Building national cyber resilience and protecting critical information infrastructure Role of National CIRT

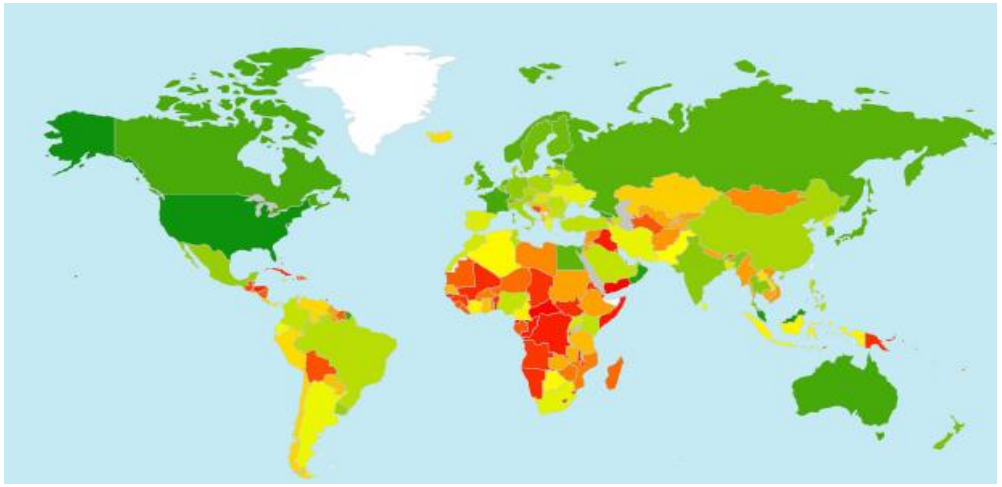
Port Moresby , PNG, 03-07 June 2019

What is Critical Information Infrastructure?

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

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.”

sectors

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

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

What Is Critical National Infrastructure?

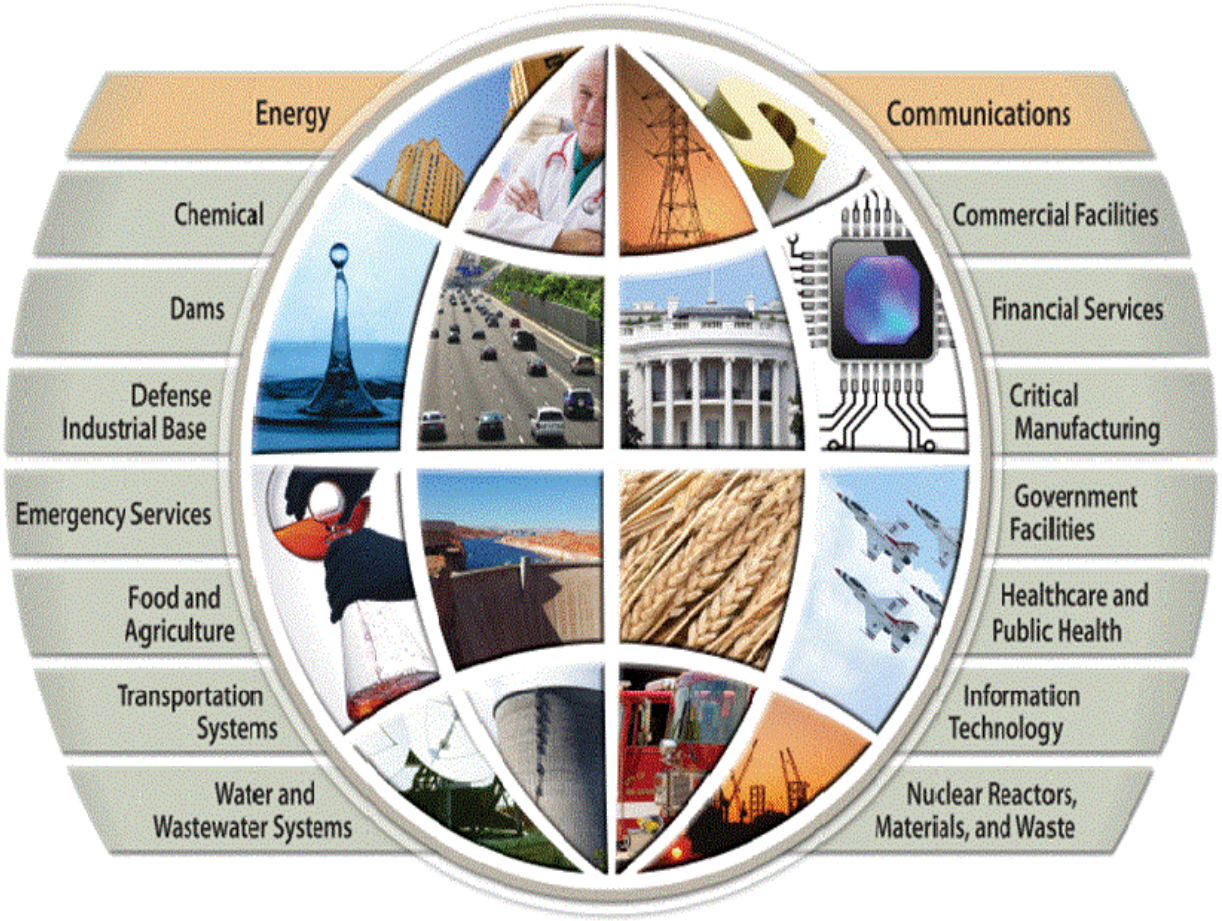
The United States of America

Definition of Critical National Infrastructure:

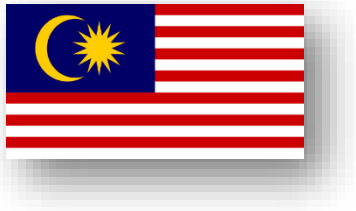
“Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

Department of Homeland Security -USA-

sectors



What Is Critical National Infrastructure?



Malaysia

Definition of Critical National Infrastructure:

