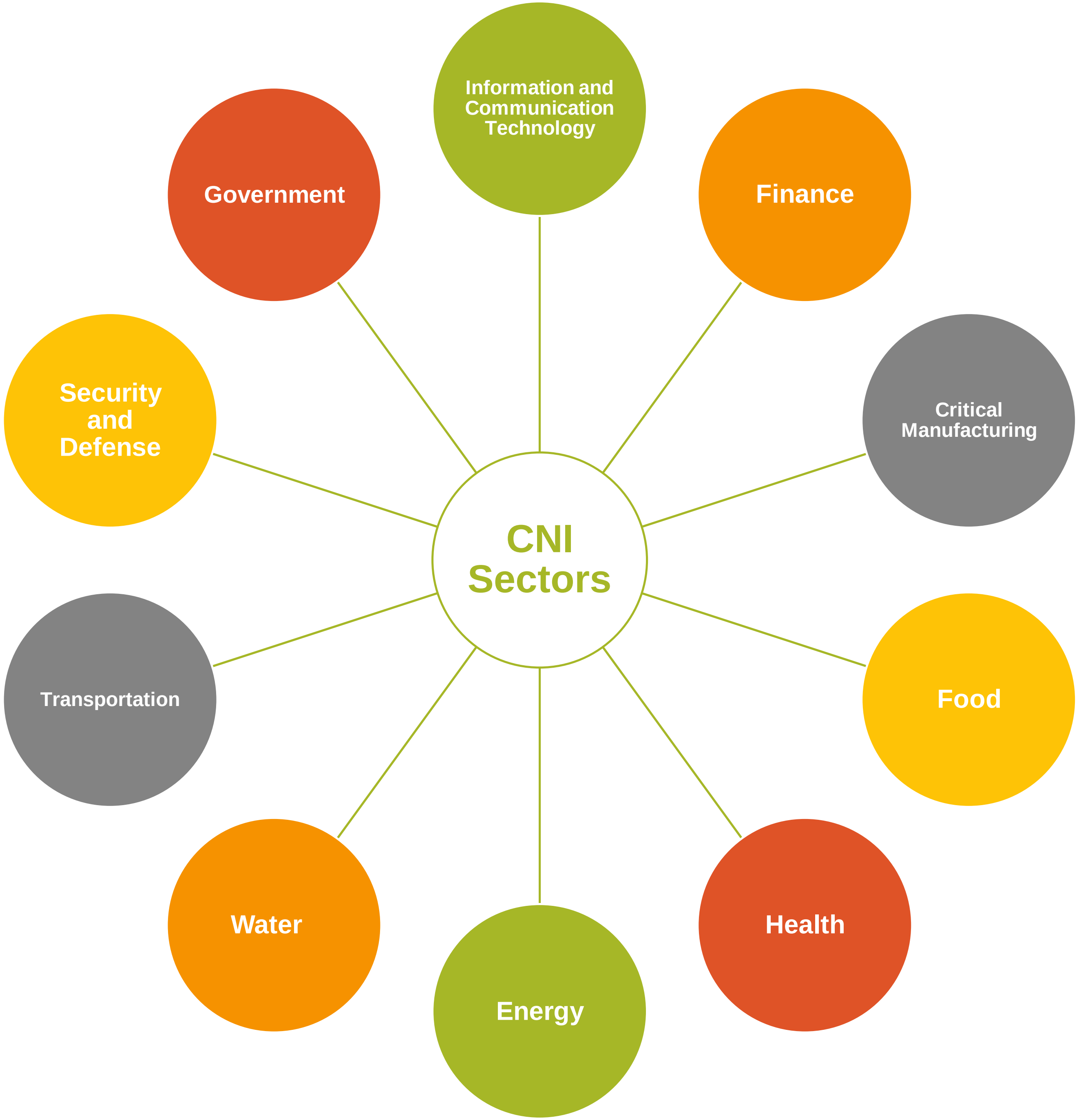
Definition of Critical National Infrastructure:

