Building Trust in Digital World

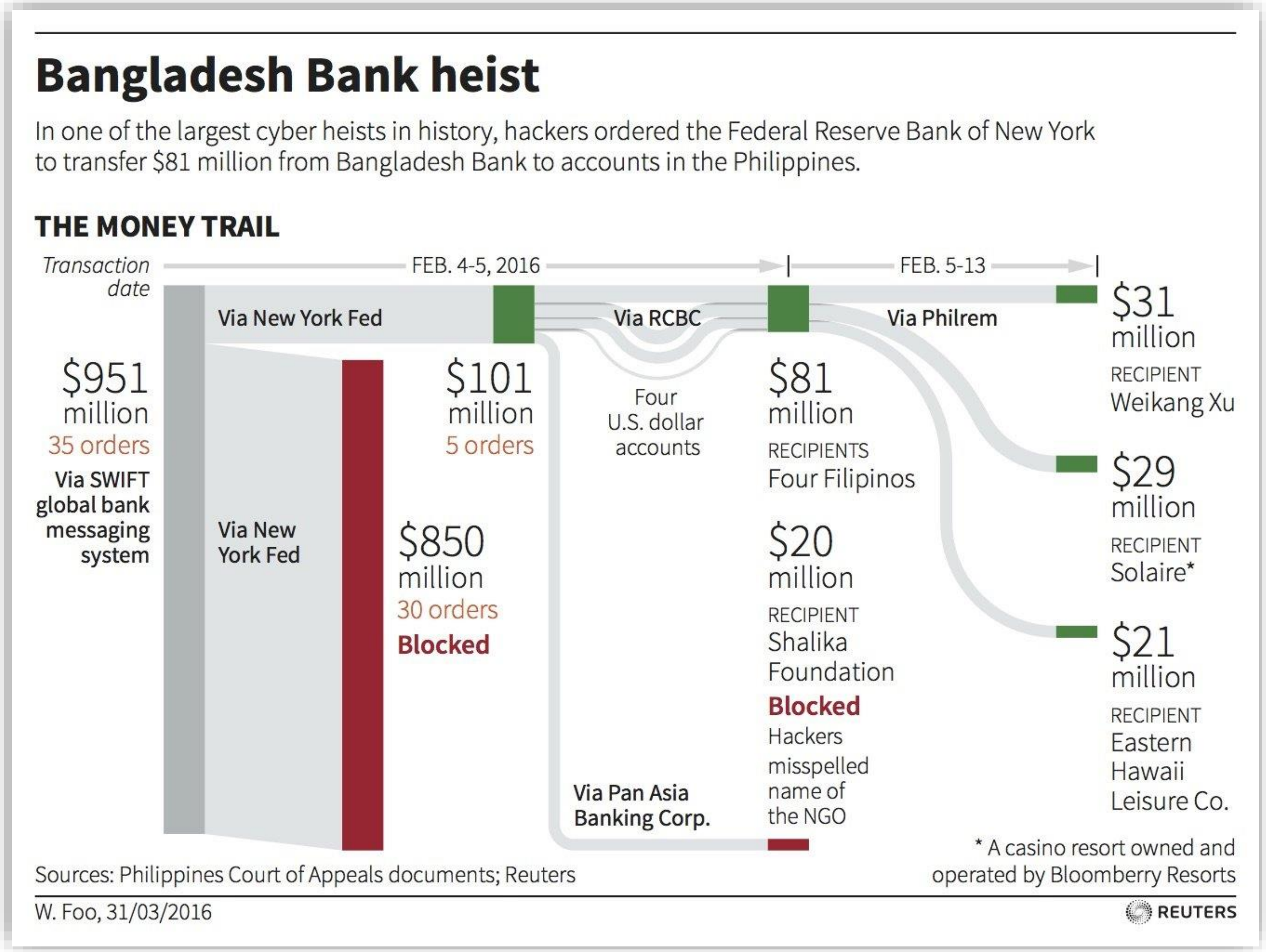
Sameer Sharma
ITU

Bangkok, Thailand
4-6 September 2019

Threats to Critical National Infrastructure-I

Bangladesh 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

* A casino resort owned and operated by Bloomberry Resorts

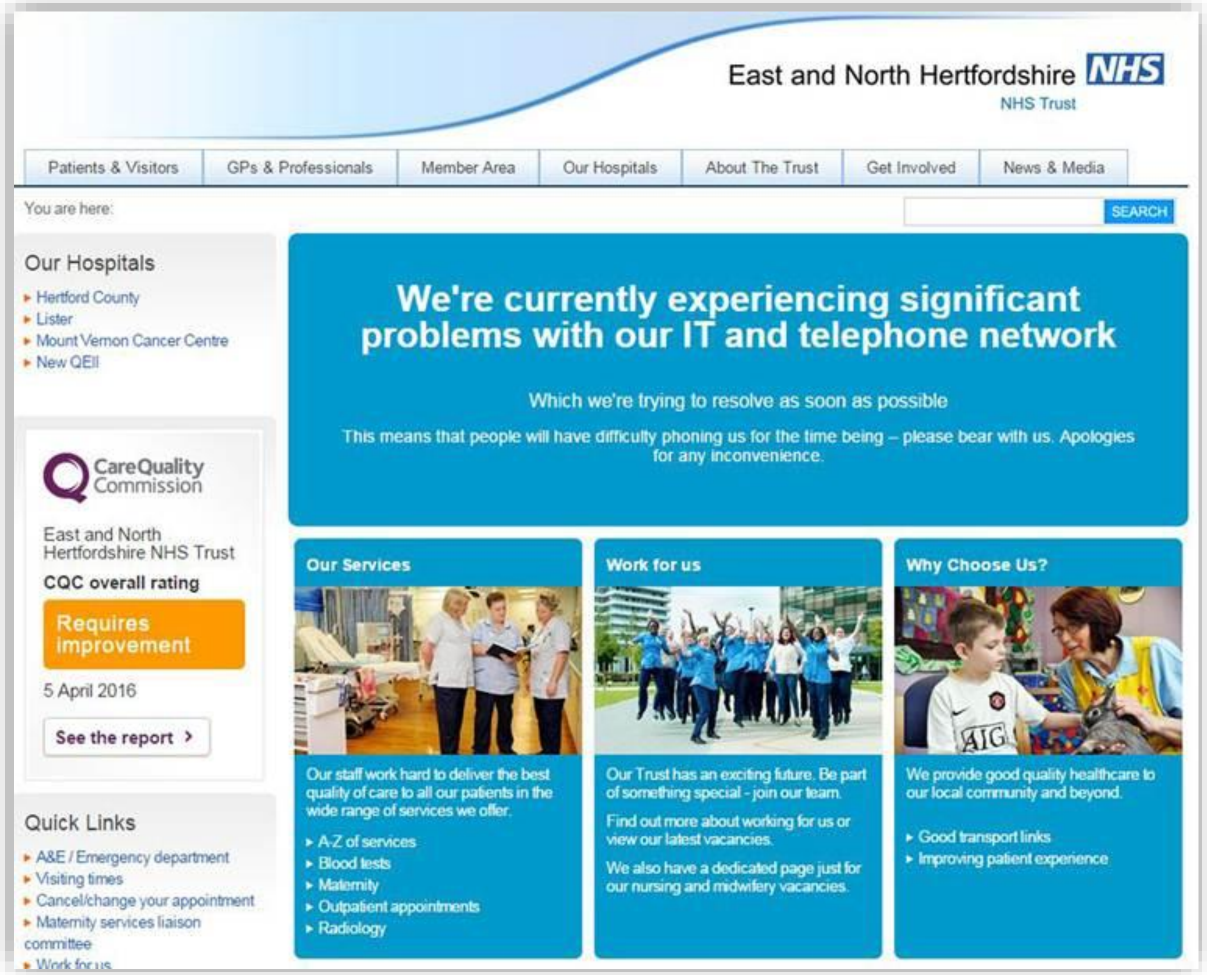
Sources: Philippines Court of Appeals documents; Reuters

W. Foo, 31/03/2016

REUTERS

Threats to Critical National Infrastructure-II

WannaCry Ransomware May 2017



Our Hospitals

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

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.

East and North Hertfordshire NHS Trust

CQC overall rating

Requires improvement

5 April 2016

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.

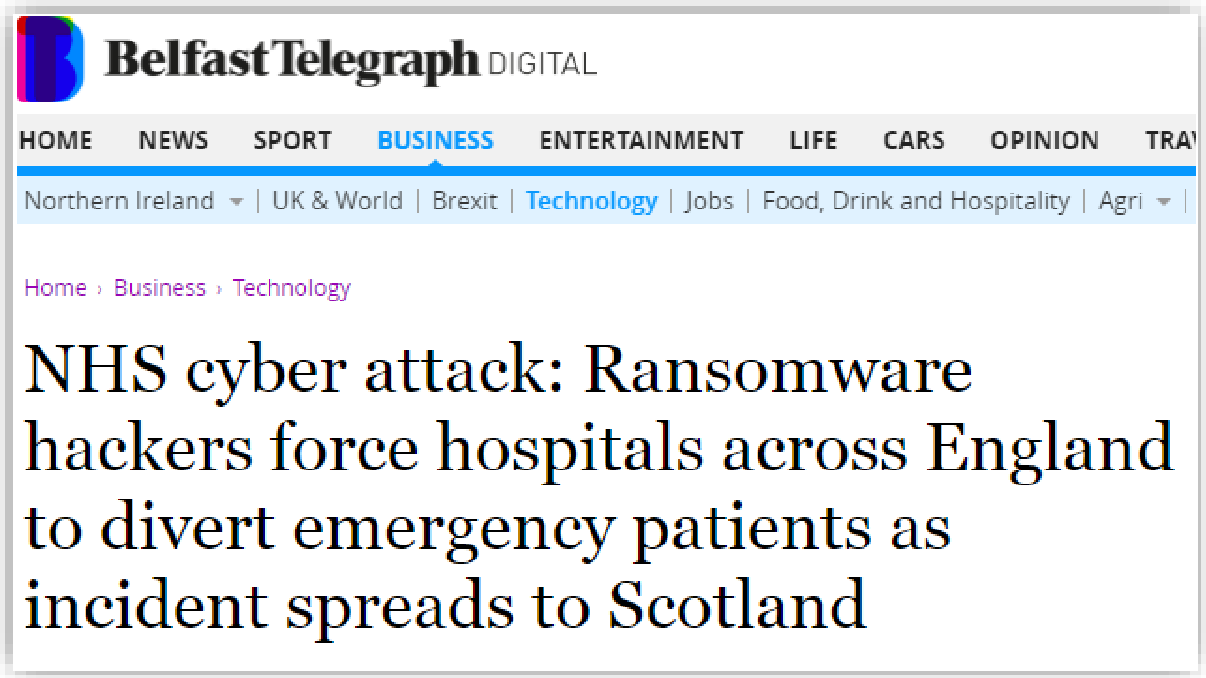
Why Choose Us?

We provide good quality healthcare to our local community and beyond.