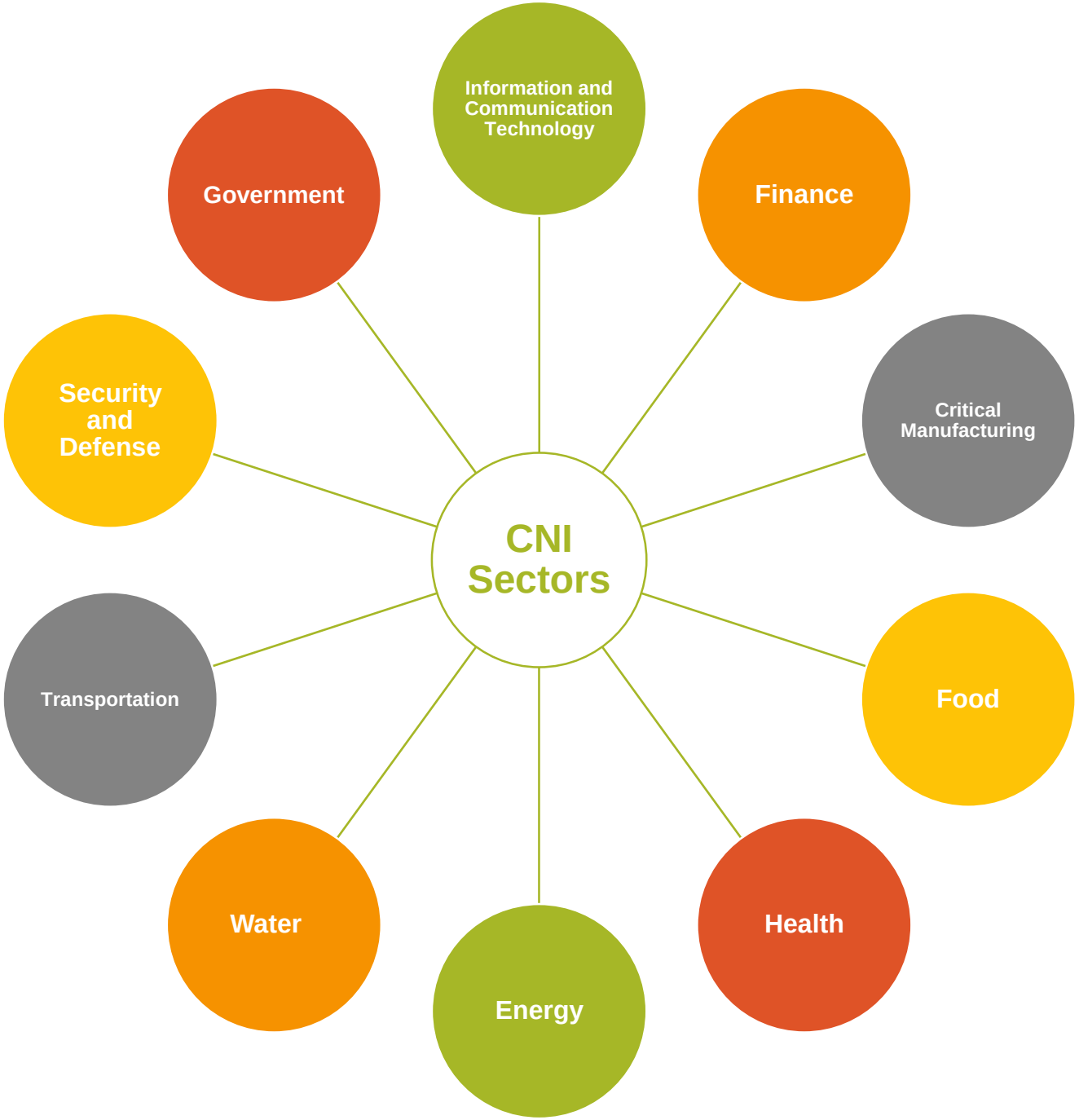
"Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on:

- 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."

CyberSecurity Malaysia - Malaysia -

sectors

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



Threats to Critical National Infrastructure

Source : https://emilms.fema.gov

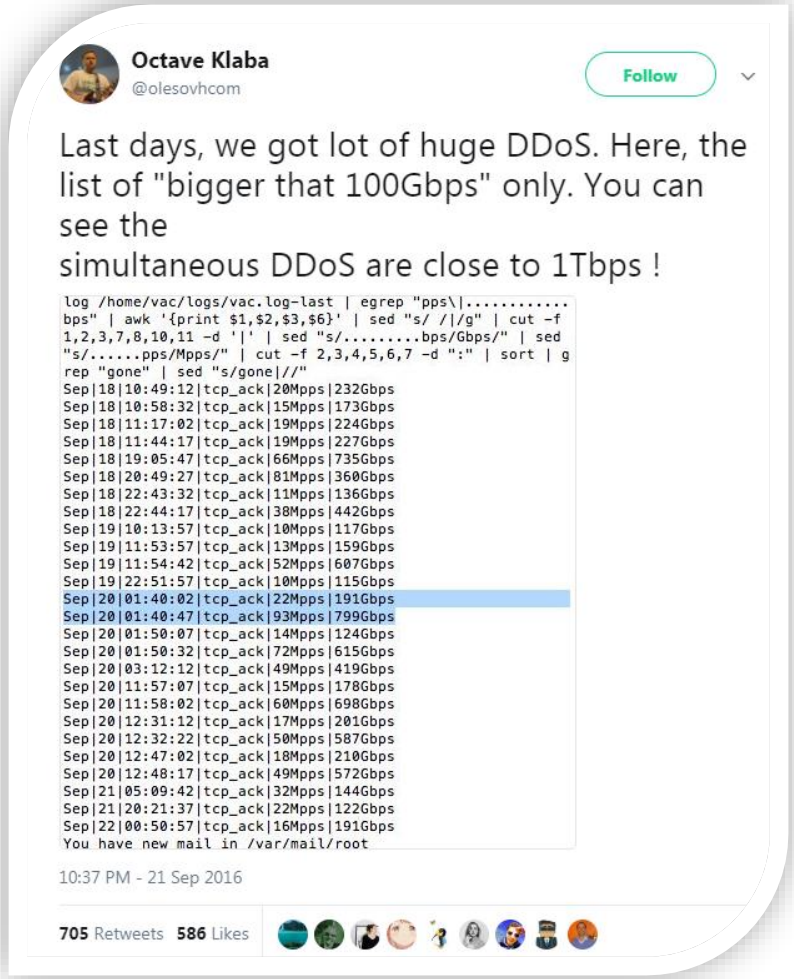
What are the Threats? Who are the Adversaries?

Threat Level	Actors	Motivation	Tools
Level 3 *Difficult to detect, extremely difficult attribution*	▪ Foreign intel agencies ▪ Well managed attack teams ▪ Insider	▪ Mostly intellectual property theft ▪ Establish covert presence on sensitive networks ▪ Potential for government secret theft	▪ Very well financed ▪ Target technology as well as information ▪ Use wide range of sophisticated tradecraft ▪ Zero-day vulnerabilities
Level 2 *Detectable, but hard to attribute*	▪ Highly skilled ▪ Criminal hacker ▪ Insider	▪ Mostly criminal & intellectual property theft ▪ Target and exploit valuable data	▪ May be well financed ▪ Target known vulnerabilities ▪ Use viruses, worms, trojans, bots to introduce more sophisticated tools ▪ Complex and crafted tools
Level 1 *Easily detected*	• Inexperienced • Script kiddies • Beginners • Insider	▪ Opportunistic behavior ▪ In it for the thrills, bragging rights	▪ Limited funding ▪ User viruses, worms, rudimentary trojans, and bots ▪ Publicly available tools

Threats to Critical National Infrastructure :Network Operators and ISPs

Mirai Botnet (未来)

September and October 2016



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.