“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 -

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

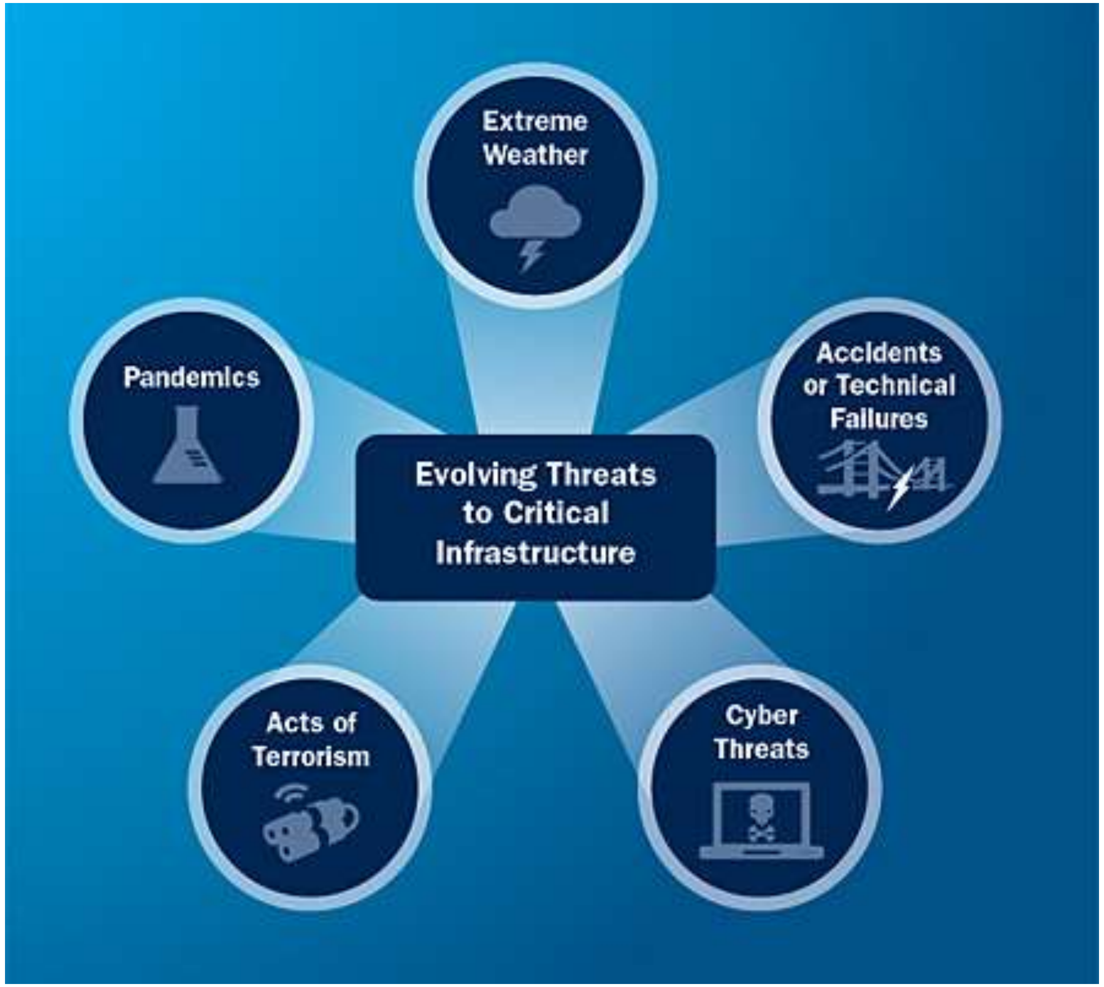
Agenda

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

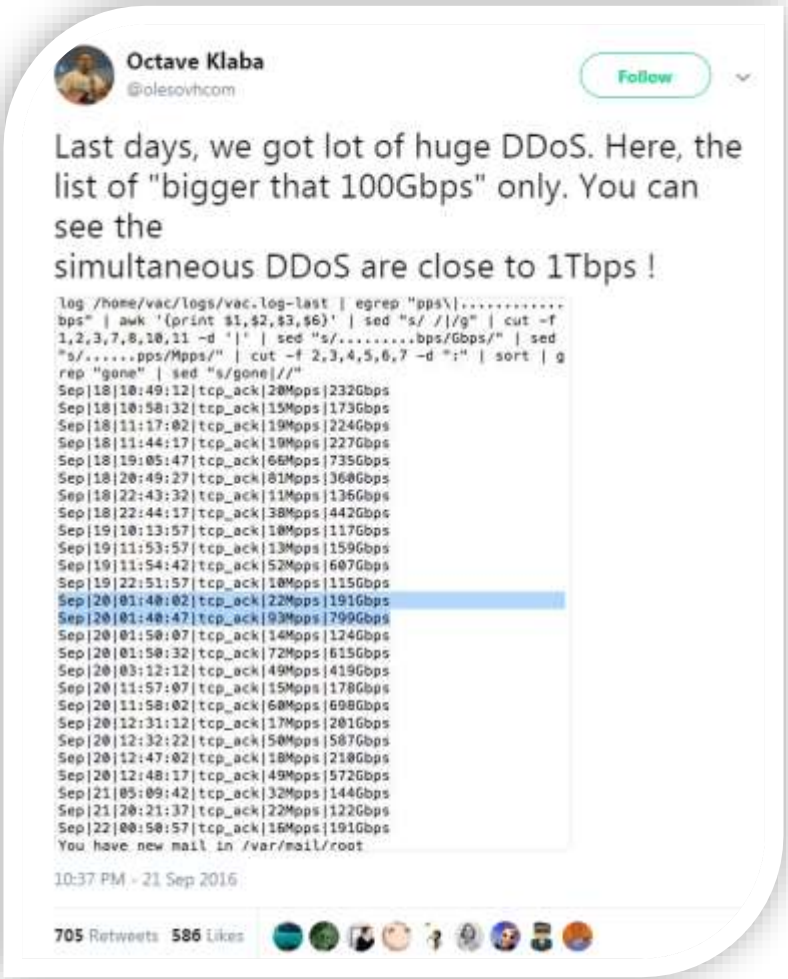

Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

Source : https://emilms.fema.gov

Threats to Critical National Infrastructure

Mirai Botnet (未来)

September and October 2016



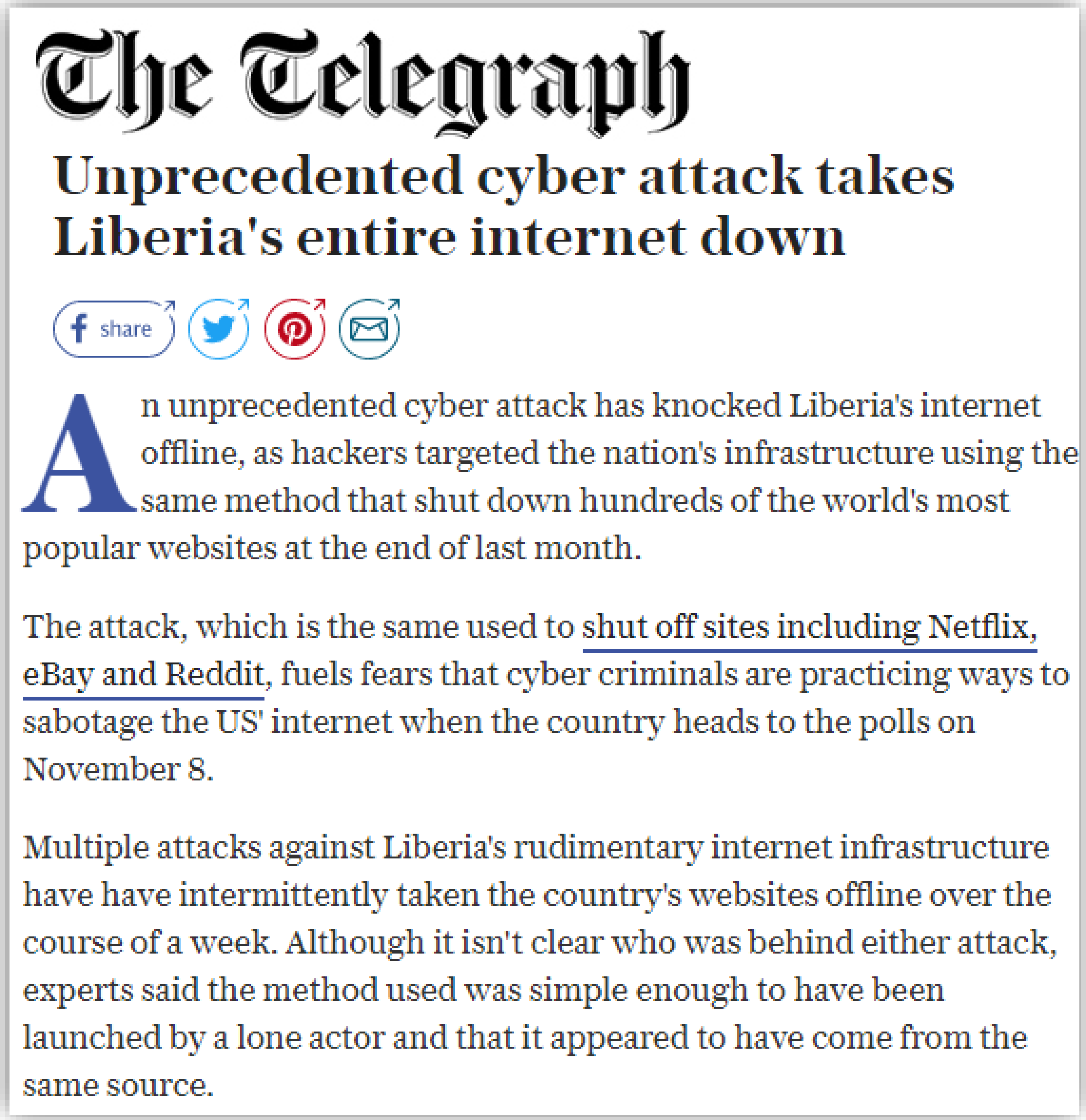
Octave Klaba
@olesovhcom

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

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.