- Good transport links
- Improving patient experience

Quick Links

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

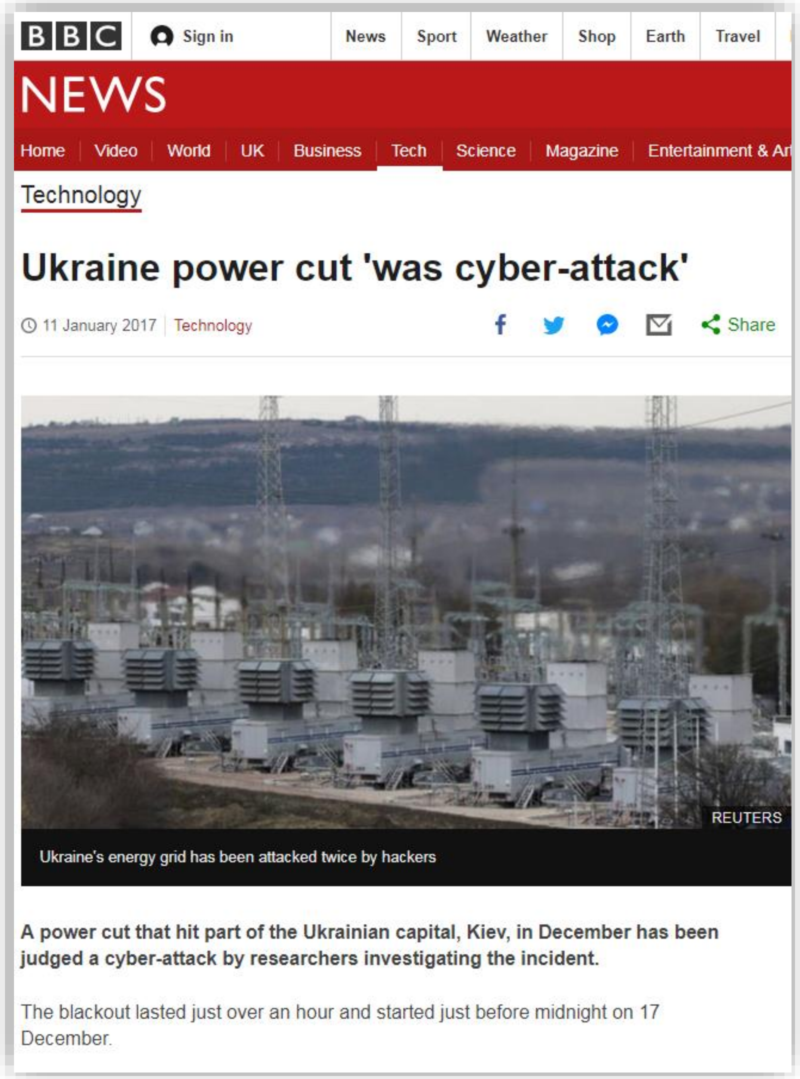


Home › Business › Technology

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

Threats to Critical National Infrastructure-III

Kiev's
power grid
December 2016



Technology

Ukraine power cut 'was cyber-attack'

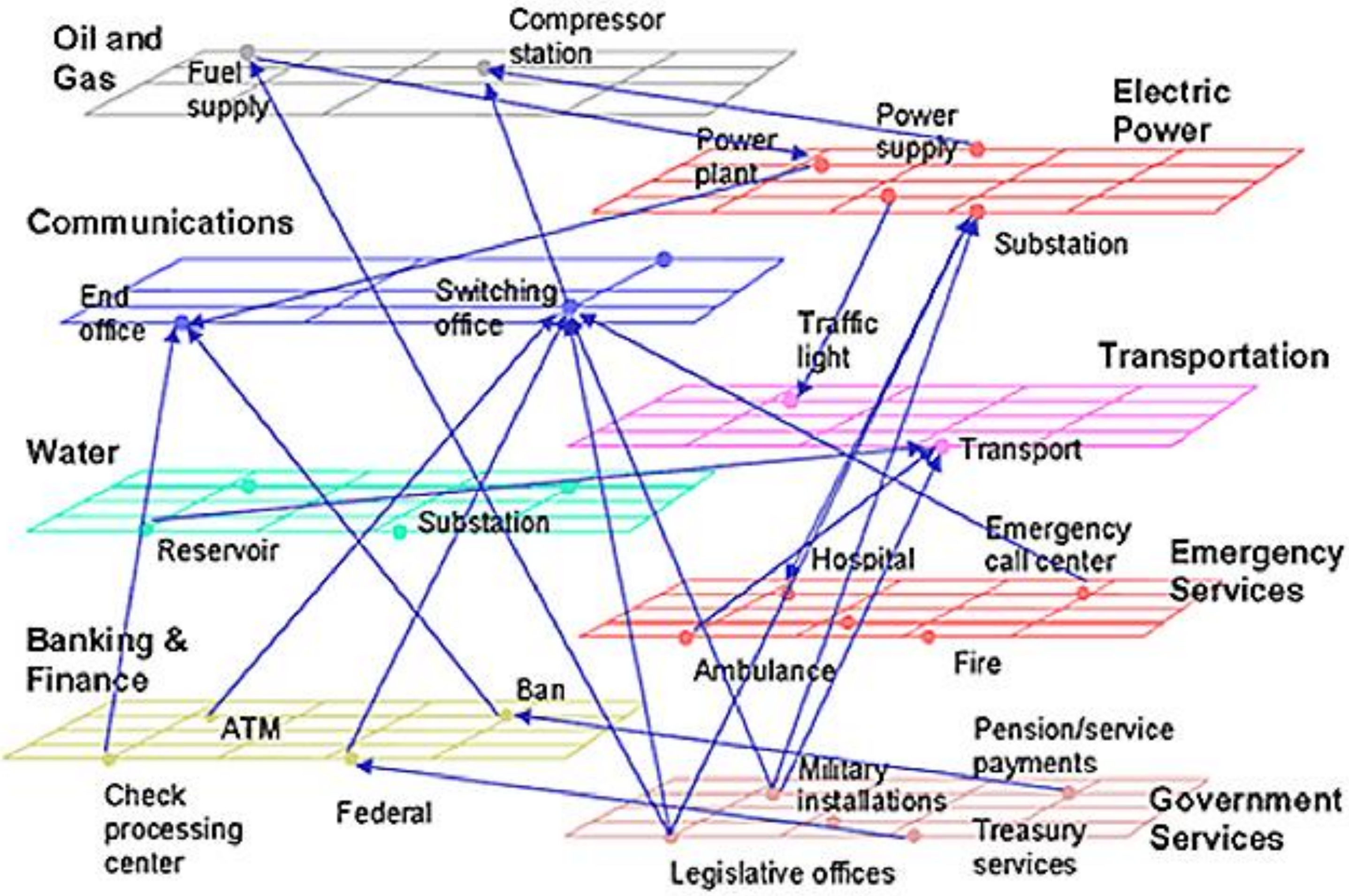
11 January 2017 | Technology

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.

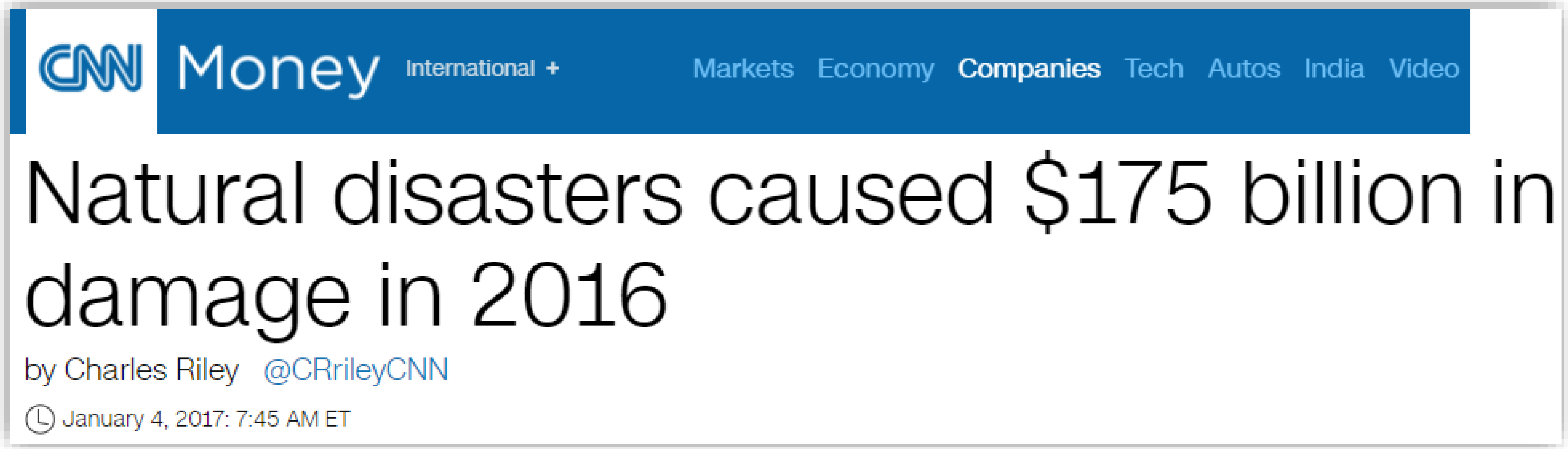
Interconnected Nature of Critical Infrastructure



Cascade effect

Source : NSA

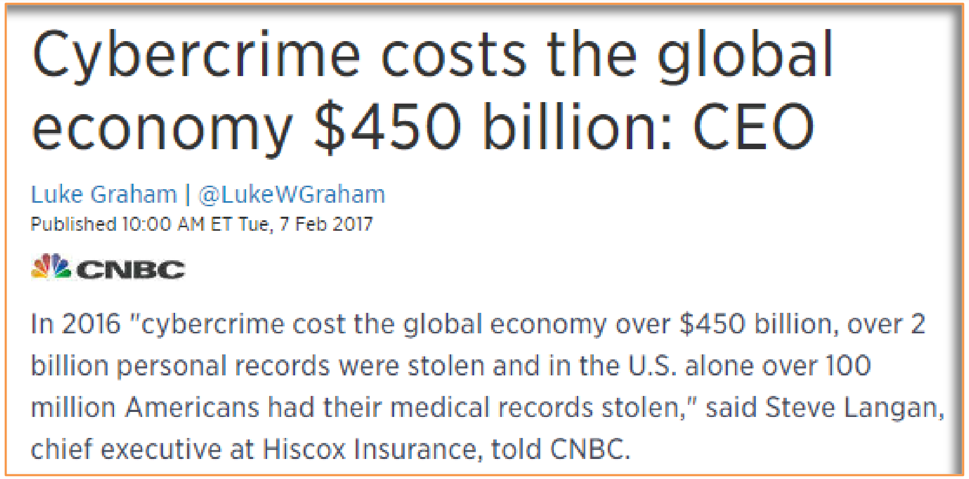
Cybercrime : Cost to Global Economy?



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

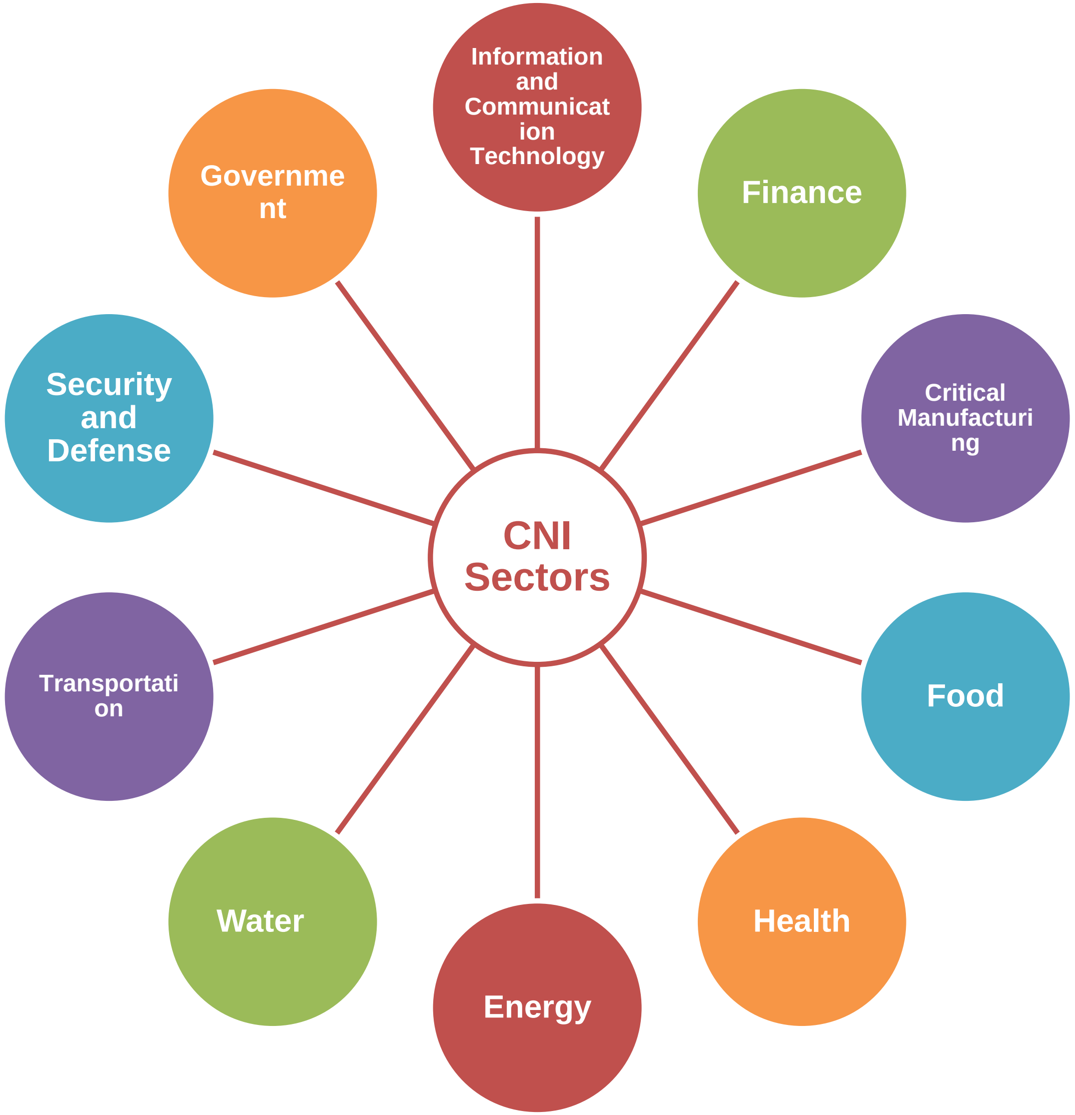
Luke Graham | @LukeWGraham

Published 10:00 AM ET Tue, 7 Feb 2017

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.