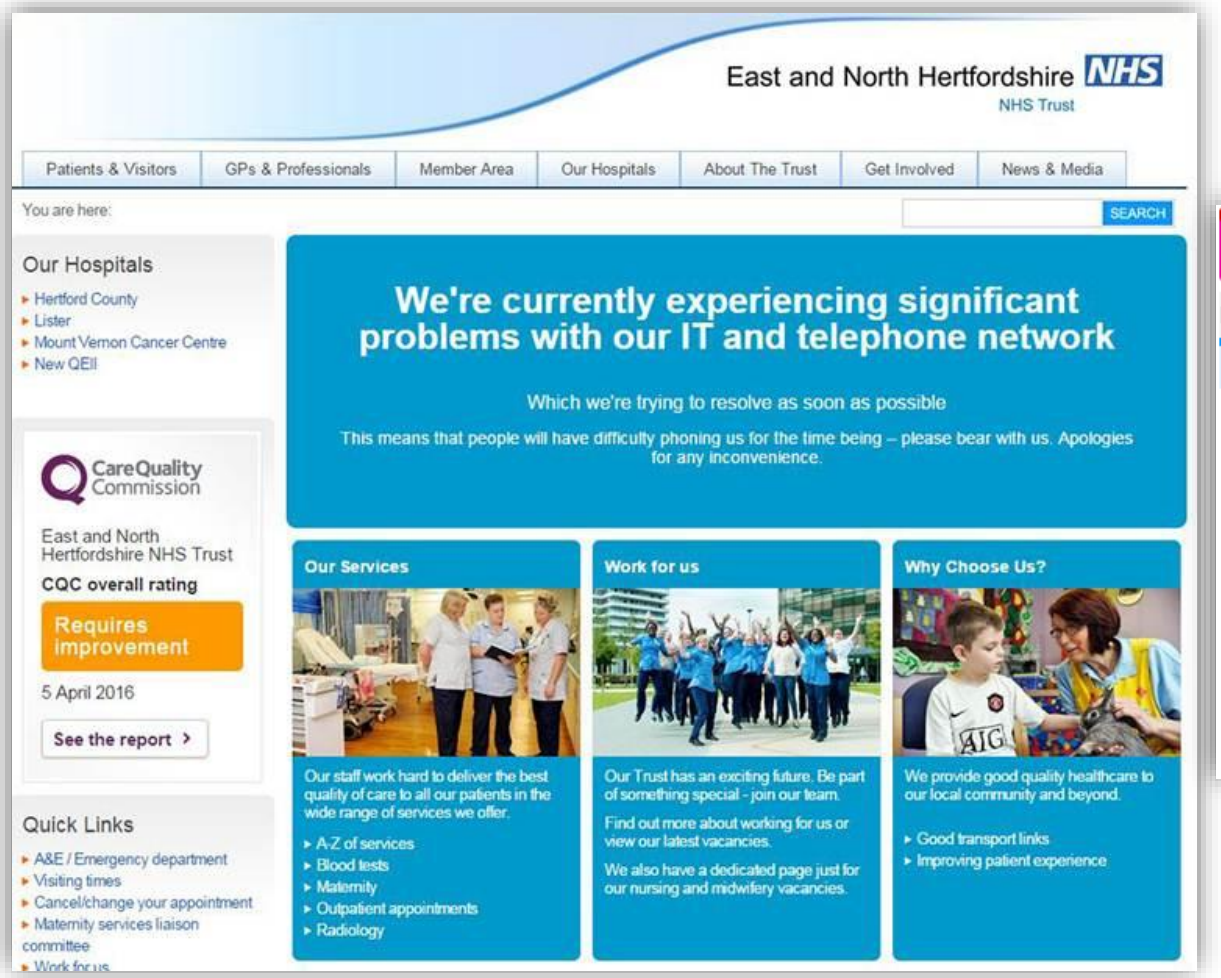
The attack, which is the same used to shut off sites including Netflix, eBay and Reddit, fuels fears that cyber criminals are practicing ways to sabotage the US' internet when the country heads to the polls on November 8.

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: Health care institutions

WannaCry ransomware

May 2017



Threats to Critical National Infrastructure: Health care institutions

THE BUFFALO NEWS

ECMC spent nearly $10 million recovering from massive cyberattack

By Henry L. Davis | Published July 26, 2017 | Updated July 26, 2017

Healthcare IT News

Erie County Medical Center systems still down 12 days after massive cyberattack

April 24, 2017 | 02:46 PM

The Buffalo-based hospital said no patient records have been compromised, but is still working to restore regular functions and continues to operate without interruption.

Buffalo-based Erie County Medical Center is still struggling to bring its computer systems back online after a virus was discovered on April 9, according to The Buffalo News.

Threats to Critical National Infrastructure : Financial Institutions

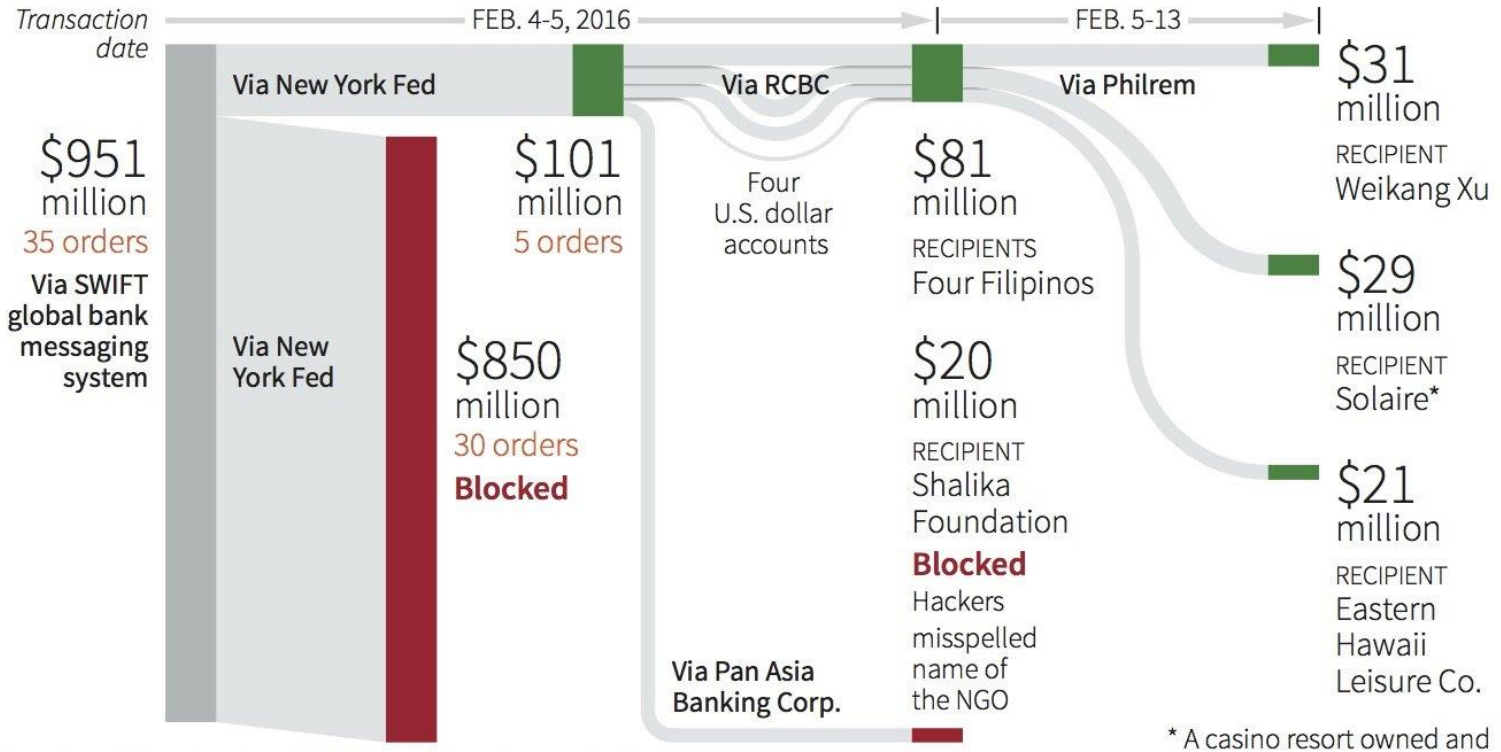
Bangladesh Central Bank

4 February 2016

Bangladesh Bank heist

In one of the largest cyber heists in history, hackers ordered the Federal Reserve Bank of New York to transfer $81 million from Bangladesh Bank to accounts in the Philippines.