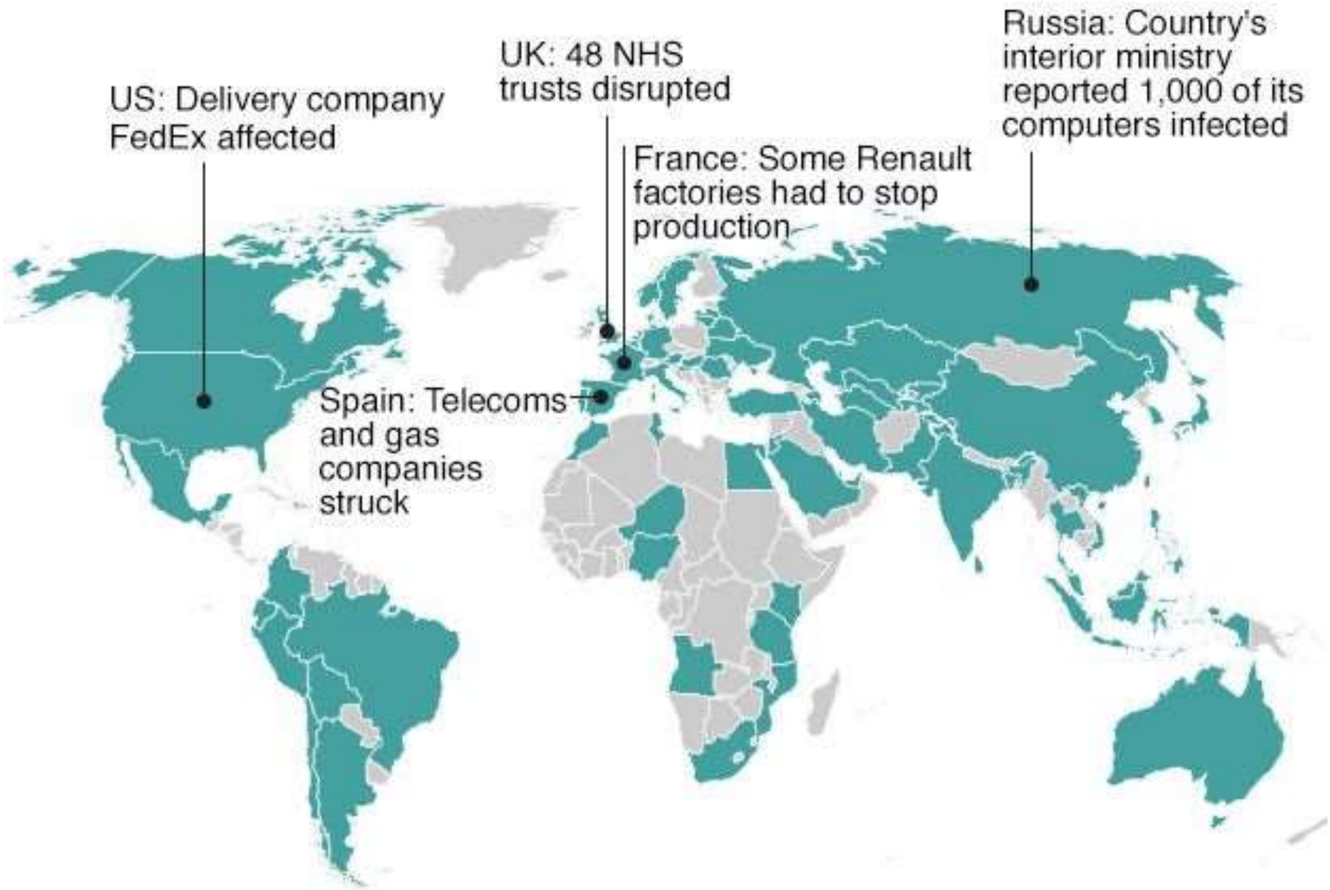
Multiple attacks against Liberia's rudimentary internet infrastructure have have intermittently taken the country's websites offline over the course of a week. Although it isn't clear who was behind either attack, experts said the method used was simple enough to have been launched by a lone actor and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

Threats to Critical National Infrastructure

WannaCry ransomware

May 2017

Countries hit in initial hours of cyber-attack



US: Delivery company FedEx affected

UK: 48 NHS trusts disrupted

France: Some Renault factories had to stop production

Russia: Country's interior ministry reported 1,000 of its computers infected

Spain: Telecoms and gas companies struck

*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Noway, where incidents have been reported since

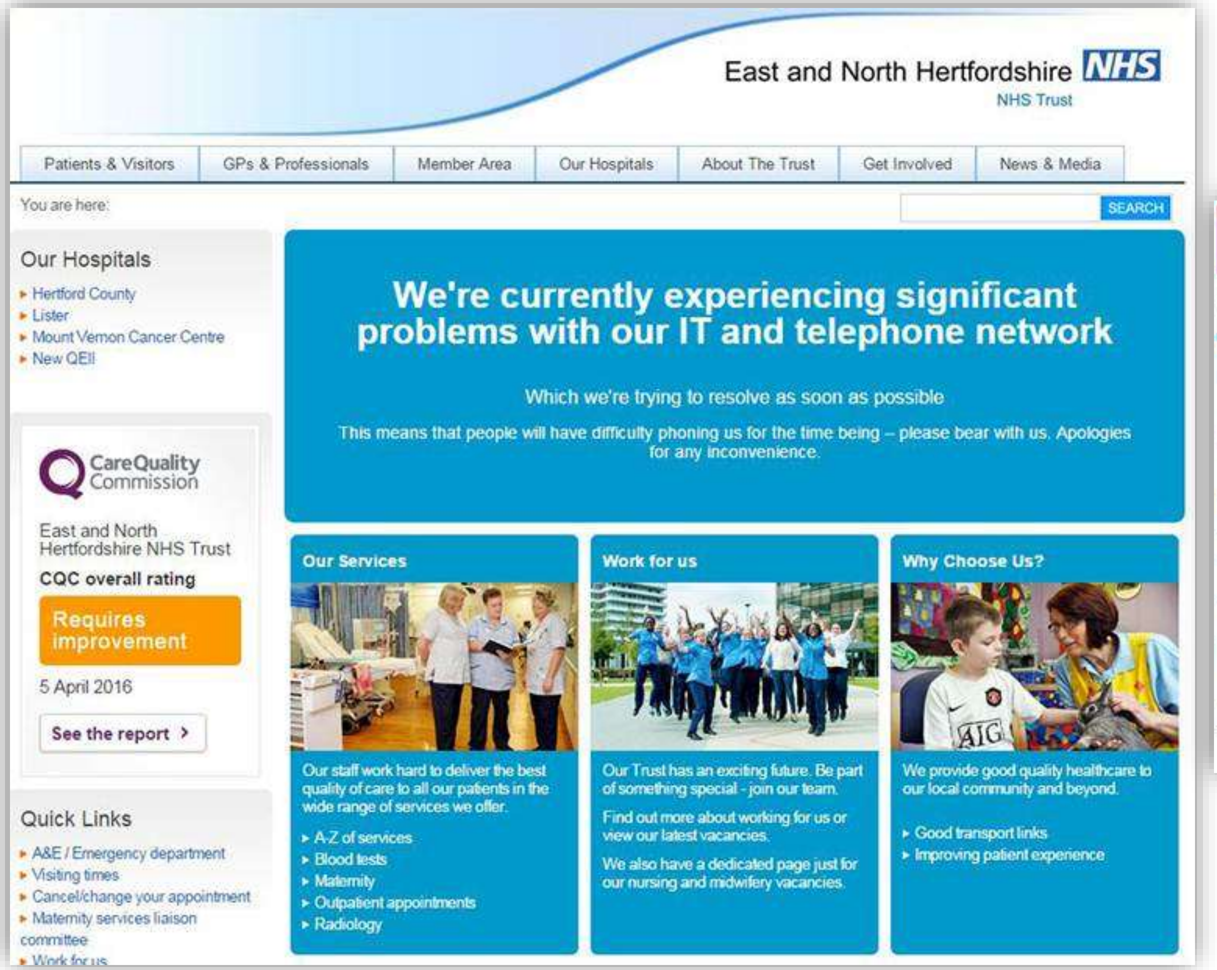
Source: Kaspersky Lab's Global Research & Analysis Team

BBC

Threats to Critical National Infrastructure

WannaCry ransomware

May 2017



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.

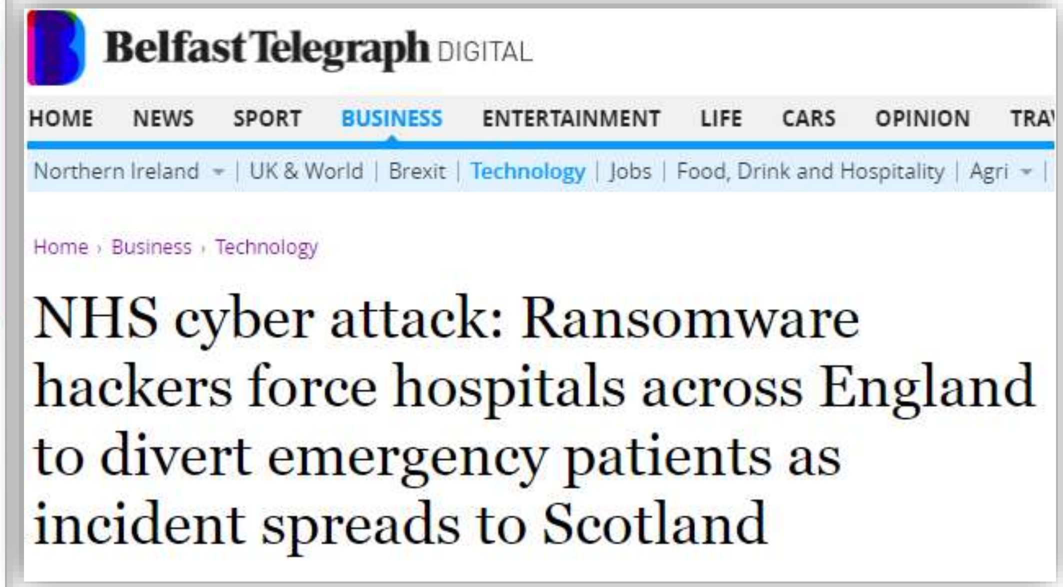
Find out more about working for us or view our latest vacancies.