Critical National Infrastructure Sectors

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



CNI Sectors

Information and Communication Technology

Finance

Critical Manufacturing

Food

Health

Energy

Water

Transportation

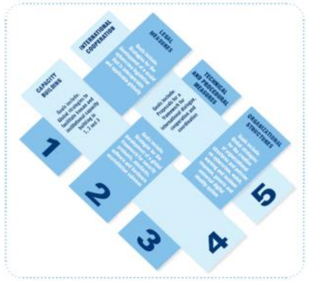
Security and Defense

Government

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


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

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.

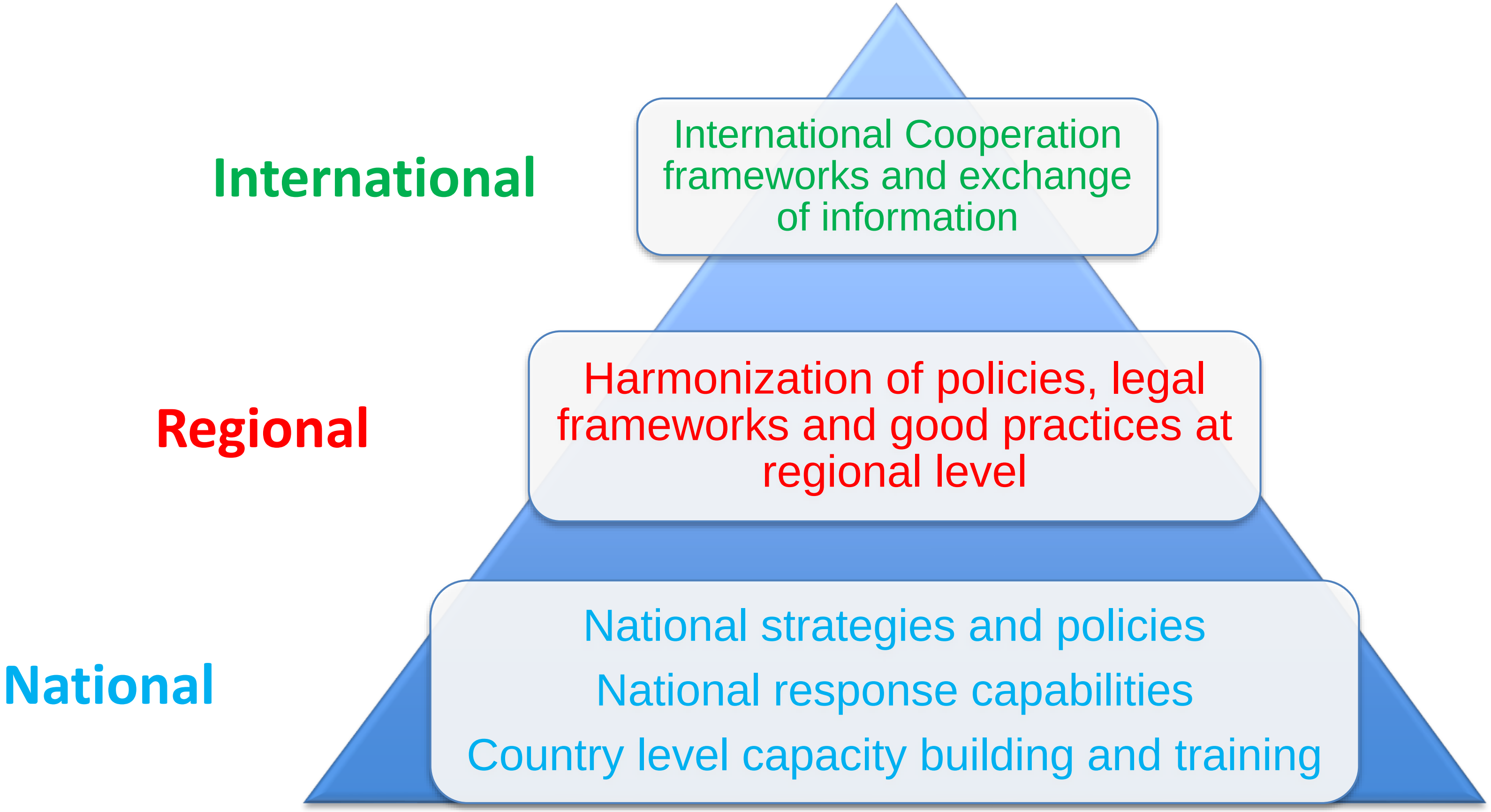
GCA GLOBAL CYBERSECURITY AGENDA

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.

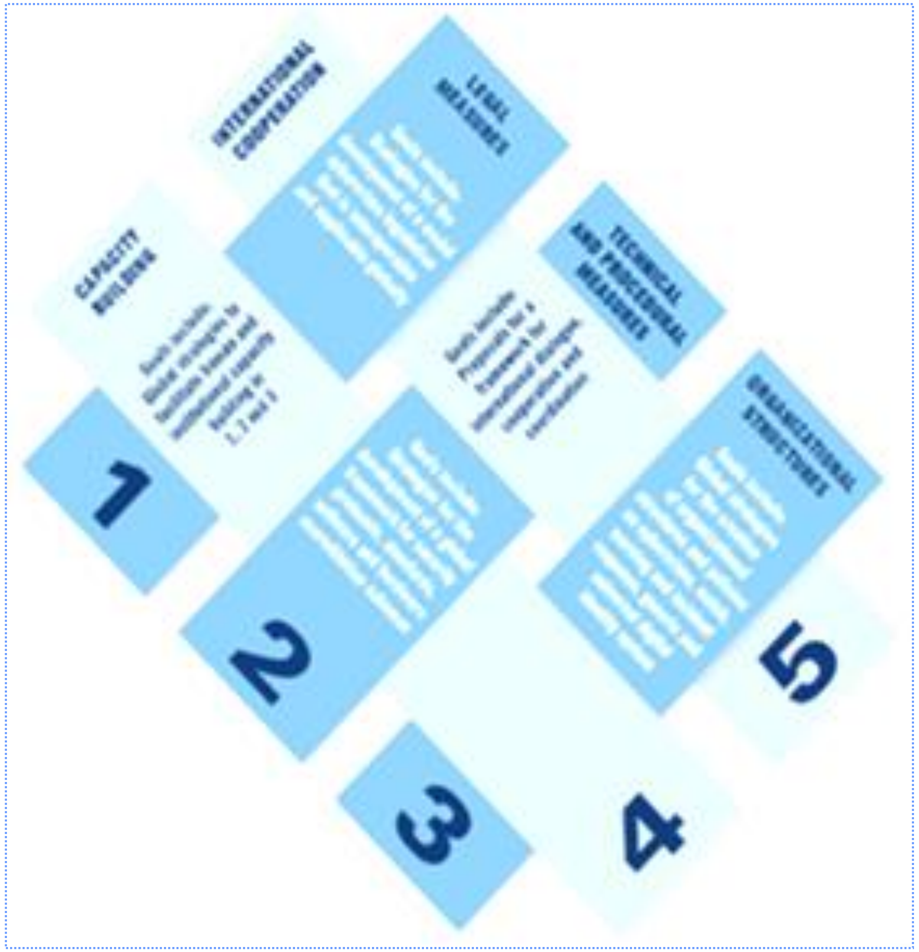
Coordinated Response

Need for a multi-level response to the cybersecurity challenges

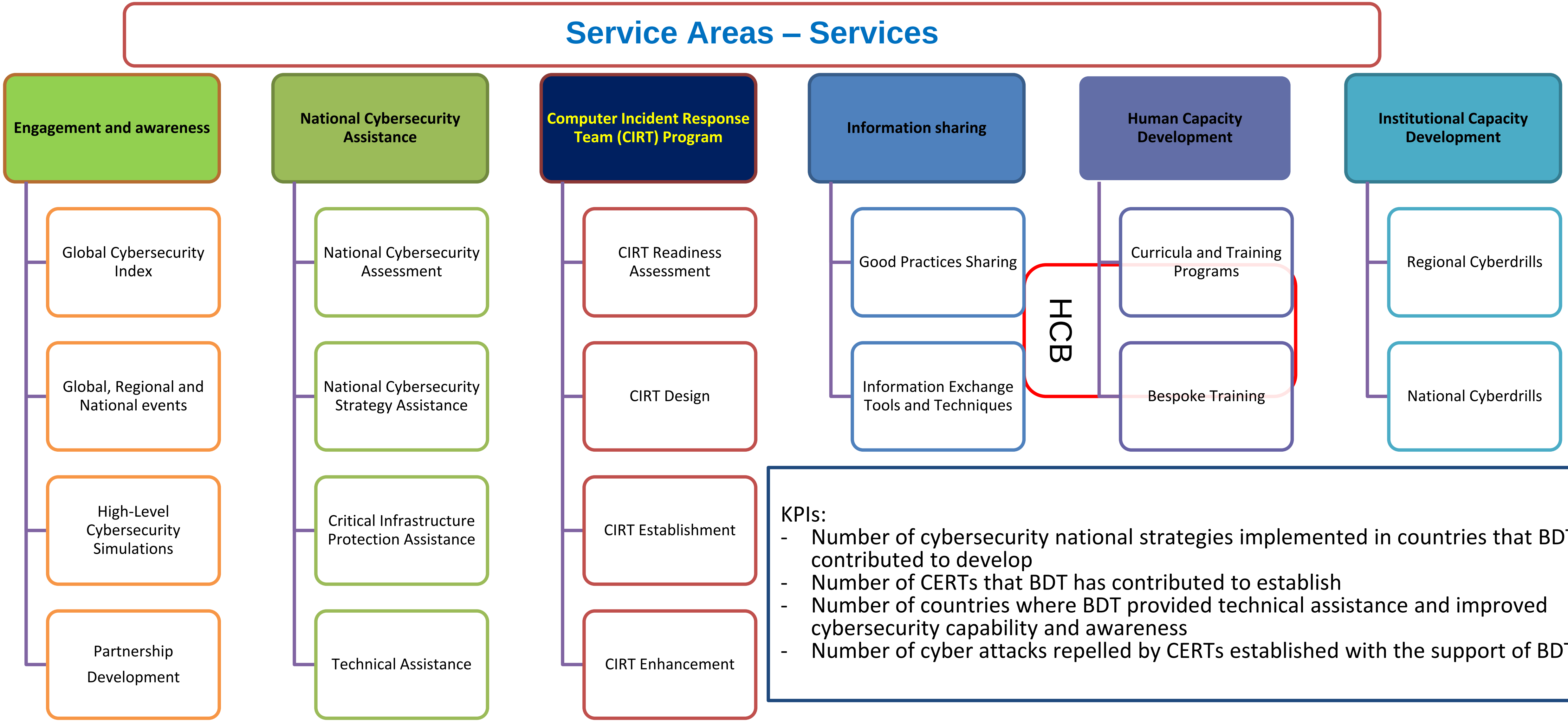

International
International Cooperation frameworks and exchange of information
Regional
Harmonization of policies, legal frameworks and good practices at regional level
National
National strategies and policies
National response capabilities
Country level capacity building and training

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

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 Assistance
- Critical Infrastructure Protection Assistance
- Technical Assistance