THE MONEY TRAIL



Sources: Philippines Court of Appeals documents; Reuters

* A casino resort owned and operated by Bloomberry Resorts

W. Foo, 31/03/2016

REUTERS

Threats to Critical National Infrastructure : Financial Institutions

EXPRESS Home of the Daily and Sunday Express

'This is just the beginning' Anonymous hackers take down nine banks in 30-day cyber attack

HACKING group Anonymous claim they have taken down central banks in Germany, Greece and Cyprus as they carry out a 30-day worldwide cyber attack.

REUTERS

TECHNOLOGY NEWS MAY 17, 2018 / 1:41 AM /

Mexico central bank says hackers siphoned $15 million from five companies

REUTERS

After Bank of Greece, Cyprus Central Bank also reports cyber attack

ATHENS (Reuters) - The website of the Central Bank of Cyprus briefly came under cyber attack, days after a hacking collective said it conducted a similar attack on the Greek central bank's site.

Threats to Critical National Infrastructure : Financial Institutions

Feb, 2019

Bank of Valletta decommissioned its systems to prevent hackers wiring money to accounts in the UK, US, Hong Kong and Czech Republic

Malta's oldest bank took the extraordinary step of shutting down its entire IT operations to counter an active overseas cyber attack in which hackers attempted to steal €13 million.

ITPRO
IT ANALYSIS. BUSINESS INSIGHT.

The Telegraph

Metro Bank has become the first major bank to be named as a victim of a new type of cyber attack targeting the codes sent via text messages to customers to verify transactions.

Hackers were able to intercept an additional layer of security offered by Metro Bank, which asks customers to type in a code sent by text message to their phones to confirm transfers and payments.

April, 2018

FINANCIAL TIMES

Seven UK banks targeted by co-ordinated cyber attack

David Bond in London APRIL 25, 2018

8

Seven of the UK's biggest banks including Santander, Royal Bank of Scotland and Tesco Bank were forced to reduce operations or shut down entire systems following a cyber attack last year using software which can be rented for as little as £11, according to the National Crime Agency.

Threats to Critical National Infrastructure :Transport Companies

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

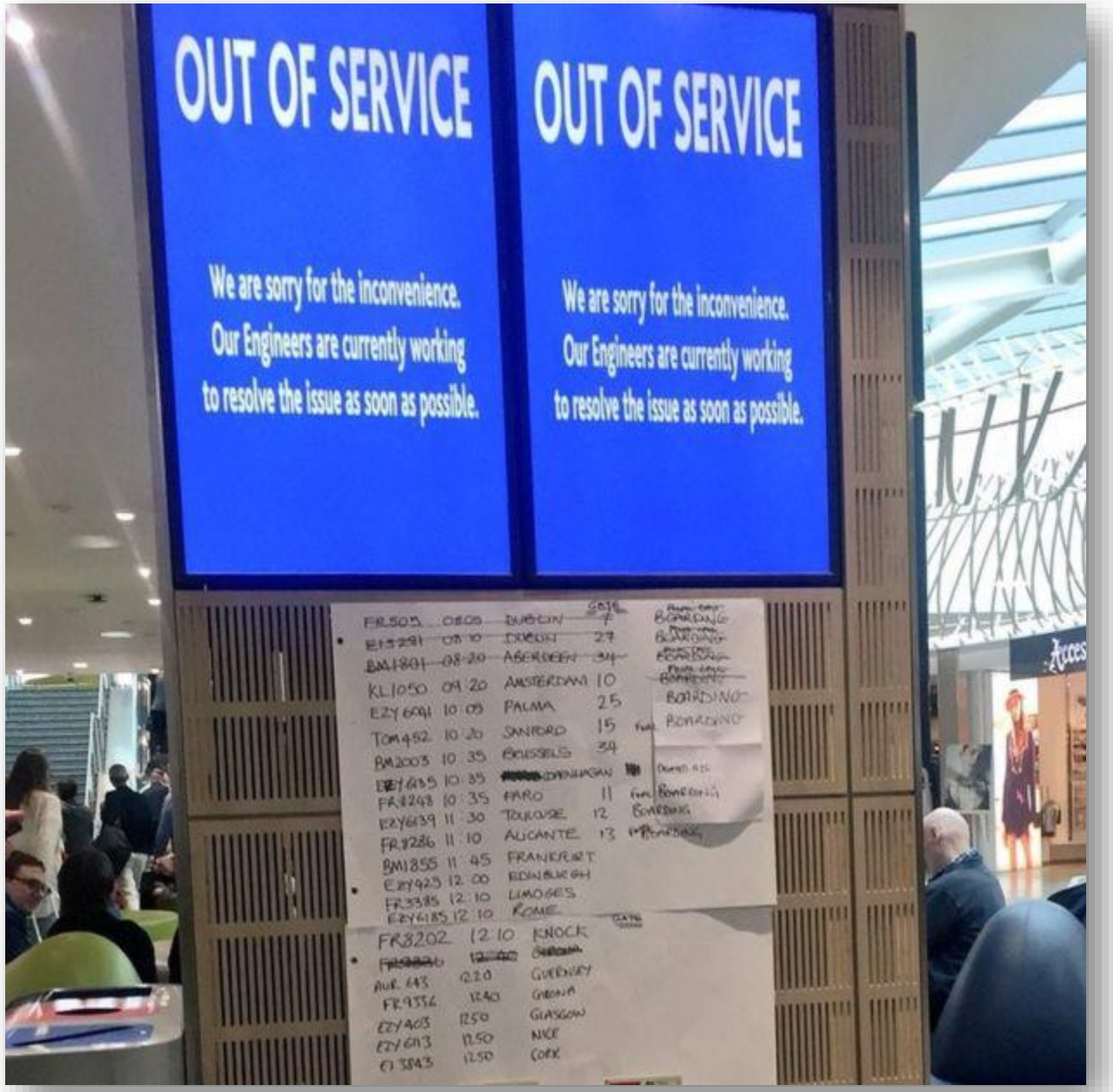
Threats to Critical National Infrastructure :Transport Companies

September 2018

Cyber attack led to Bristol Airport blank screens

BBC NEWS

Spokesman James Gore said: "We believe there was an online attempt to target part of our administrative systems and that required us to take a number of applications offline as a precautionary measure, including the one that provides our data for flight information screens.