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.

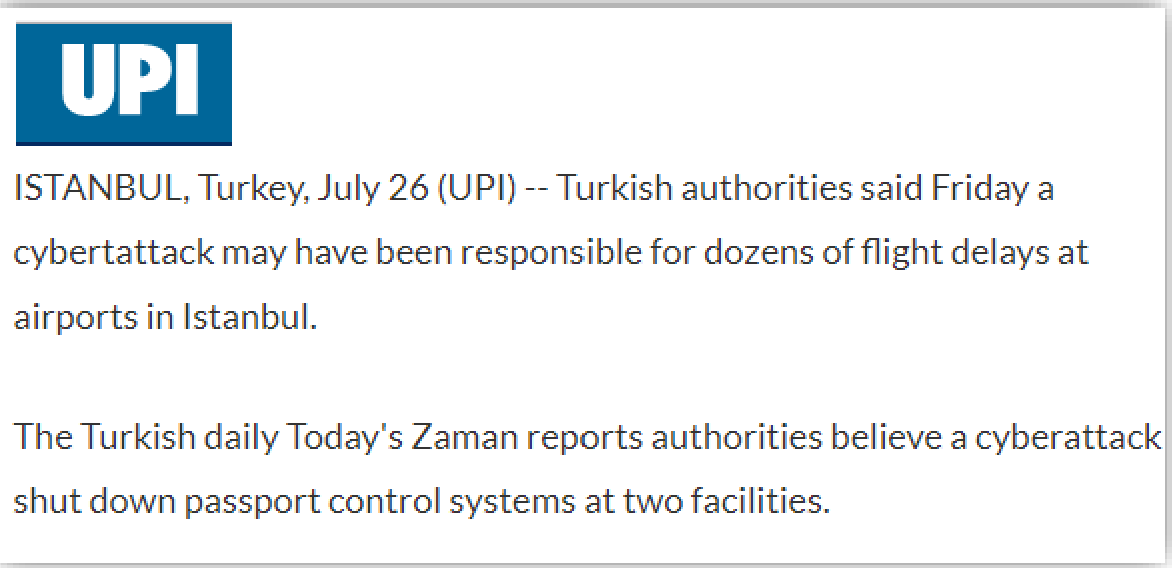
- Good transport links
- Improving patient experience



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

Threats to Critical National Infrastructure

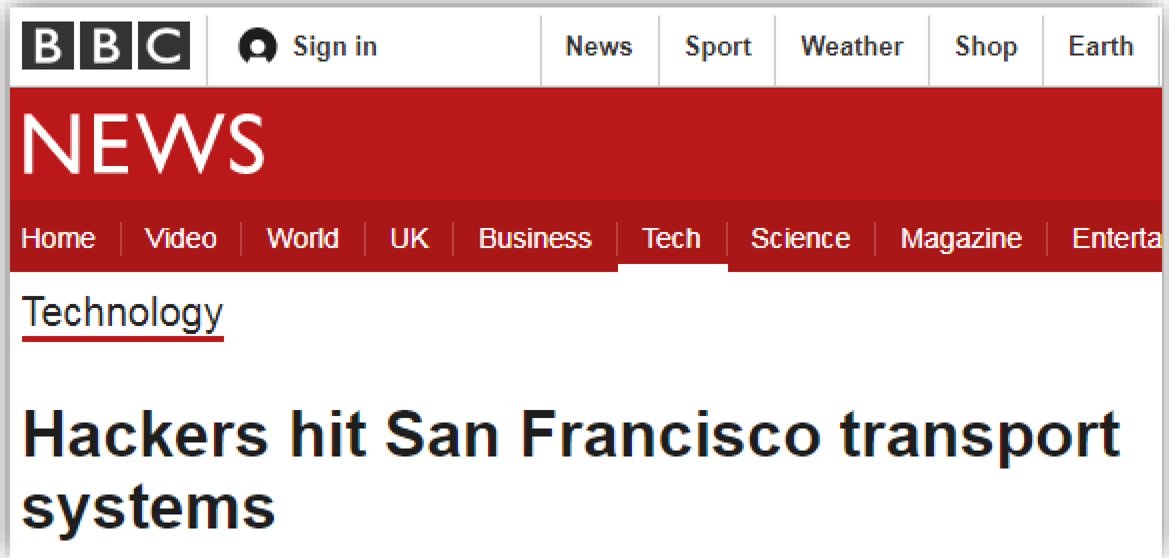
Istanbul Airports
July 2016



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.

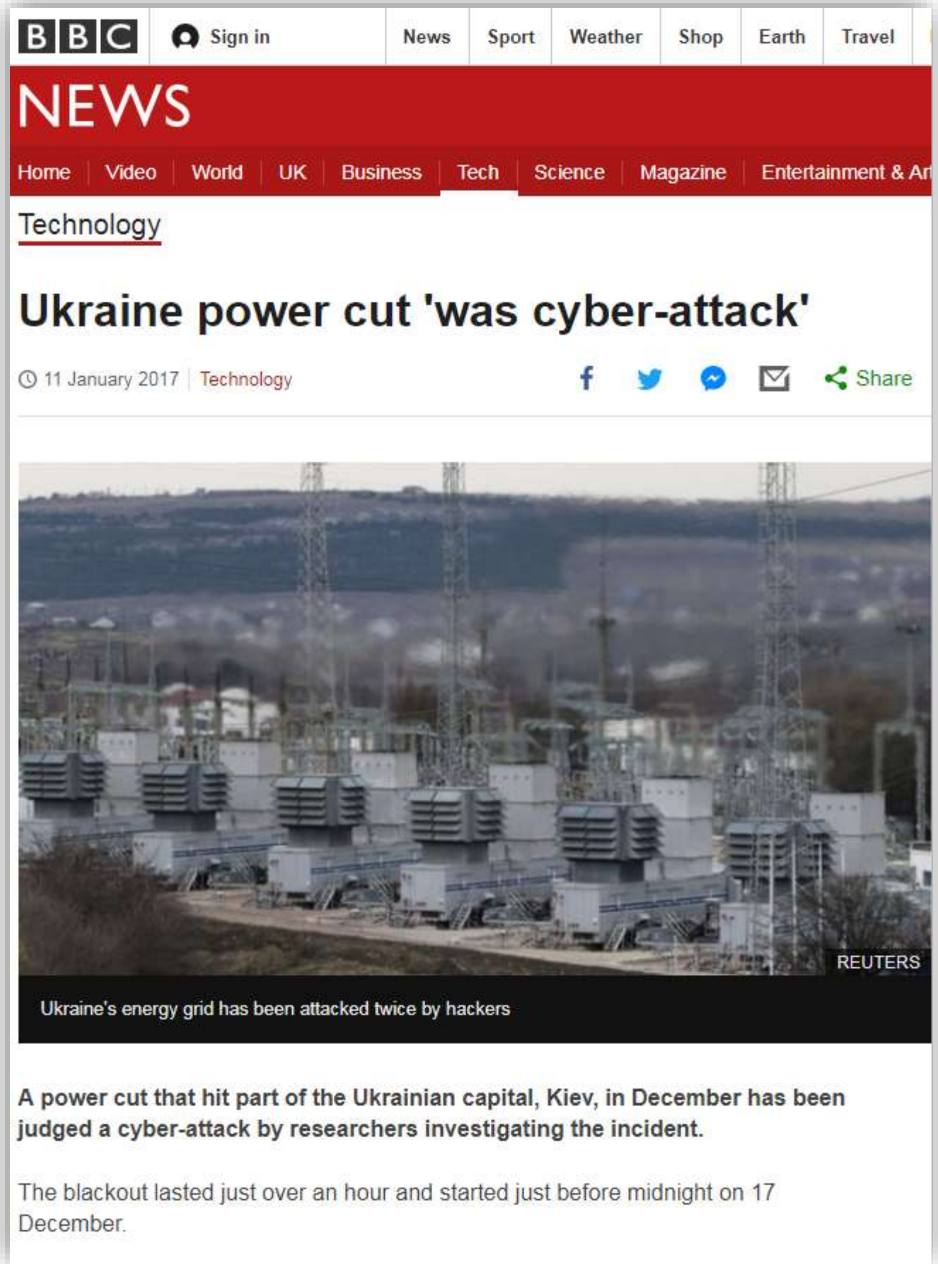
San Francisco train system
November 2016