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

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

Human Capacity Development
- Curricula and Training Programs
- Bespoke Training

HCB

Institutional Capacity Development
- Regional Cyberdrills
- National Cyberdrills

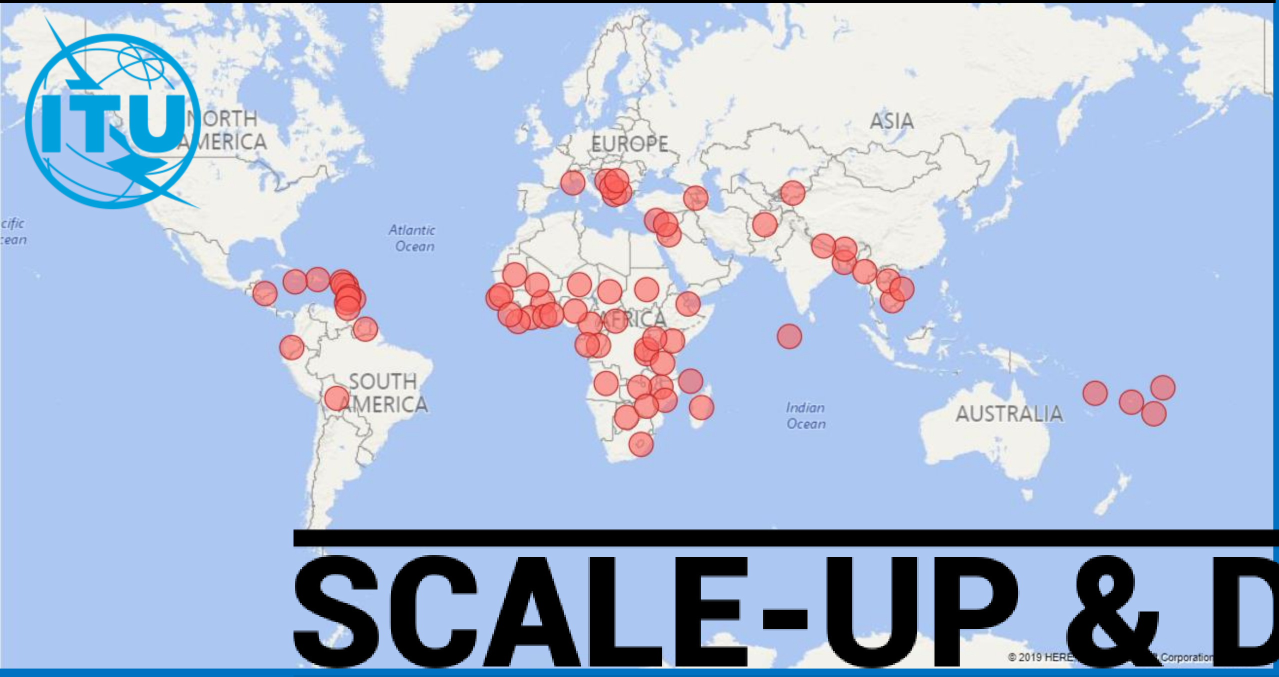
KPIs:
- Number of cybersecurity national strategies implemented in countries that BDT contributed to develop
- Number of CERTs that BDT has contributed to establish
- Number of countries where BDT provided technical assistance and improved cybersecurity capability and awareness
- Number of cyber attacks repelled by CERTs established with the support of BDT

CIRT Services

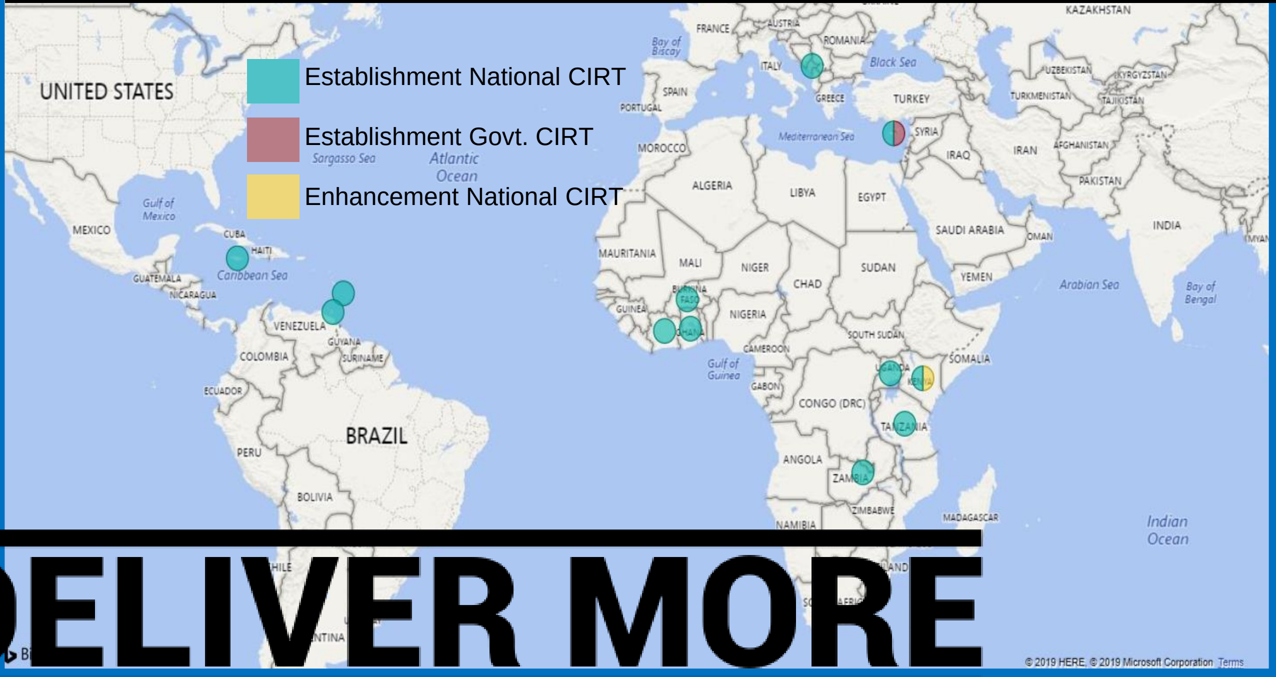
SCALE-UP & DELIVER MORE

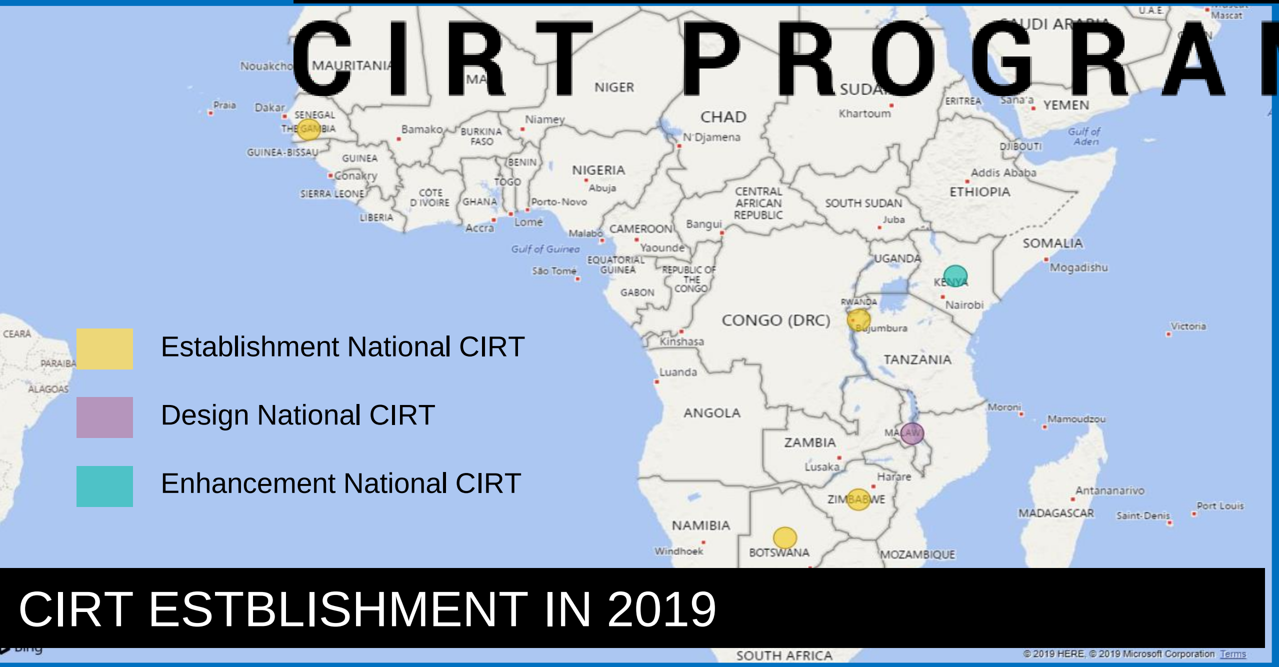
CIRT PROGRAMME EXAMPLE

75 CIRT READINESS ASSESSMENTS

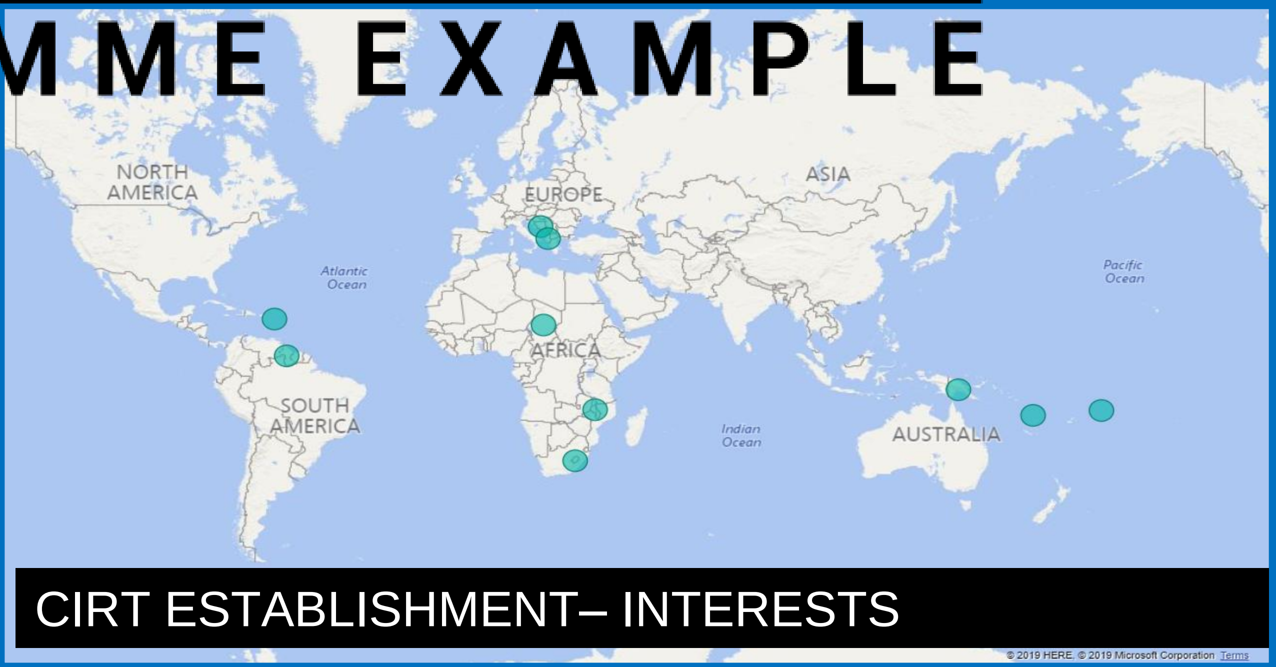


13 CIRT ESTABLISHMENT + 1 ENHANCEMENT


🟦 Establishment National CIRT
🟥 Establishment Govt. CIRT
🟨 Enhancement National CIRT
UNITED STATES
BRAZIL
Atlantic Ocean
Indian Ocean
© 2019 HERE, © 2019 Microsoft Corporation Terms