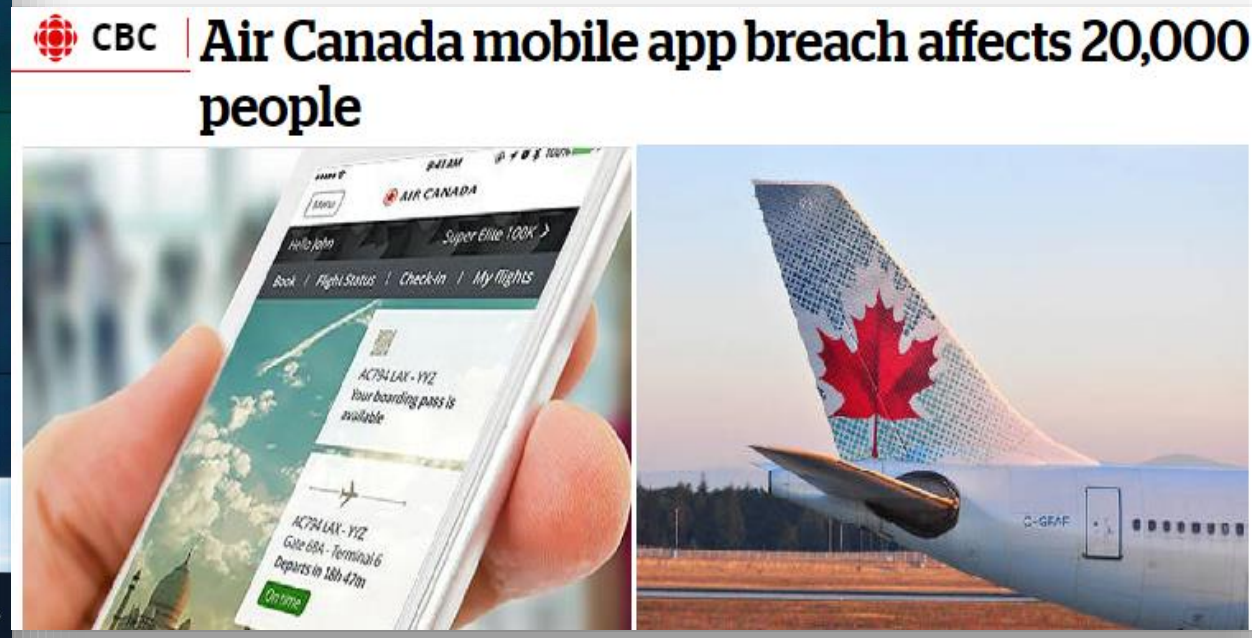


Threats to Critical National Infrastructure :Transport Companies

September 2018

380,000 Passengers Affected By 'Malicious' British Airways Hack

August 2018



Air Canada's app has suffered a data breach resulting in the suspected loss of thousands of its customers' personal details.

Threats to Critical National Infrastructure: E-voting system

BBC Sign in

NEWS

Philippines elections hack 'leaks voter data'

By Leisha Chi
BBC reporter

The Philippines is set to hold its general elections in May using automated machines for the third time

The Philippines may have suffered its worst-ever government data breach barely a month before its elections.

Personal information, including fingerprint data and passport information, belonging to around 70 million people is said to have been compromised by hackers.

The **Philippine Commission on the Elections** (Comelec) saw its website defaced at the end of March.

The Anonymous Philippines group has claimed responsibility for the attack.

Threats to Critical National Infrastructure: Power Generation Plants

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

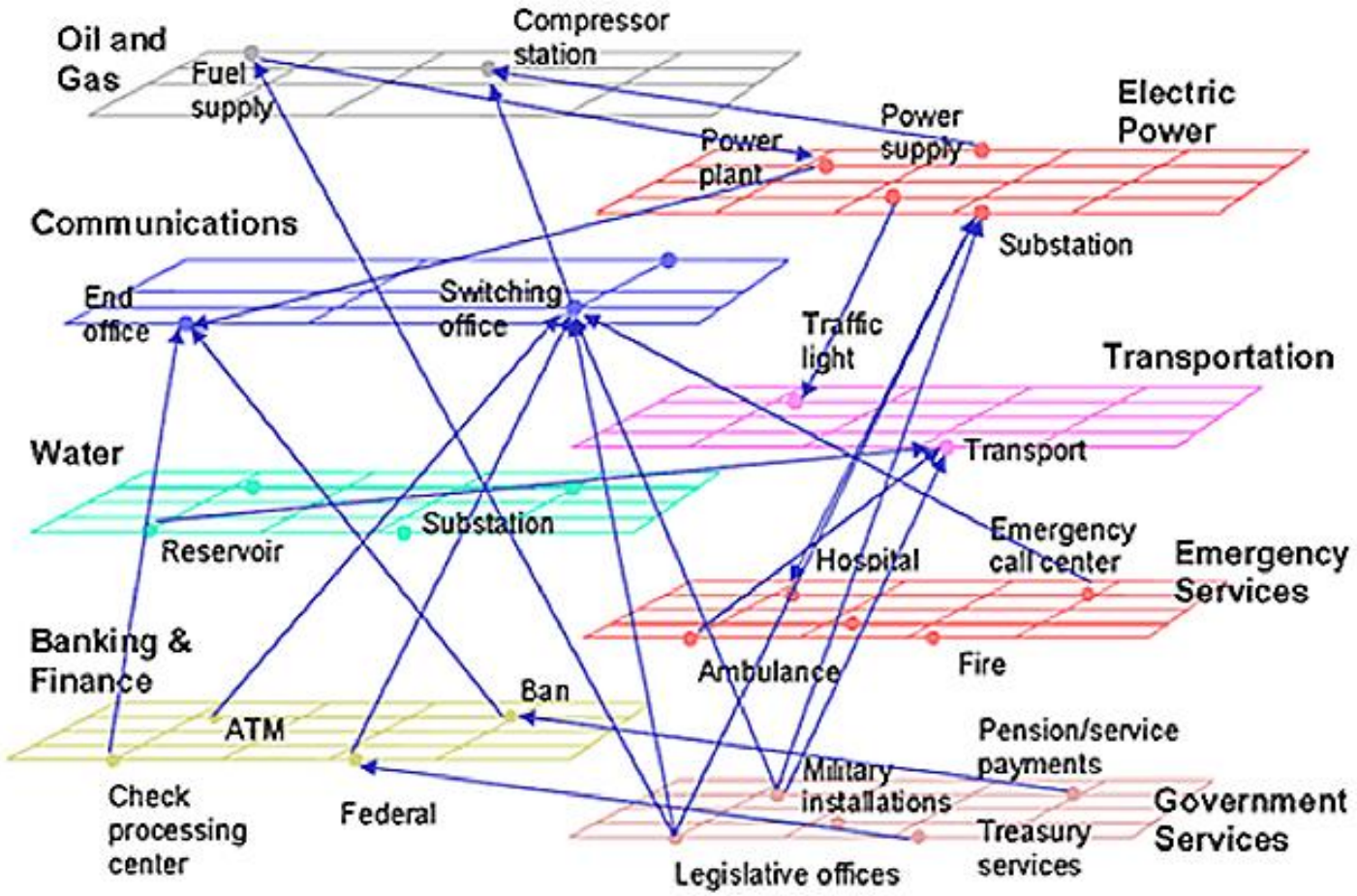
Share

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



Source : NSA

Interconnected Nature of Critical Infrastructure

Cascade effect

Cost of Cyberattack in 2017

BBC Sign in

NEWS

Cost of global disasters 'jumps to $306bn in 2017'

21 December 2017 Share

Disasters in 2017 caused losses of $306bn (£229bn), according to estimates from insurance giant Swiss Re.

The figure represents a 63% jump from last year, and is well above the average of the past decade.

CYBERSECURITY

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Cybercrime 'pandemic' may have cost the world $600 billion last year