Hackers hit San Francisco transport systems

Threats to Critical National Infrastructure

Kiev's power grid
December 2016



Technology

Ukraine power cut 'was cyber-attack'

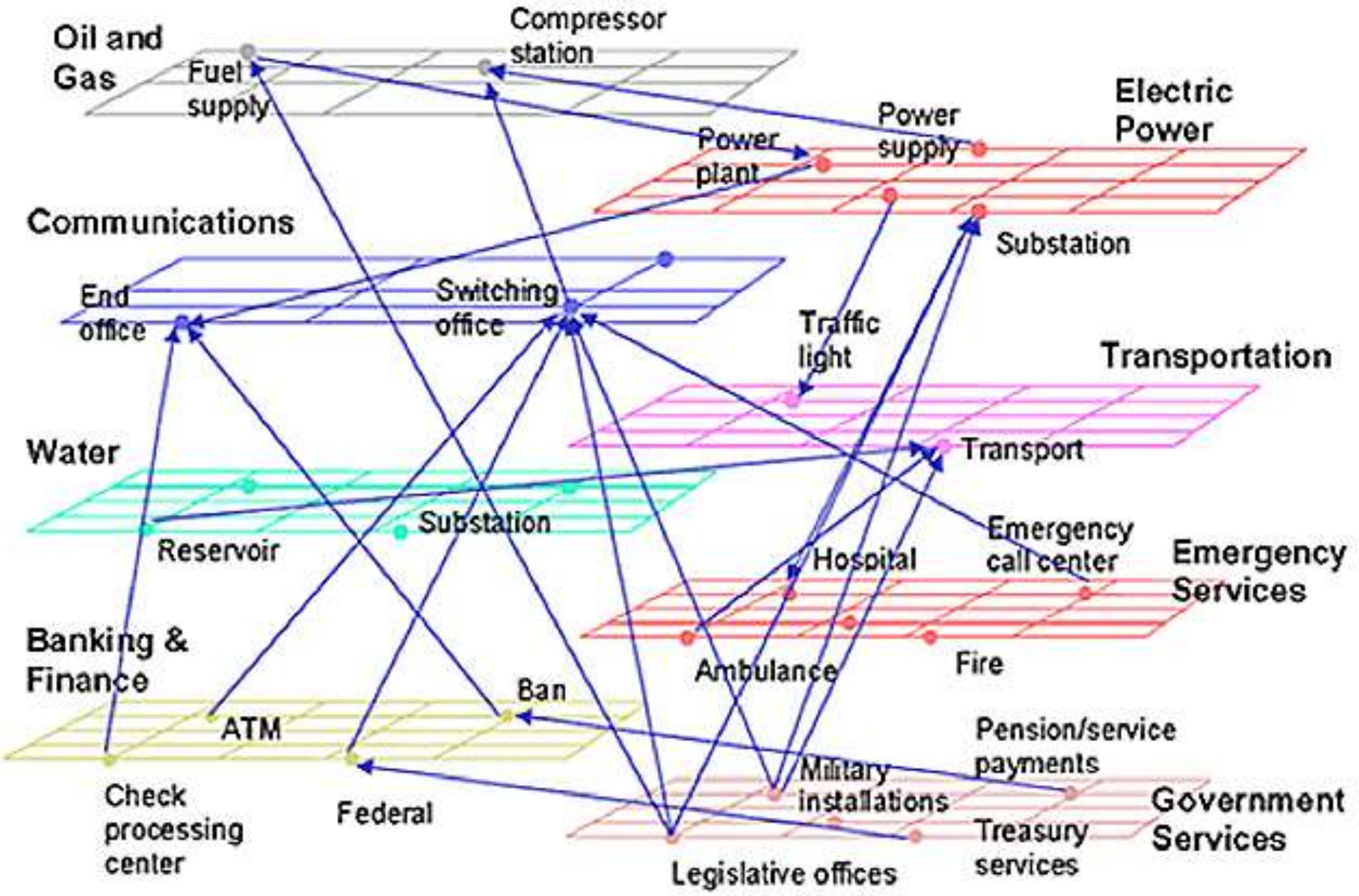
11 January 2017 | Technology

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

Agenda

1. What Is National Critical Information Infrastructure?

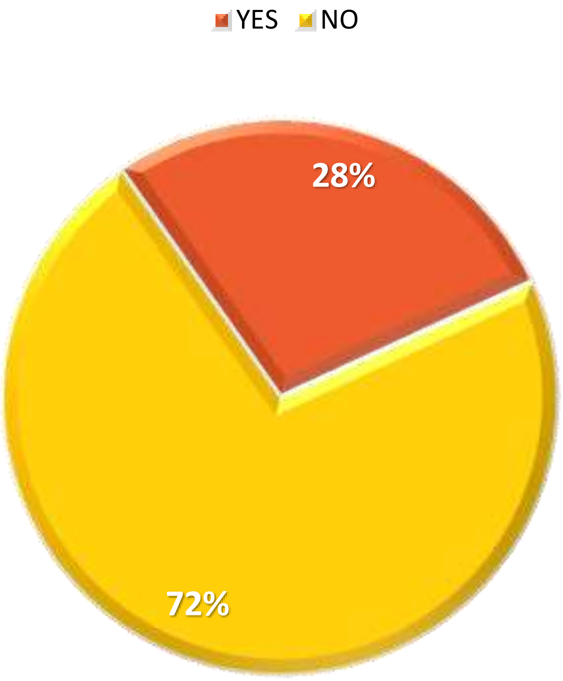
2. Threats to National Critical Information Infrastructure

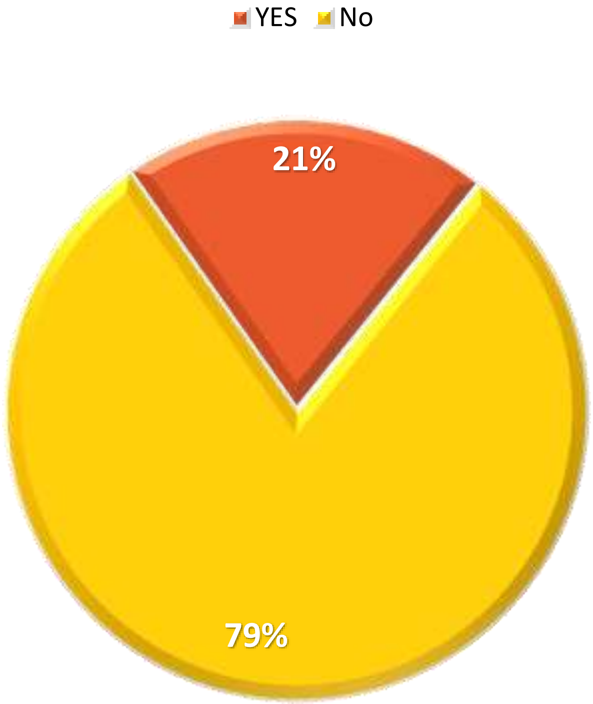
3. **The Role of the national CIRT in the CIIP**

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?