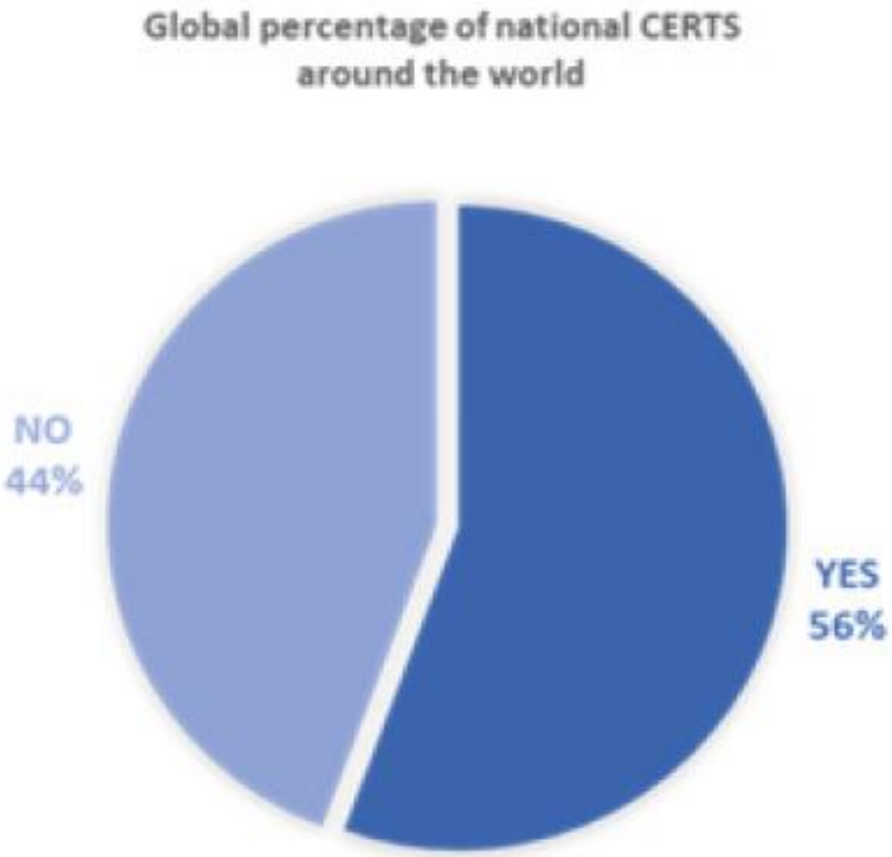


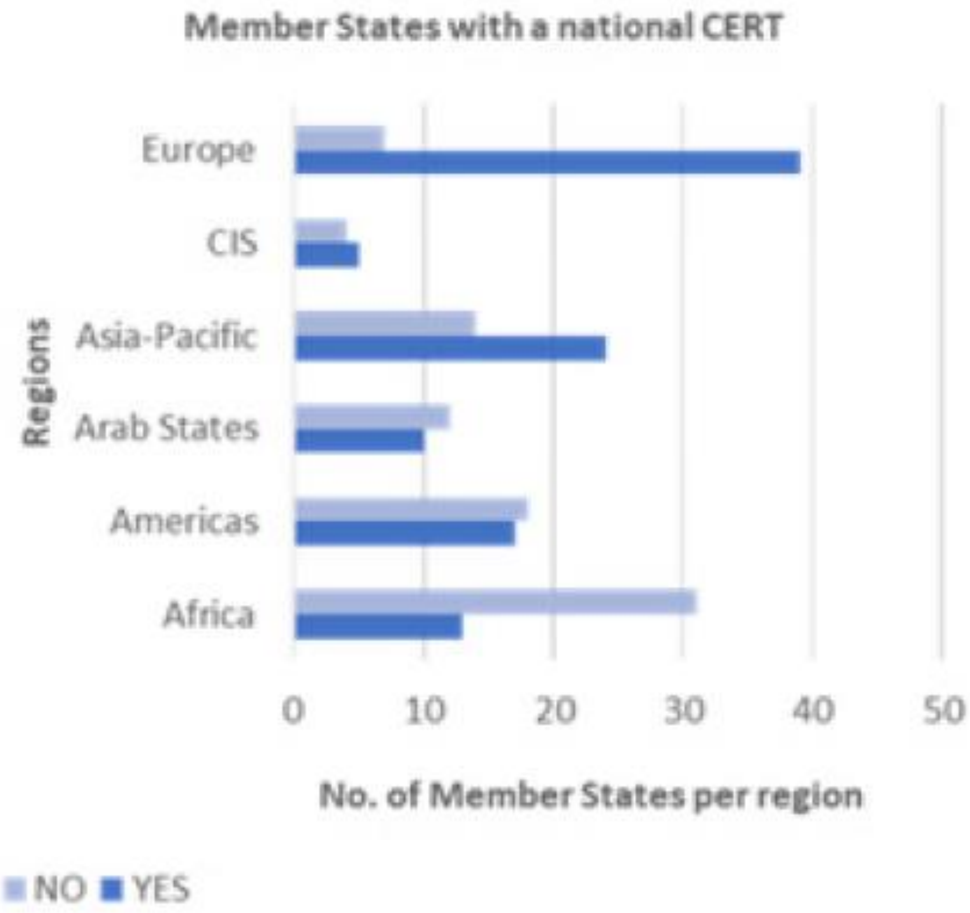
CIRT ESTBLISHMENT IN 2019



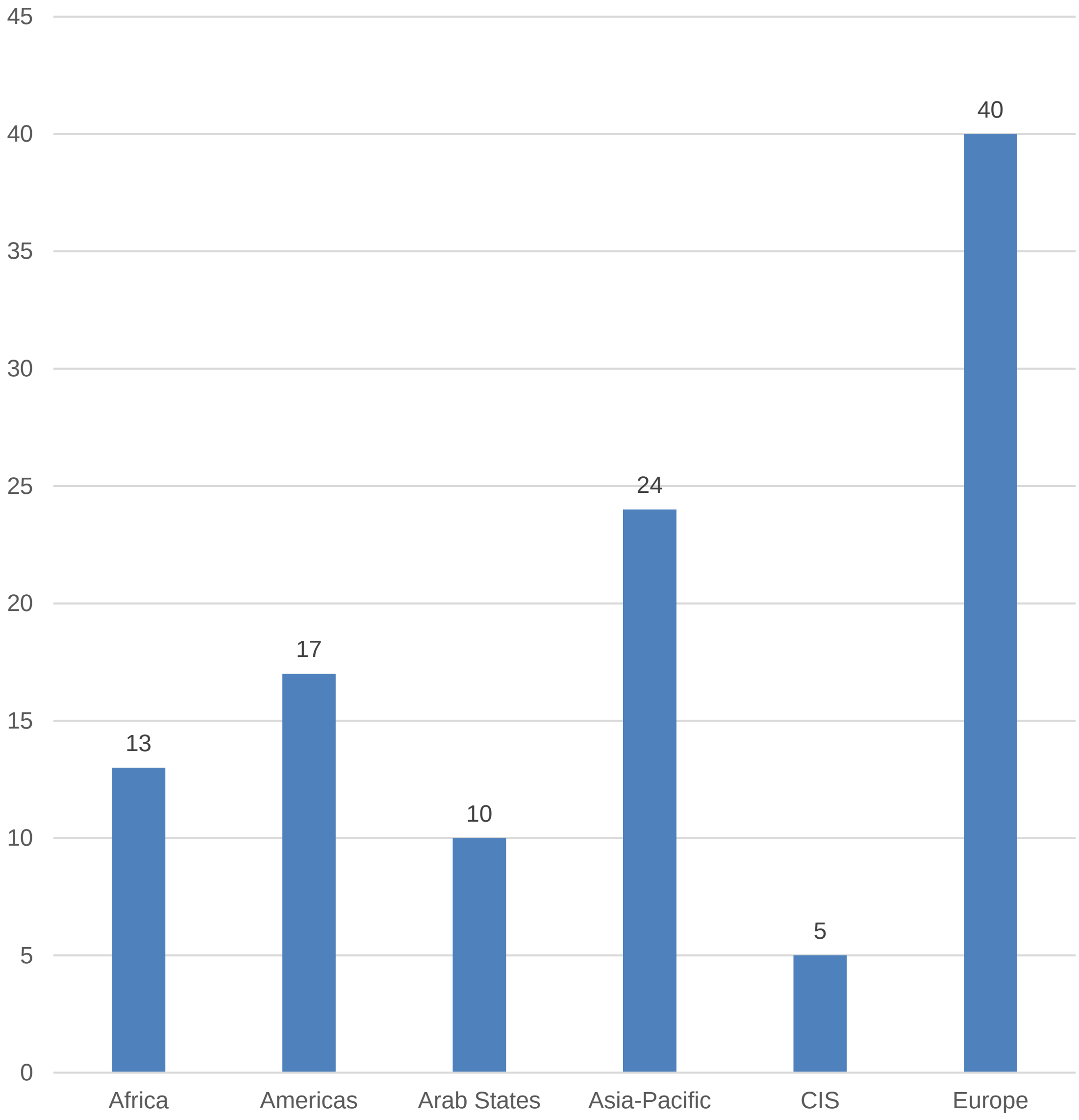
CIRT ESTABLISHMENT– INTERESTS

National CERT/CIRT/CSIRT globally and per region





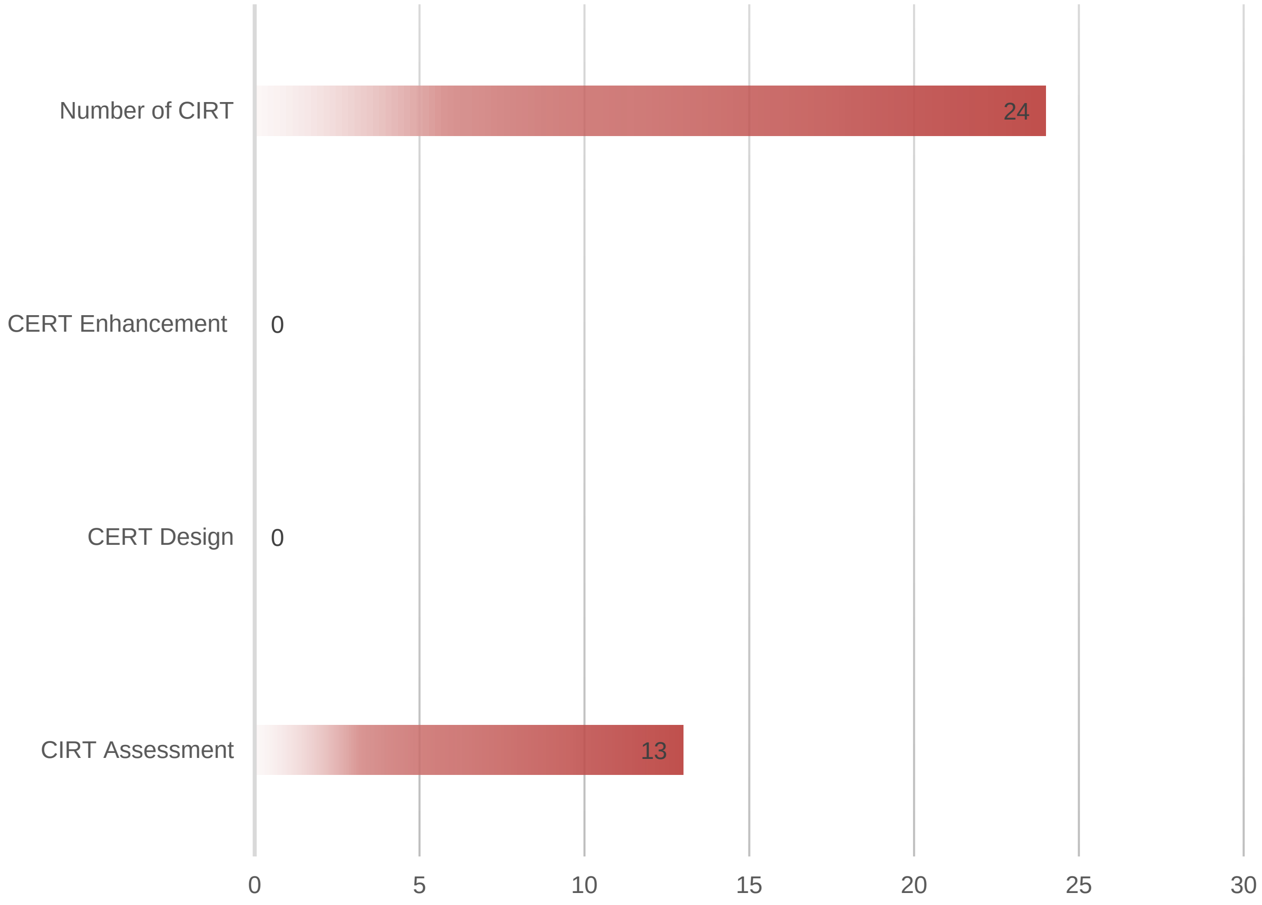
Number of CIRT activities around the world