Lynette Lau

Published 7:19 PM ET Thu, 22 Feb 2018

CNBC

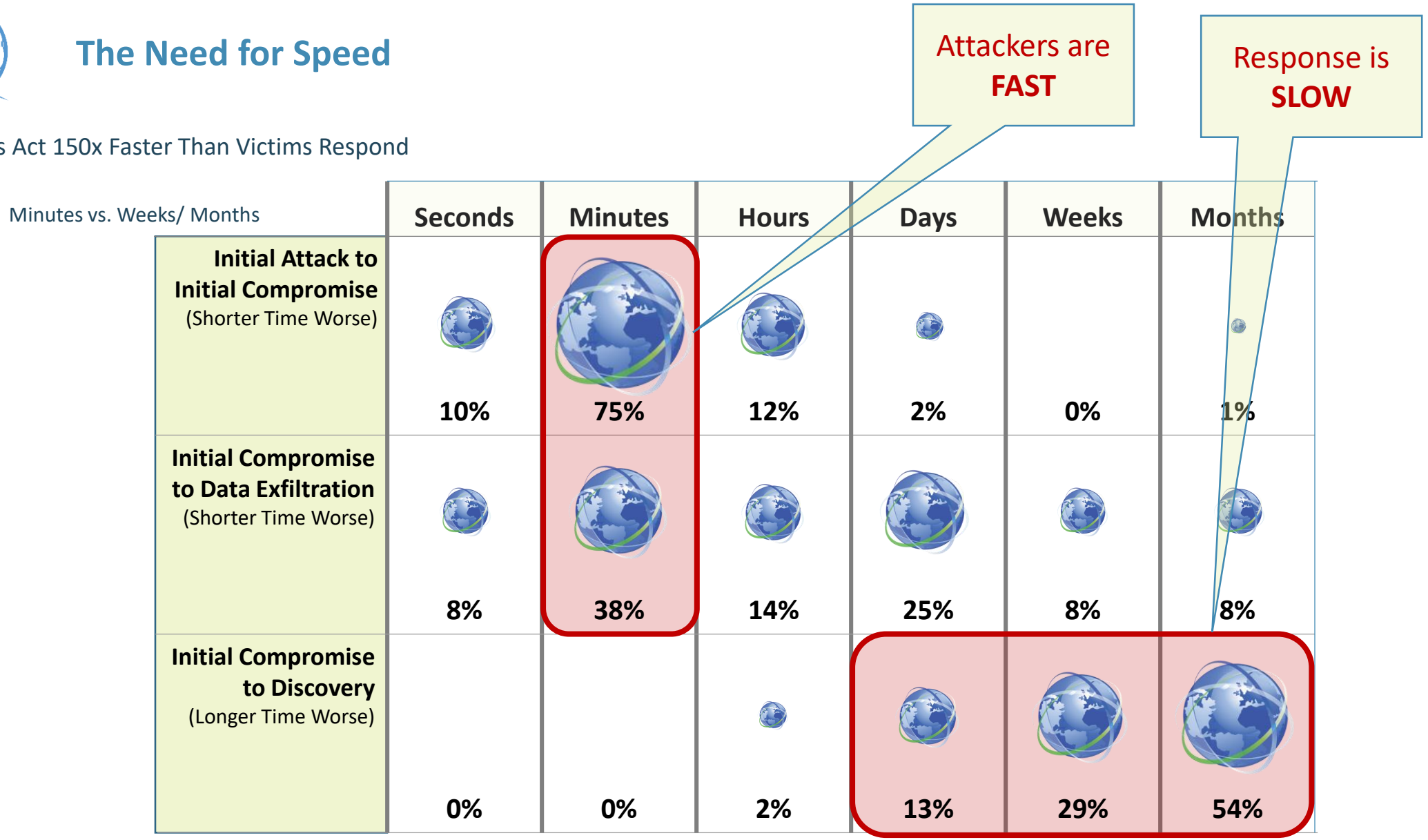
CNBC

The global cost of cybercrime has now reached as much as $600 billion — about 0.8 percent of global GDP — according to a new report.

More worrying than that figure may be the massive growth from 2014, when the same analysis showed the cost was only as much as $445 billion.

The Need for Speed

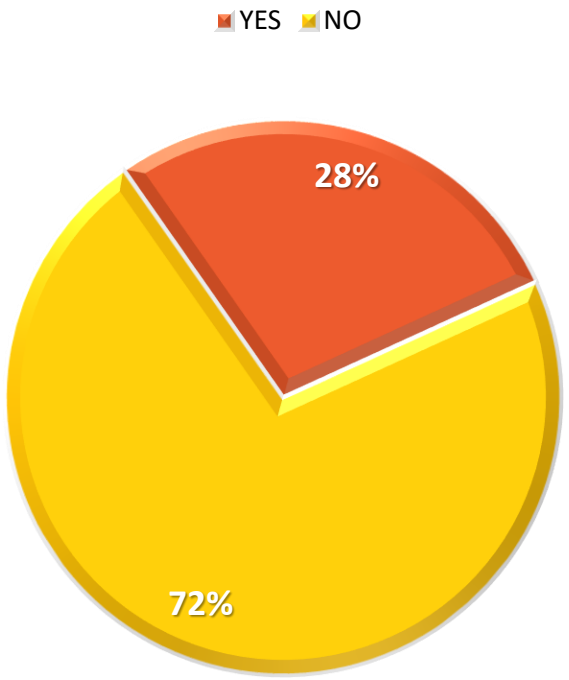
- Attackers Act 150x Faster Than Victims Respond



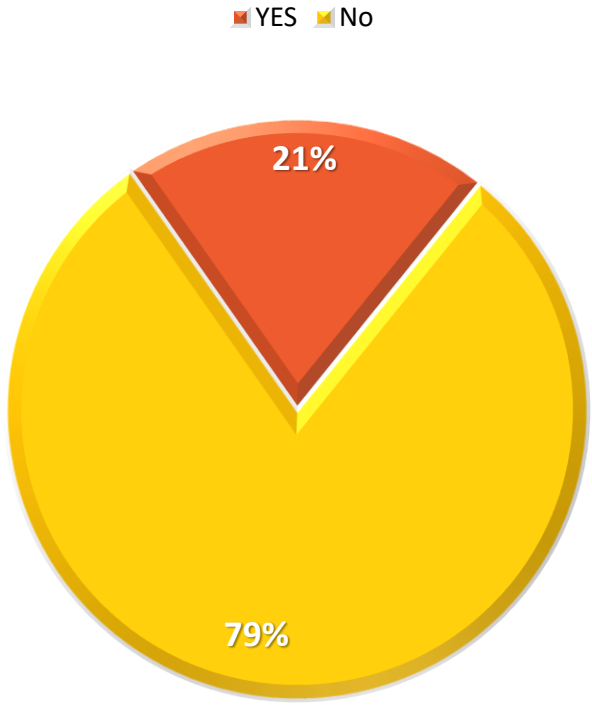
http://www.soltra.com/en/

Gap analysis

Key findings of GCI 2017 on CIIP (LEGAL)



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



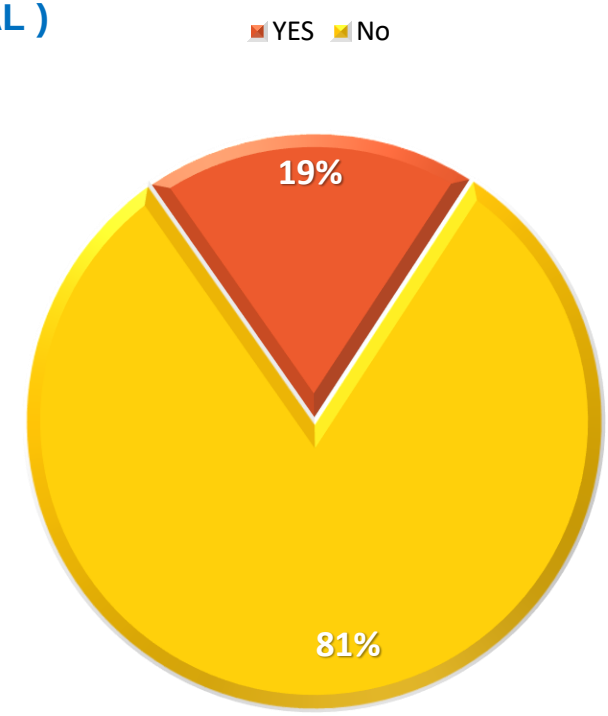
Does the legislation or regulation impose cybersecurity audits on the critical infrastructure operators ?