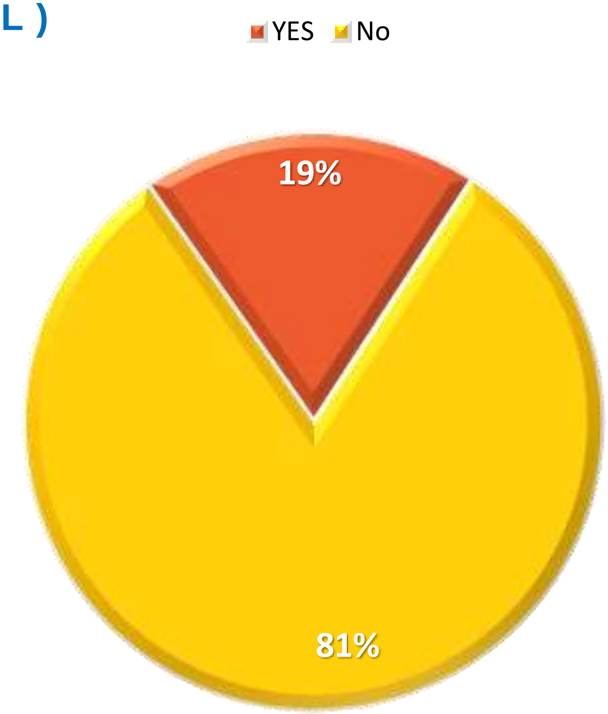
Does the legislation or regulation impose cybersecurity audits on the critical infrastructure operators ?

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

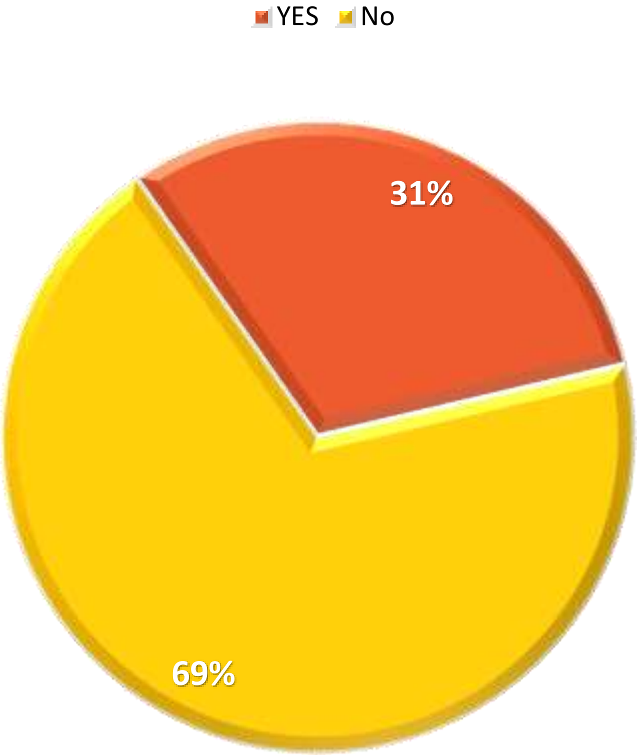
CIRT The Role of the national CIRT in the CIIP

Key findings of GCI 2017 on CIIP

(ORGANIZATIONAL)



Does national cybersecurity strategy include a national resilience plan ?



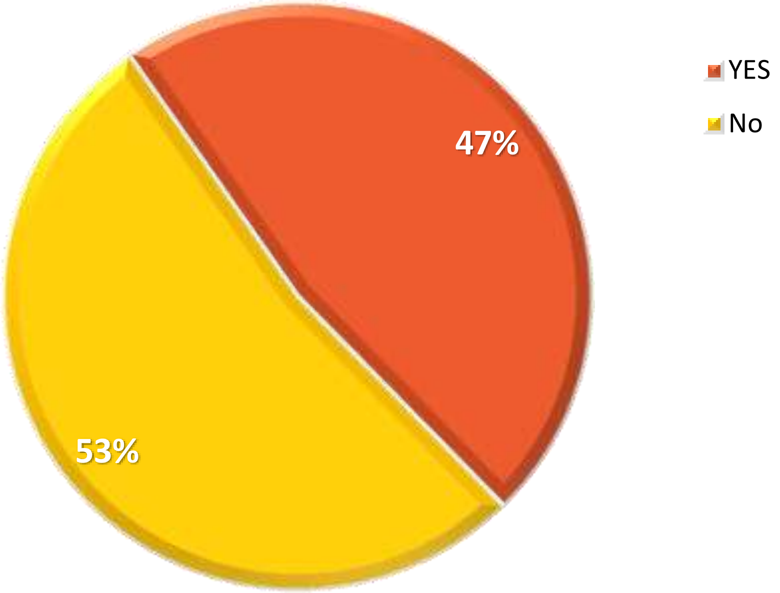
In the national strategy for cybersecurity , Is there a section on the protection of critical information infrastructure?

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

CIRT The Role of the national CIRT in the CIIP

Type Of Incident Response Team

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

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

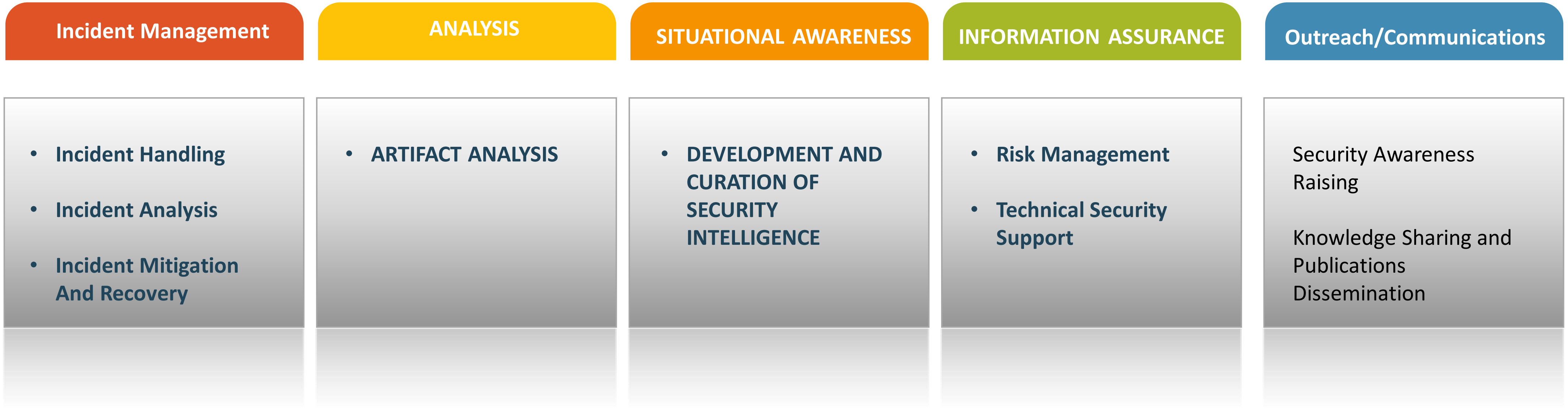
  UN-CSIRT , CERT-EU
- **Sectorial Incident Response Team**