CIRTs in Asia-Pacific:

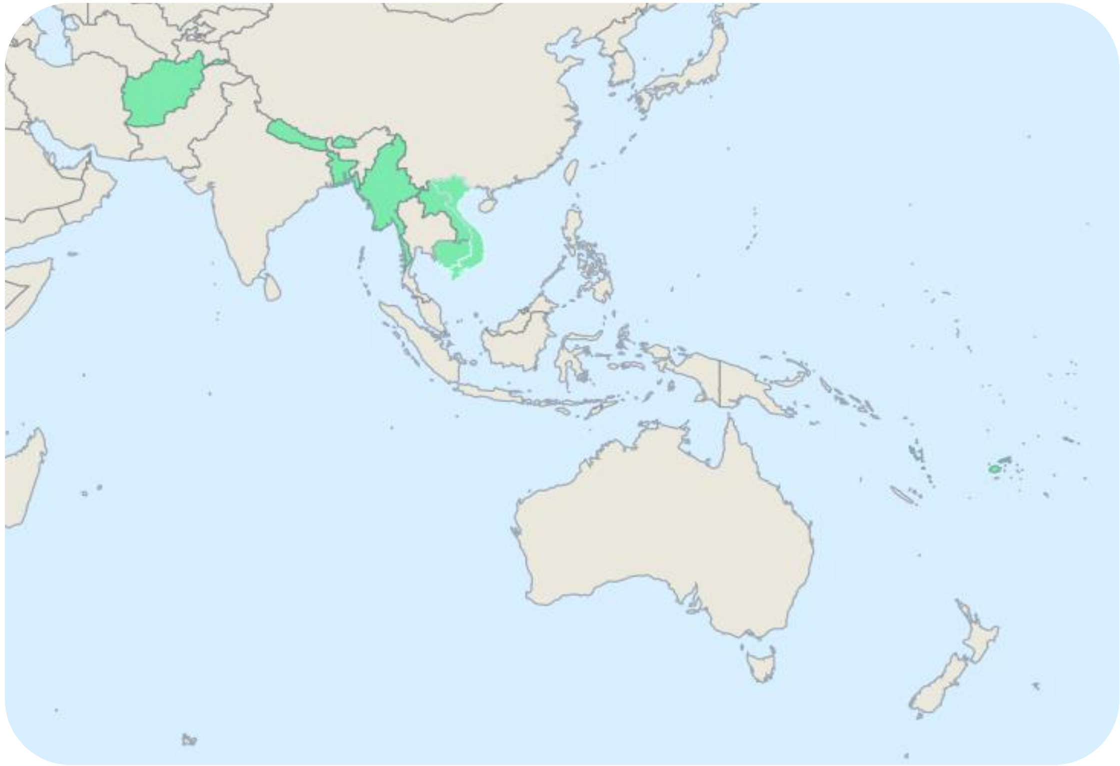
Afghanistan, Australia, Bangladesh,
Brunei Darussalam, Cambodia, China, India, Indonesia, Iran, Japan, Laos, Malaysia, Myanmar, New Zealand, Pakistan, Papua New Guinea, Philippines, Republic of Korea, Singapore, Sri Lanka, Thailand, Tonga, Vanuatu, Viet Nam

Good Practices: An analysis of the Asia-Pacific CIRT establishment



13 CIRT assessment done by ITU in Asia-Pacific :

Afghanistan, Bangladesh , Bhutan, Cambodia, Fiji, Laos, Maldives, Myanmar, Nepal , Samoa, Tonga, Vanuatu, Vietnam



EXAMPLES OF SOME CYBERSECURITY BEST PRACTICES IN THE REGION

Japan: The National centre of Incident is building an information sharing system among public-private sectors. The Japan National Institute of Information and Communications Technology has established a National Cyber Training Center that has developed many projects, such as CYDER, CYBER COLOSSEO and SecHack 365 (a security innovator training programme for young talents).

Singapore: The Cybersecurity Agency of Singapore (CSA), in partnership with InfoComm Media Development Authority (IMDA), launched the Cyber Security Associates and Technologists (CSAT) programme to encourage industry to train fresh and mid-career professionals in ICT or STEM (Science, Technology, Engineering and Mathematics) for cybersecurity roles through structured on-the-job training and courses.

Mongolia: The Government started a feasibility study to establish a CERT and an IT security audit system for Mongolia. The feasibility study project aims to identify the status of the cybersecurity environment such as the organization/manpower, ICT infrastructure, legal environment and standards, IT security/auditing process, and to investigate a development plan. In addition, this project aims to make a proposal for the To-Be Model of a Mongolia CERT.

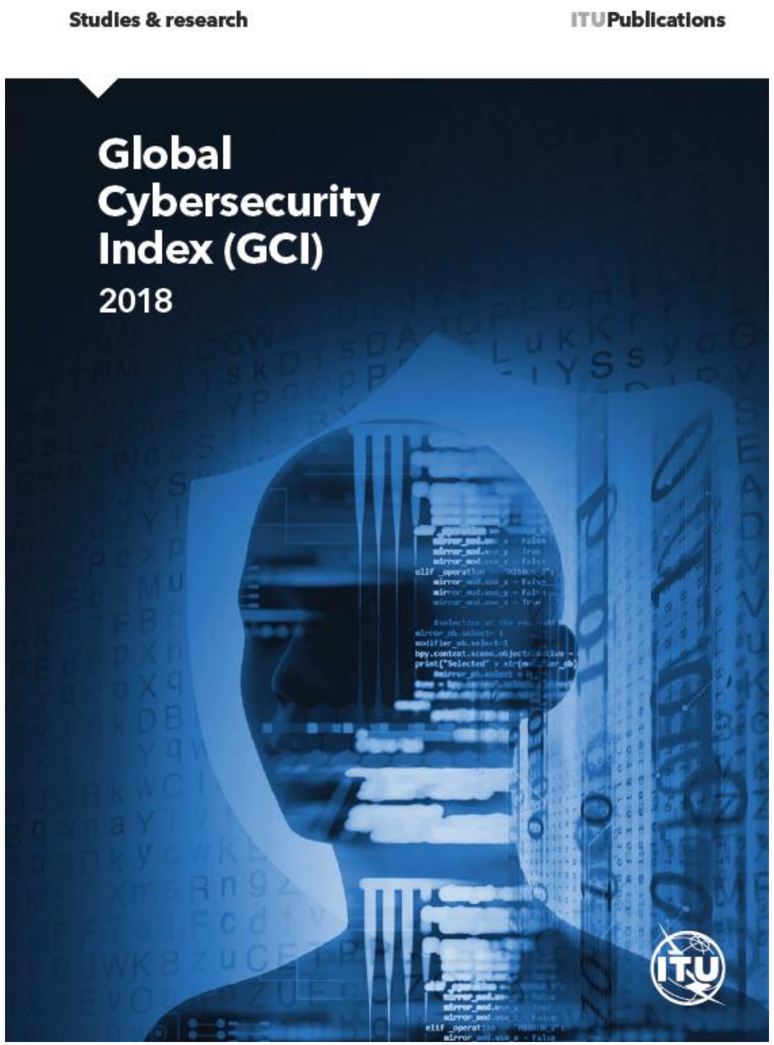
Malaysia: The National Cyber Drill (X-Maya) is testing and improving the technical skills of CNII IT personnel to handle cyber incidents. The Coordinated Malware Eradication and Remediation Project (CMERP) has implemented a pilot project to tackle malware threats at the national level.

Global Cybersecurity Index (GCI)

What is GCI …

GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States’ ***cybersecurity commitment*** with regard to the five pillars identified by the High-Level Experts and endorsed by the GCA.

“GCI is a capacity building tool, to support countries to improve their national cybersecurity”



Studies & research

ITUPublications

Global Cybersecurity Index (GCI)
2018

Background

- GCIv1 – the 1st iteration of the GCI has started in 2013-2014 period -**105** countries responded
- GCIv2 – the 2nd iteration covered 2016-2017 period – **134** countries responded
- **GCIv3 – 3rd iteration <u>started in March 2018 – 137 countries as of today</u>**

ITU
General Secretariat
Radiocommunication
Standardization
Development
ITU Telecom
Members' Zone
Join ITU
About
Accessibility
Join ITU-D
Partners
Projects
Publications
Regional Presence
TDAG
WTDC
Study Groups
YOU ARE HERE HOME > ITU-D > CYBERSECURITY > GLOBAL CYBERSECURITY INDEX
SHARE
About
National Strategies
Legal Measures
CIRT Programme
Global Cybersecurity Index
Combating SPAM
Global Partnerships
Cyberthreat Insight
Publications
Events
Documents
Previous versions
Media
GLOBAL CYBERSECURITY INDEX
GCIv3
MEASURING COMMITMENT TO CYBERSECURITY
LEGAL
Cybercriminal Legislation, Substantive law, Procedural cybercriminal law, Cybersecurity Regulation.
TECHNICAL
National CIRT, Government CIRT, Sectoral CIRT, Standards for organizations, Standardization body.
ORGANIZATIONAL
Strategy, Responsible agency, Cybersecurity metrics.
CAPACITY BUILDING
Public awareness, Professional training, National education programmes, R&D programmes, Incentive mechanisms, Home-grown industry.
COOPERATION
Intra-state cooperation, Multilateral agreements, International fora, Public-Private partnerships, Inter-agency partnerships.
PARTN
RESPO
#ICT4SDG
Global Cybersecurity Index
GCI 2017
GCI 2014

Global Cybersecurity Index

The Global Cybersecurity Index (GCI) is a multi-stakeholder initiative to measure the commitment of countries to cybersecurity. Cybersecurity has a wide field of application that cuts across many industries and sectors. Each country's level of development will therefore be analyzed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation.

- Invitation letter (English, عربي, 中文, Español, Français, Русский)
- Questionnaire guide (English, عربي, 中文, Español, Français, Русский)
- Guidelines to Member States
- Reference model
- Tentative timeframe

GCIV3

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.The 3rd iteration of GCI was elaborated with an enhanced index, more open consultations and more partners. A multi-stakeholder approach, that leverages the expertise of different organizations, with the objectives of improving the quality of the GCI, instigating international cooperation, and promoting knowledge exchange on this topic, has been formulated.

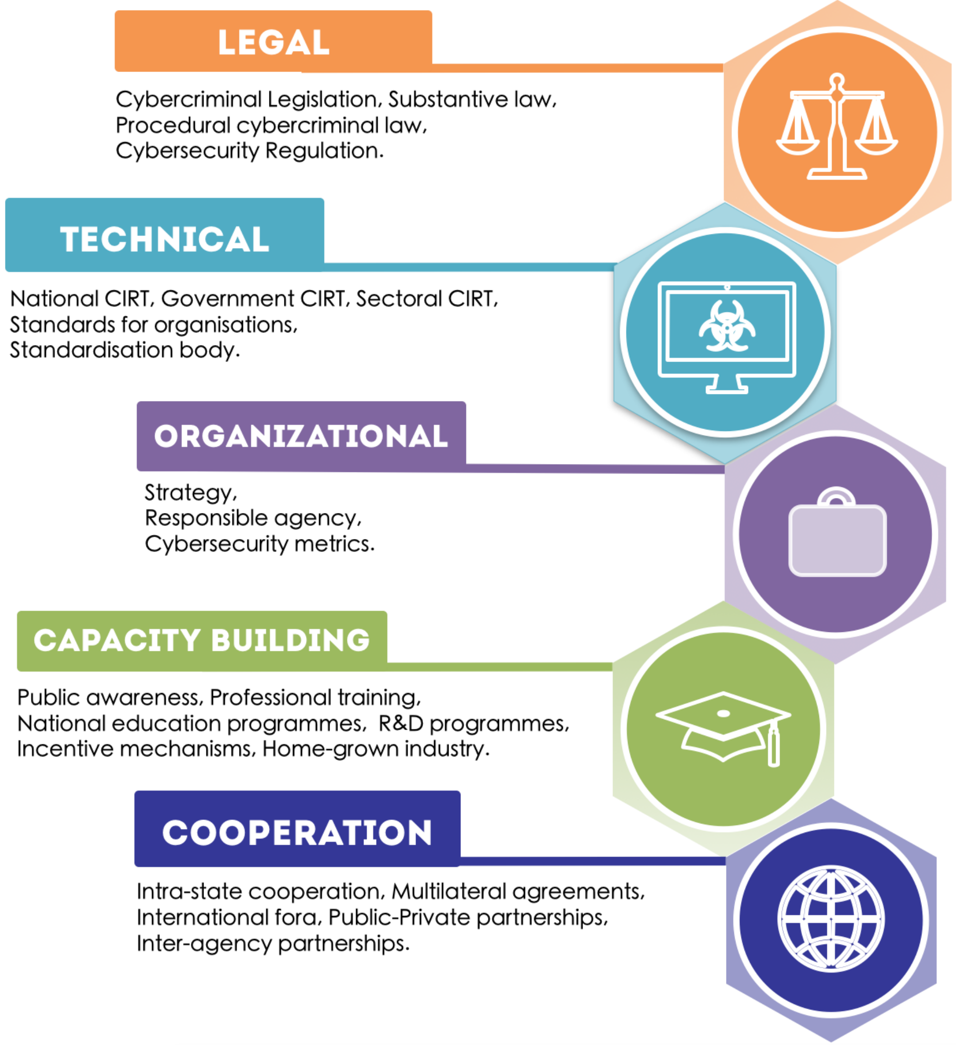
The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was also collected.