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

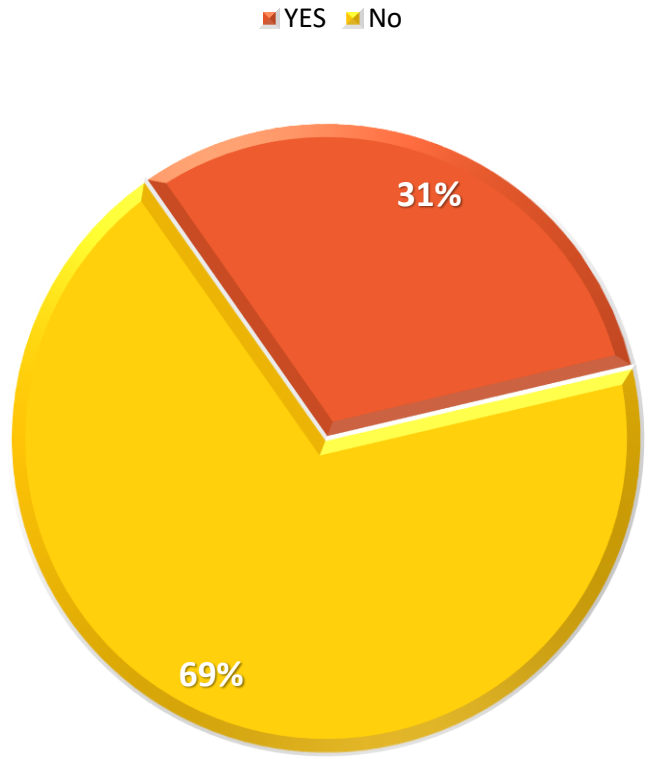
Gap analysis

Key findings of GCI 2017 on CIIP

(ORGANIZATIONAL)



Does national cybersecurity strategy include a national resilience plan ?

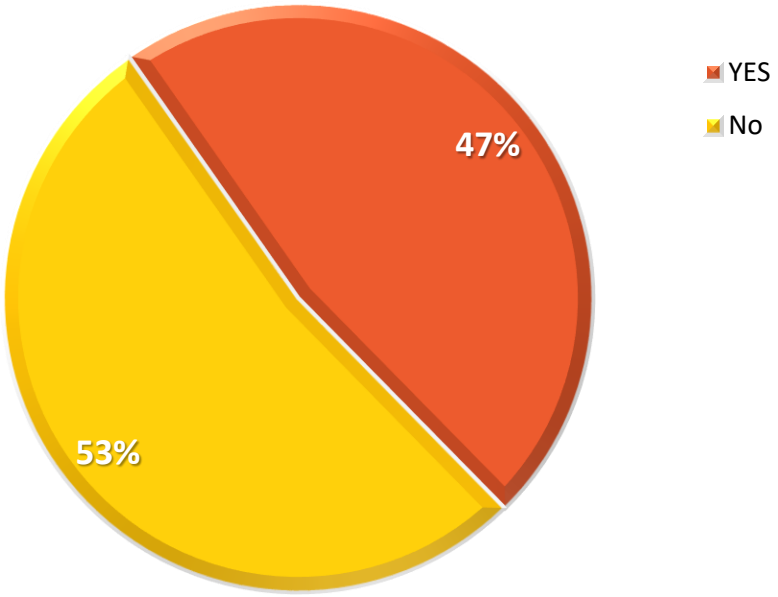


In the national strategy for cybersecurity , Is there a section on the protection of critical information infrastructure?

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

Gap analysis

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

- **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

The Role of the national CIRT in the CIIP

What is a National CIRT?

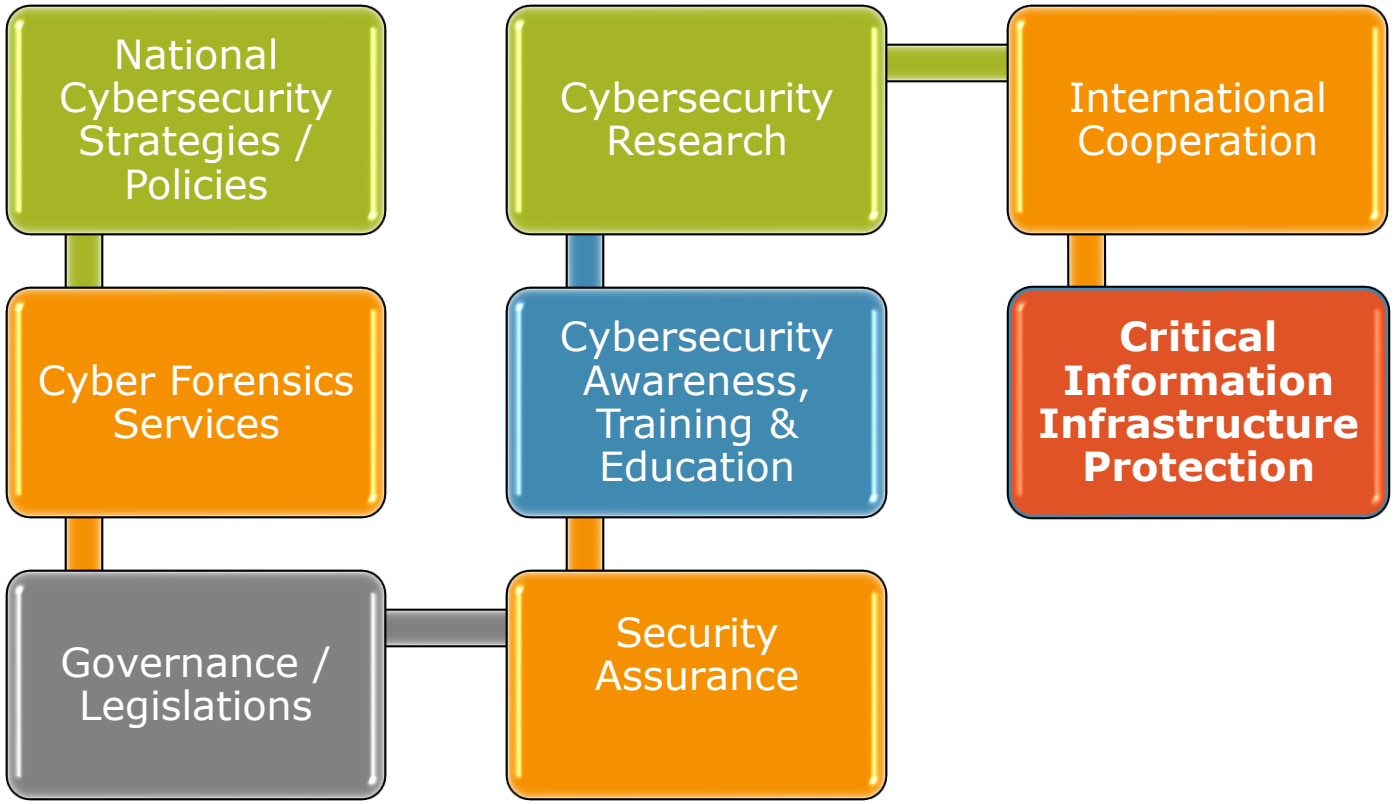
A national / governmental CERT typically handles incidents at a national level, identifies incidents that could affect critical infrastructures, warns critical stakeholders about computer security threats, and helps to build effective incident response across its constituency in both, public and private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