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

  AfricaCERT, APCERT , OIC-CERT

CIRT The Role of the national CIRT in the CIIP

Basic Services of a National CIRT



Incident Management

- Incident Handling
- Incident Analysis
- Incident Mitigation And Recovery

ANALYSIS

- ARTIFACT ANALYSIS

SITUATIONAL AWARENESS

- DEVELOPMENT AND CURATION OF SECURITY INTELLIGENCE

INFORMATION ASSURANCE

- Risk Management
- Technical Security Support

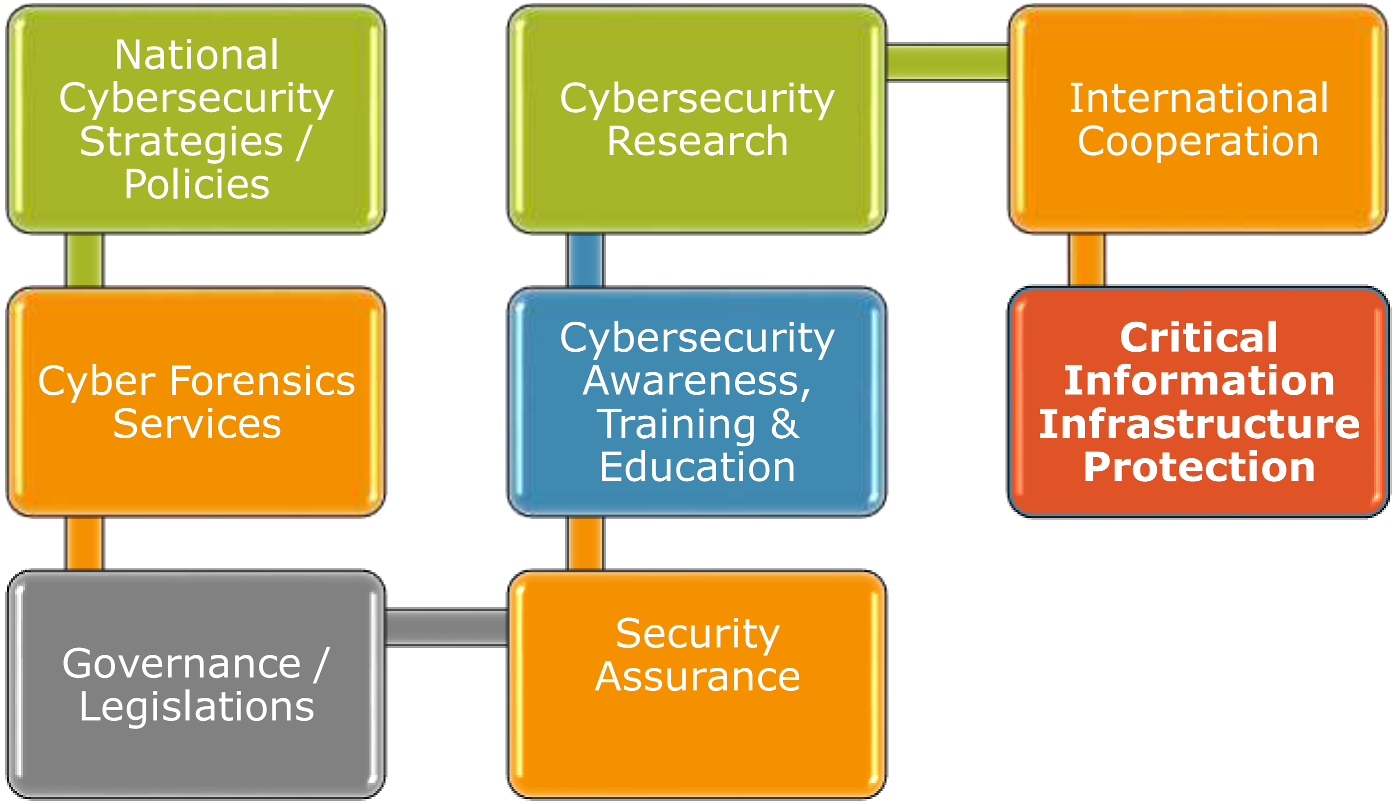
Outreach/Communications

Security Awareness Raising

Knowledge Sharing and Publications Dissemination

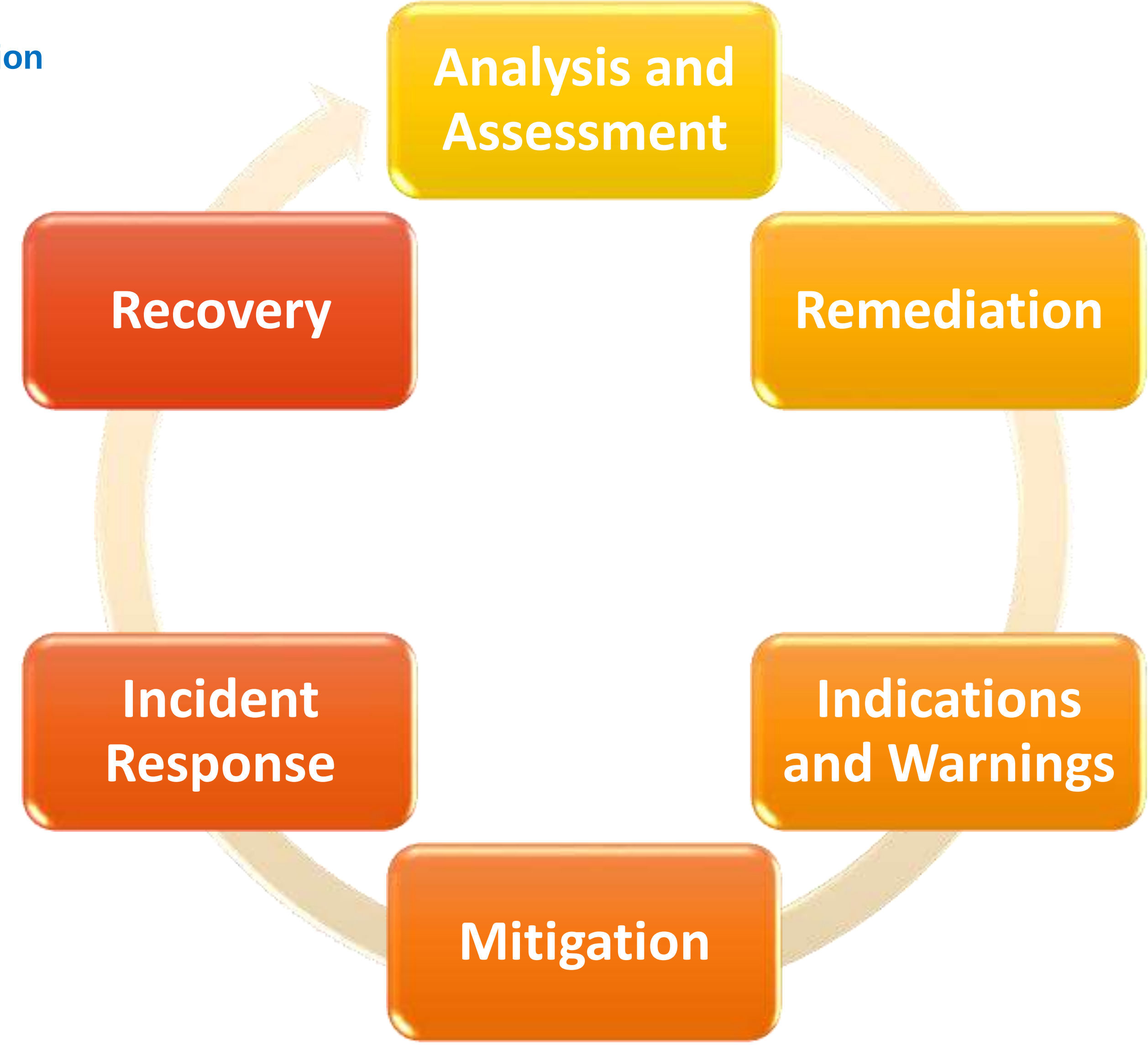
CIRT The Role of the national CIRT in the CIIP

National CIRT as enabler


National Cybersecurity Strategies / Policies
Cybersecurity Research
International Cooperation
Cyber Forensics Services
Cybersecurity Awareness, Training & Education
Critical Information Infrastructure Protection
Governance / Legislations
Security Assurance

CIRT The Role of the national CIRT in the CIIP

The Six Phases of Critical information Infrastructure Protection (CIIP)