All iterations include primary research in order to provide global coverage of the 194 Member States

GCI overall approach

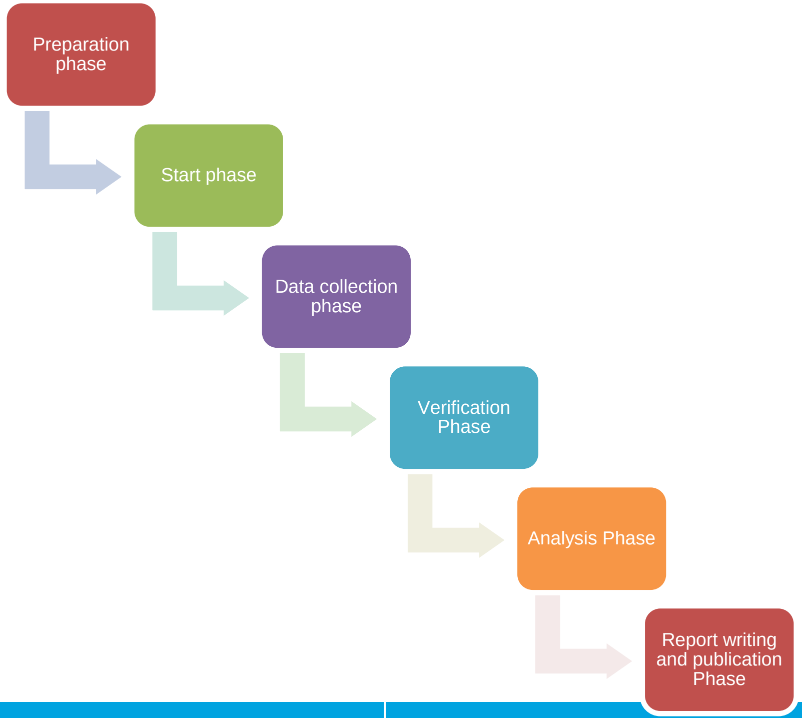
The GCIv3 includes 25 indicators and 50 questions. The indicators used to calculate the GCI were selected on the basis of the following criteria:

- relevance to the five GCA (Global Cybersecurity Agenda) pillars and in contributing towards the main GCI objectives and conceptual framework;
- data availability and quality;
- possibility of cross verification through secondary data.

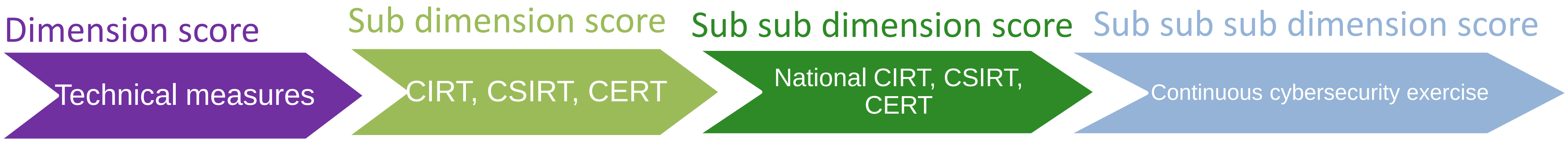

LEGAL
Cybercriminal Legislation, Substantive law,
Procedural cybercriminal law,
Cybersecurity Regulation.
TECHNICAL
National CIRT, Government CIRT, Sectoral CIRT,
Standards for organisations,
Standardisation body.
ORGANIZATIONAL
Strategy,
Responsible agency,
Cybersecurity metrics.
CAPACITY BUILDING
Public awareness, Professional training,
National education programmes, R&D programmes,
Incentive mechanisms, Home-grown industry.
COOPERATION
Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.

How it functions. Main steps.

- Preparation phase
  - Elaboration of the survey in collaboration with experts and partners
  - Development of online survey system
  - Preparation of supporting documentation (guides, conceptual framework, letters etc.)
  - Announcement on the ITU website
- Start phase
  - Informing/invitation Member States via official letter from the BDT Director to Administrations (Responsible Ministry, organization, agency…)
  - Collection of contact details of Focal Point(s) assigned by the Administration
  - Contacting FPs and providing access to the online survey together with all necessary documents and instructions
  - Technical Support
- Data collection phase
  - Filling the questionnaire (FPs provide data, links, supporting documents etc.)
  - Collection of data from open sources for non-respondents (ITU helps Member States to appear in the Report)
- Verification Phase
  - ITU specialists verify all provided data and contact FPs for more details if needed.
  - ITU shares the verified data with FPs
- Analysis Phase
  - Analysis of all collected data (for respondents and non-respondents).
  - Ranking. Preparation of comparison charts, maps, tables and other statistical elements.
  - Illustrative practices extraction.
- Report writing and publication Phase
  - Elaboration of the GCI Report
  - Publication on the ITU website and printing
  - Official launch and informing Member States
  - Follow-up