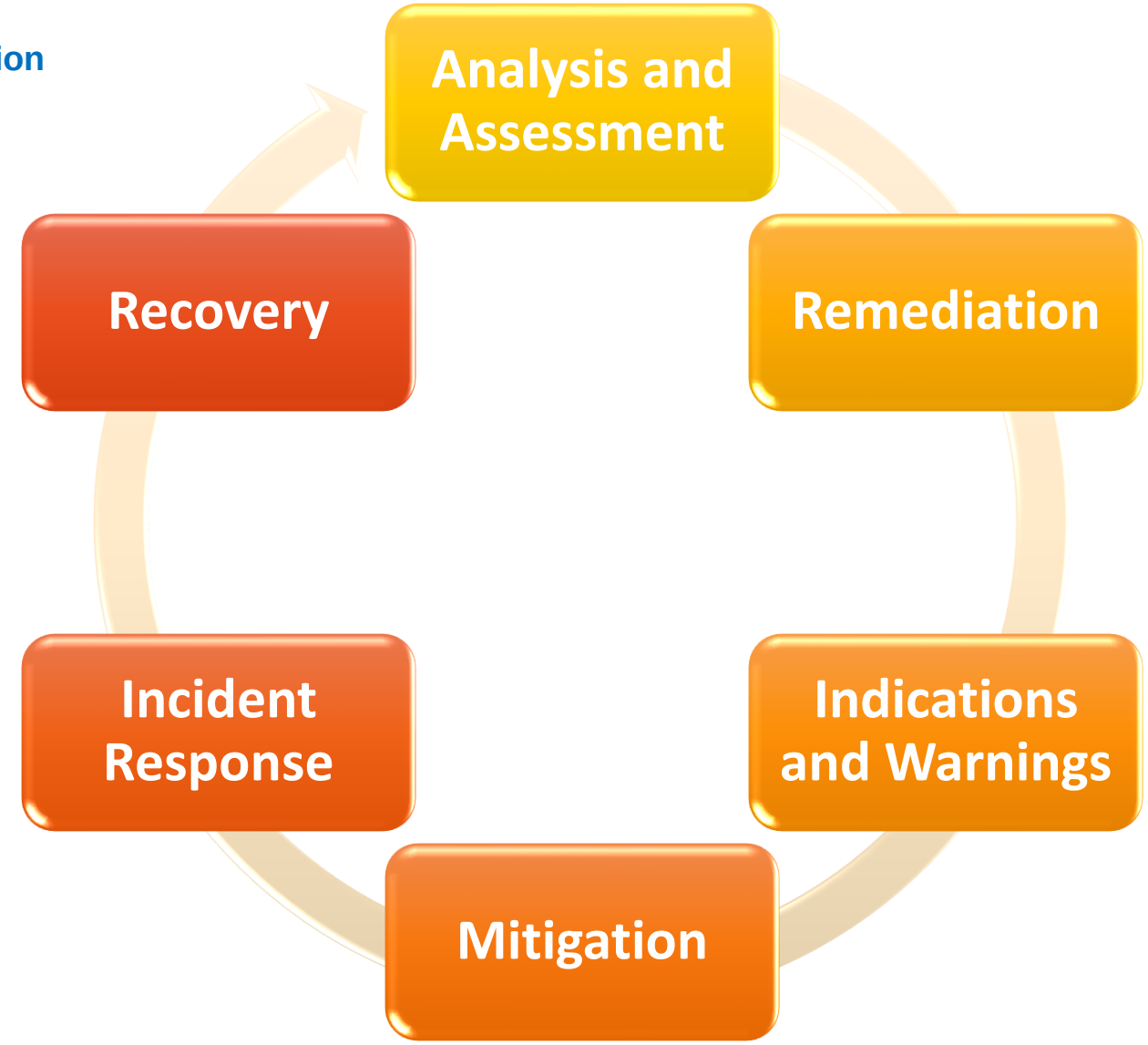
CIRT The Role of the national CIRT in the CIIP

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

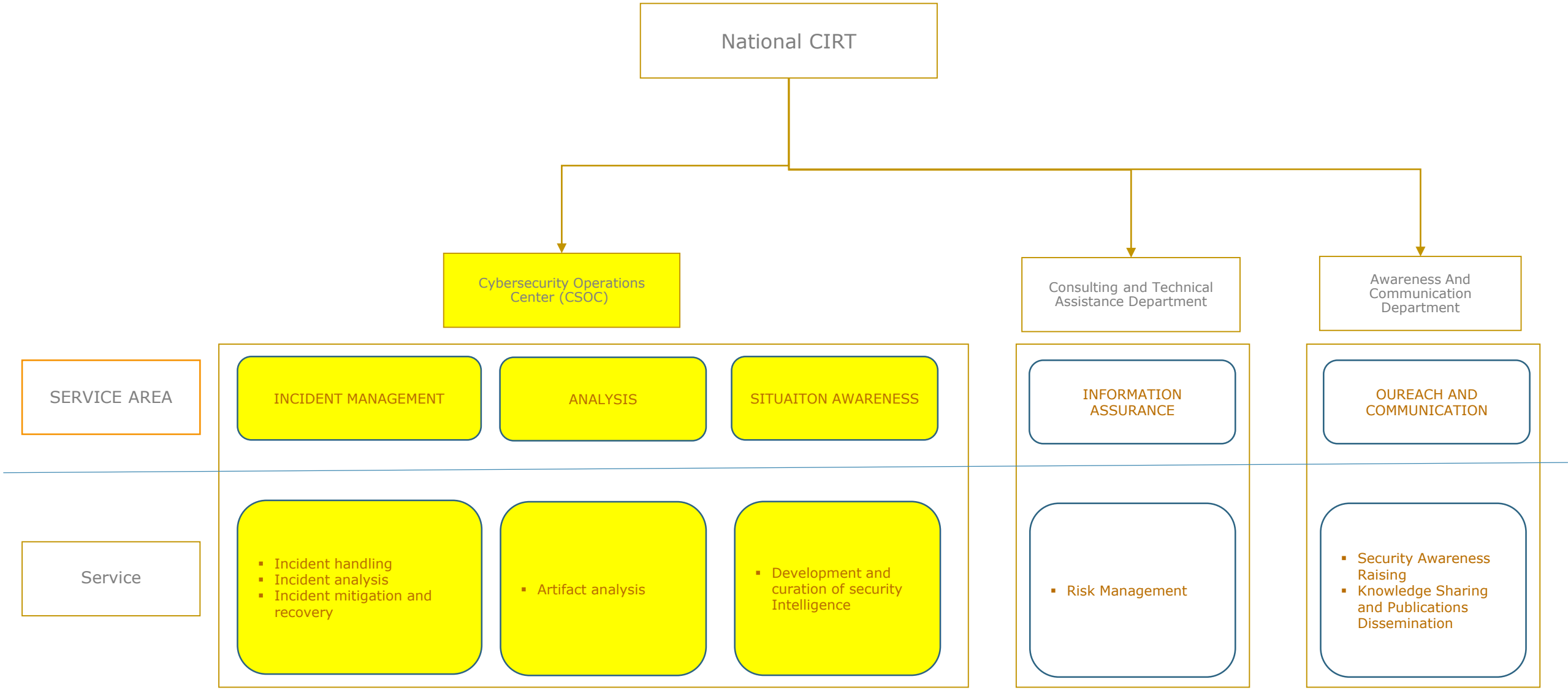
Role of CIRT within the CIIP

- 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

CIRT ➔

Better Detect, Investigate and Respond to Security Incidents that target the CNII

The Basic Services Offered by a CIRT



Cybersecurity Operations Center (CSOC)

Cybersecurity Operations Center (CSOC)