Analysis and Assessment

Remediation

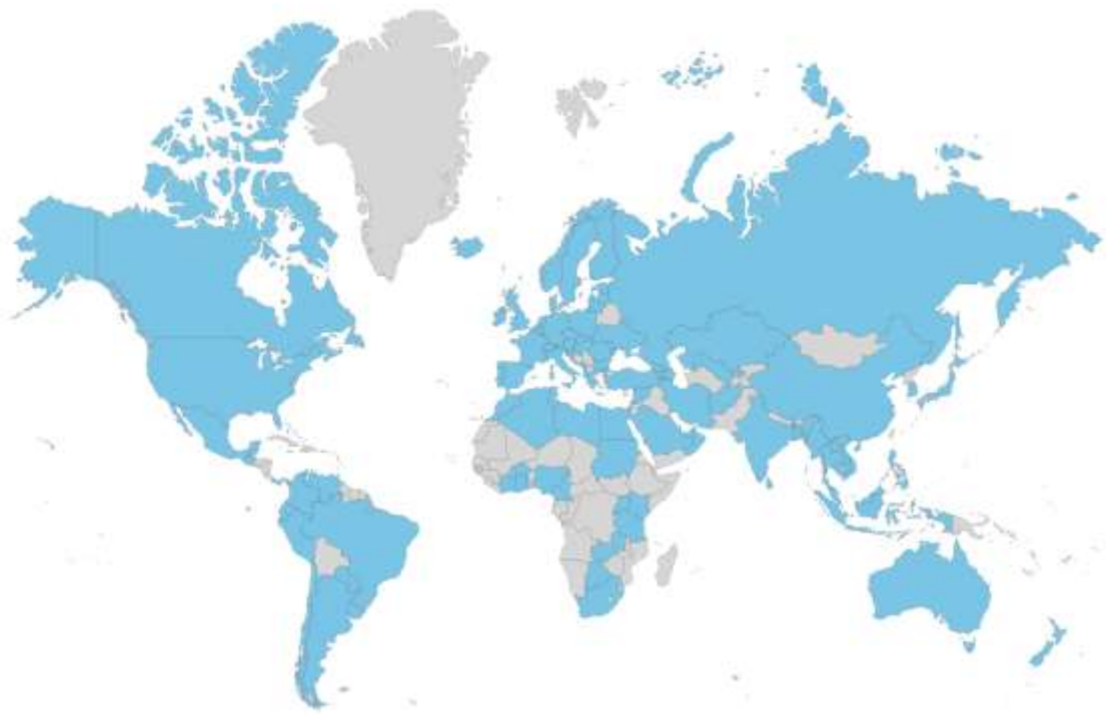
Indications and Warnings

Mitigation

Incident Response

Recovery

National CIRTs are in the first line of cyber-response

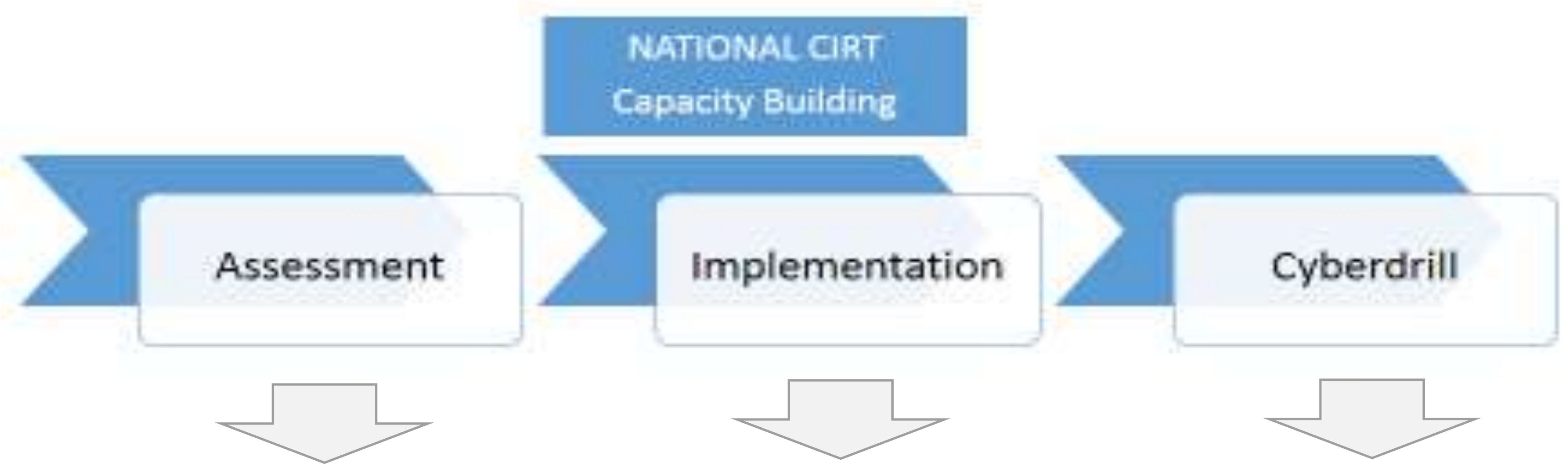


102 National CIRTs Worldwide

Need to fill the gaps

- Providing incident response support;
- Dissemination of early warnings and alerts;
- Facilitating communications and information sharing among stakeholders;
- Developing mitigation and response strategies and coordinating incident response;
- Sharing data and information about the incident and corresponding responses;
- Publicizing best practices in incident response and prevention advice;
- Coordinating international cooperation on cyber incidents;

ITU’s National CIRT Programme



NATIONAL CIRT
Capacity Building

Assessment

- Assess existing capability of/need for national cybersecurity mechanisms
- On-site assessment through meetings, training, interview sessions and site visits
- Form recommendations for plan of action (institutional, organizational and technical requirements)

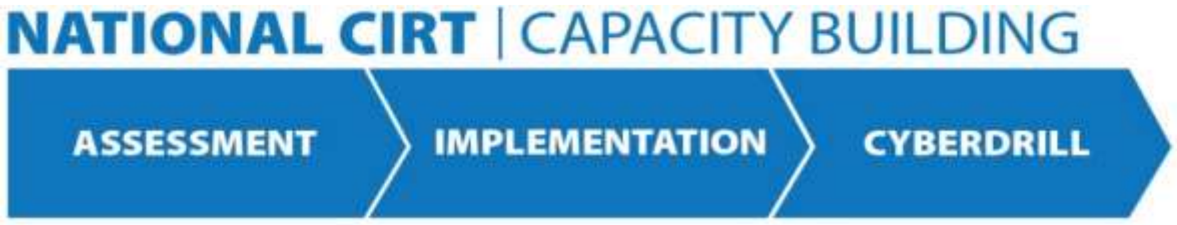
Implementation

- Design and Implement CIRT based on the identified needs and organizational structures of the country
- Assist with planning, implementation, and operation of the CIRT.
- Continued collaboration with the newly established CIRT for additional support
- Capacity Building and trainings on the operational and technical details
- Further improvement and enhancement overtime

Cyberdrill

- Exercises organized at both regional and international level
- Help enhance the communication and response capabilities of the participating CIRTs
- Improve overall cybersecurity readiness in the region
- Provide opportunities for public-private cooperation

ITU’s National CIRT Programme



NATIONAL CIRT | CAPACITY BUILDING

ASSESSMENT

IMPLEMENTATION

CYBERDRILL

- Assessments conducted for **68** countries
- Implementation completed for **12** countries

Barbados, Burkina Faso, Côte d'Ivoire, Cyprus, Ghana, Jamaica, Kenya, Montenegro, Tanzania, Trinidad and Tobago, Uganda, Zambia

- Implementation in progress for **4** countries

Burundi, Gambia, Palestine and Zimbabwe

- **18** Regional cyber drills conducted with participation of over 115 countries

National Cyber Security Guide

A Joint Effort by 15 Partners

Co-authored Multi-stakeholder approach

UNITED NATIONS
UNCTAD

Microsoft

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Organization of
American States

GCSP

ITU

CCDCOE

POTOMAC INSTITUTE FOR POLICY STUDIES

INTELLIUM

OECD
BETTER POLICIES FOR BETTER LIVES

RAND EUROPE

ENISA

CTO
COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

The Commonwealth
Cybercrime Initiative

Global
Cyber Security
Capacity Centre

All project partners contribute their knowledge and expertise in the National Cyber Security domain, thereby providing a high added value to the toolkit definition

Ongoing project to produce one reference guide on devising a national cybersecurity strategy to be followed by implementation in countries

Expected release in 2018

THANK YOU