Score calculation



Dimension score

Technical measures

Sub dimension score

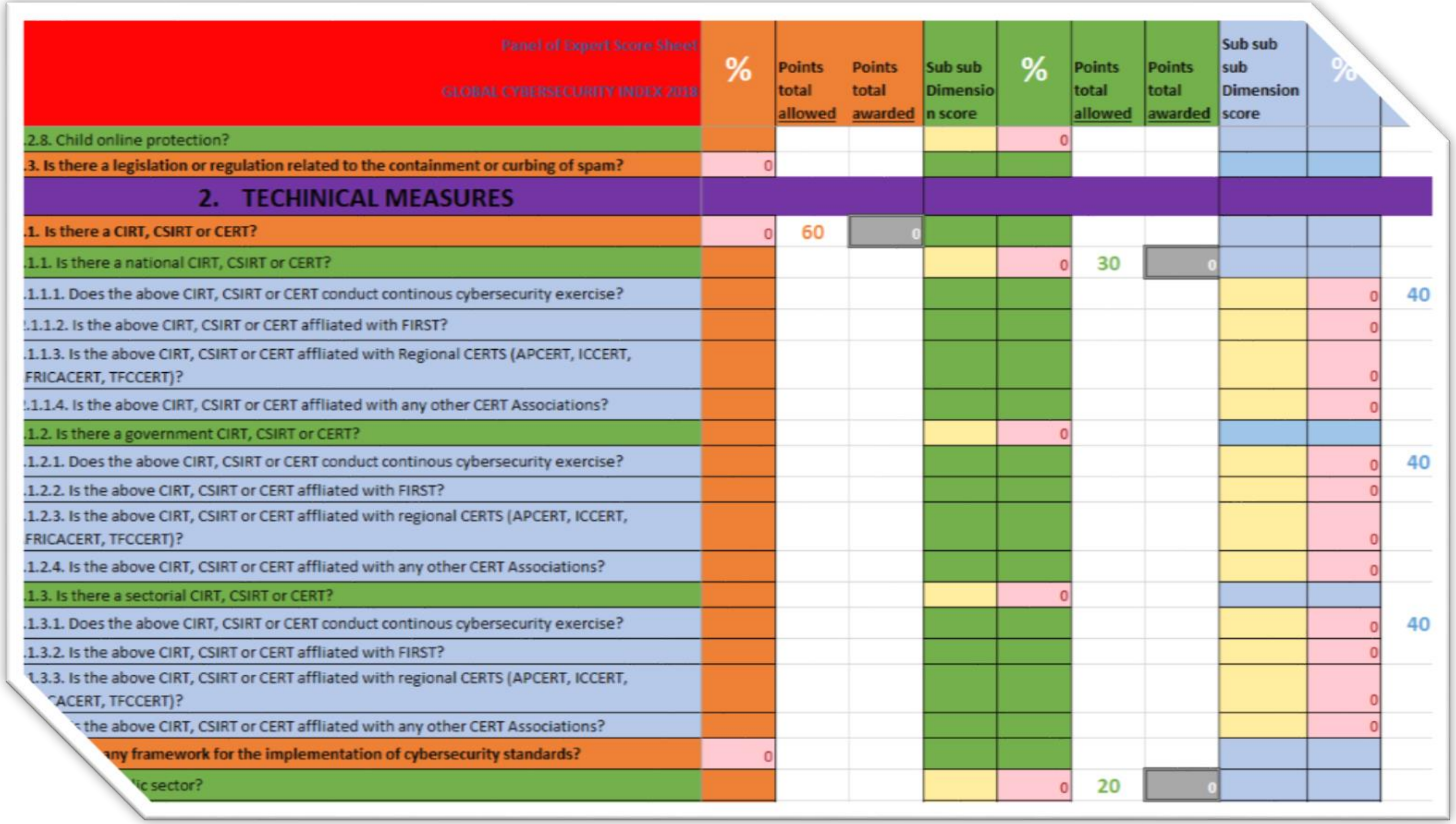
CIRT, CSIRT, CERT

Sub sub dimension score

National CIRT, CSIRT, CERT

Sub sub sub dimension score

Continuous cybersecurity exercise

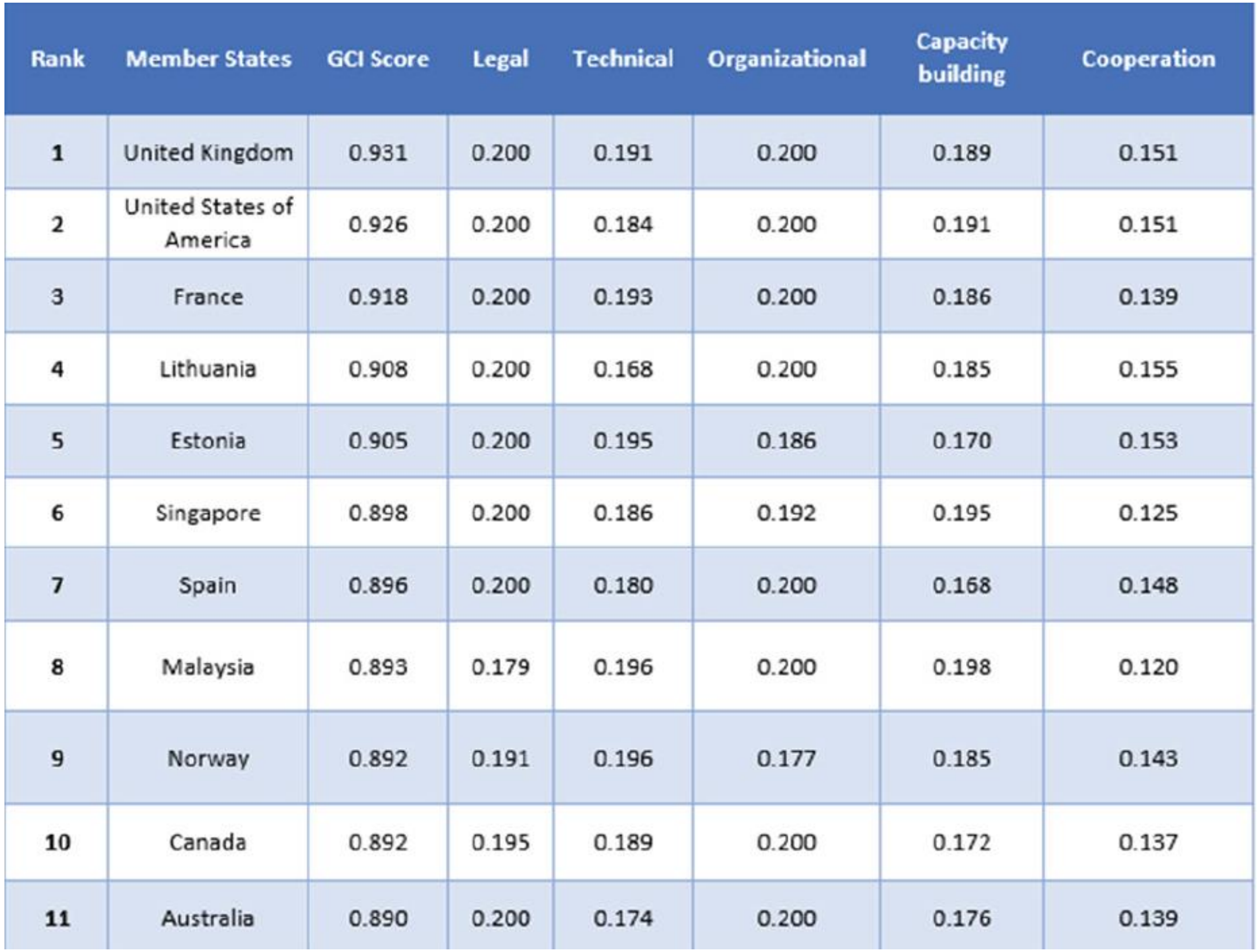


Panel of Expert Score Sheet GLOBAL CYBERSECURITY INDEX 2018	%	Points total allowed	Points total awarded	Sub sub Dimension score	%	Points total allowed	Points total awarded	Sub sub sub Dimension score	%	
.2.8. Child online protection?					0					
.3. Is there a legislation or regulation related to the containment or curbing of spam?	0									
2. TECHINICAL MEASURES										
.1. Is there a CIRT, CSIRT or CERT?	0	60	0							
.1.1. Is there a national CIRT, CSIRT or CERT?					0	30	0			
.1.1.1. Does the above CIRT, CSIRT or CERT conduct continous cybersecurity exercise?									0	40
.1.1.2. Is the above CIRT, CSIRT or CERT affliated with FIRST?									0	
.1.1.3. Is the above CIRT, CSIRT or CERT affliated with Regional CERTS (APCERT, ICCERT, FRICACERT, TFCCERT)?									0	
.1.1.4. Is the above CIRT, CSIRT or CERT affliated with any other CERT Associations?									0	
.1.2. Is there a government CIRT, CSIRT or CERT?					0					
.1.2.1. Does the above CIRT, CSIRT or CERT conduct continous cybersecurity exercise?									0	40
.1.2.2. Is the above CIRT, CSIRT or CERT affliated with FIRST?									0	
.1.2.3. Is the above CIRT, CSIRT or CERT affliated with regional CERTS (APCERT, ICCERT, FRICACERT, TFCCERT)?									0	
.1.2.4. Is the above CIRT, CSIRT or CERT affliated with any other CERT Associations?									0	
.1.3. Is there a sectorial CIRT, CSIRT or CERT?					0					
.1.3.1. Does the above CIRT, CSIRT or CERT conduct continous cybersecurity exercise?									0	40
.1.3.2. Is the above CIRT, CSIRT or CERT affliated with FIRST?									0	
1.3.3. Is the above CIRT, CSIRT or CERT affliated with regional CERTS (APCERT, ICCERT, ACERT, TFCCERT)?									0	
the above CIRT, CSIRT or CERT affliated with any other CERT Associations?									0	
any framework for the implementation of cybersecurity standards?	0									
lic sector?					0	20	0			

GCI most committed countries globally in 2018

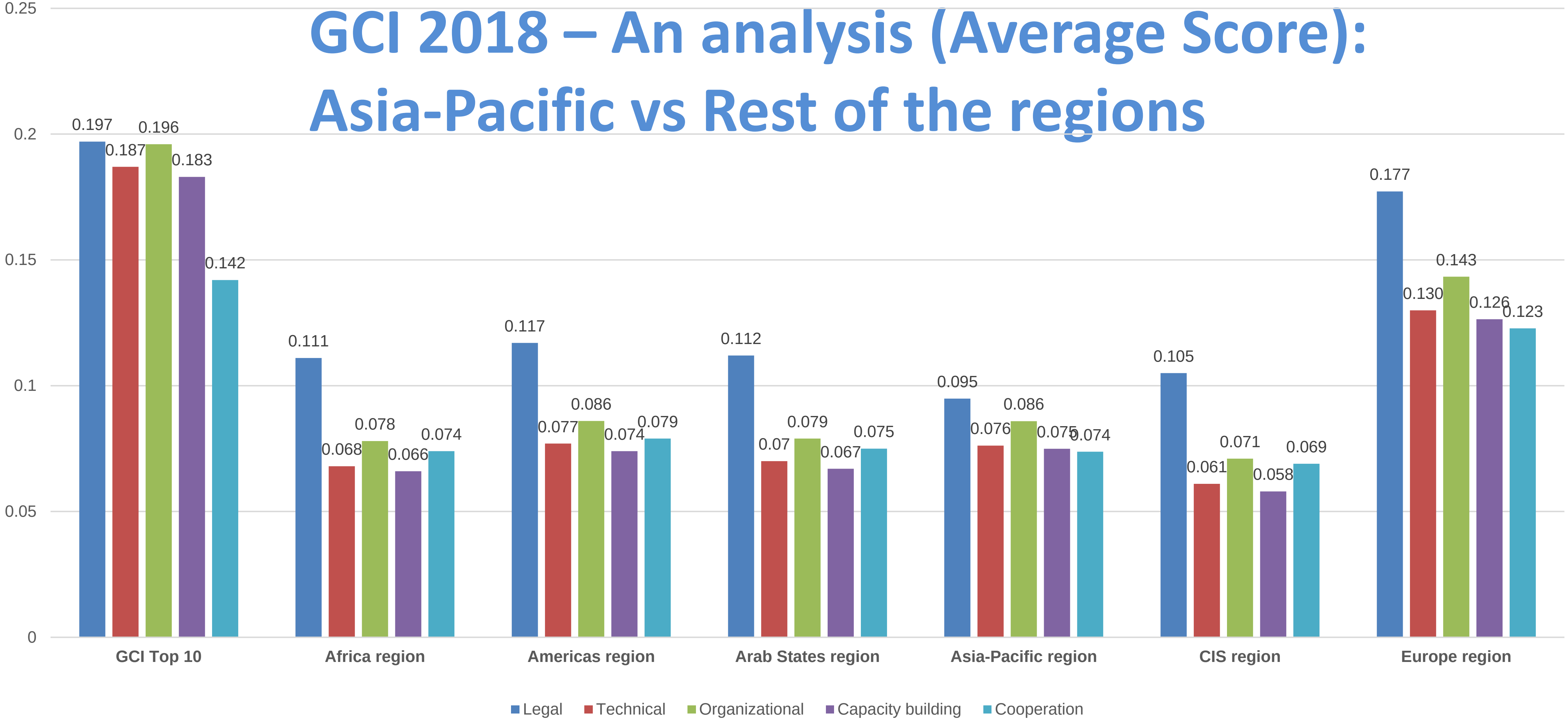
In 2018, only three regions are represented with countries having the most level of commitment: six countries from the Europe region, three from the Asia-Pacific region, and two from the Americas region

Table 4 shows countries that scored well in the legal and organizational pillars reaching a peak score of 20 (0.200). Almost all countries mentioned above show low commitment in the cooperation pillar, with Lithuania scoring only 0.155



Rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
2	United States of America	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
10	Canada	0.892	0.195	0.189	0.200	0.172	0.137
11	Australia	0.890	0.200	0.174	0.200	0.176	0.139

GCI 2018 – An analysis (Average Score): Asia-Pacific vs Rest of the regions



Cyberdrills

Regional Cyberdrills -Objectives

1 Enhancing cybersecurity capacity and capabilities through regional collaborations and cooperation;

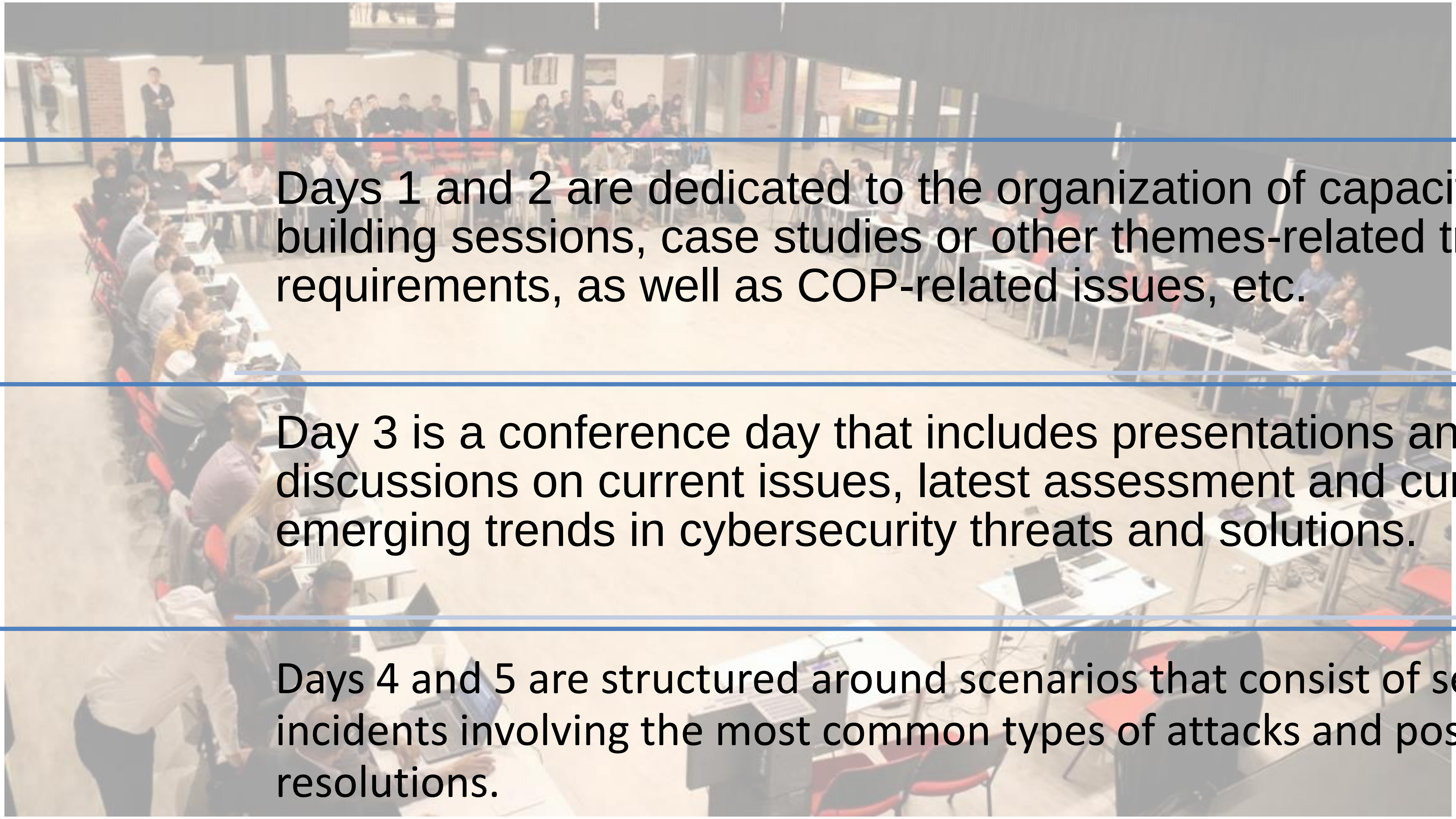
2 Enhancing the awareness and the capability of countries to participate and to contribute to the development and deployment of a strategy of defeating a cyber threat;

3 Strengthening international cooperation between Member States to ensure continued collective efforts against cyber threats;

4 Enhancing Member States' and incident response capabilities and communication;

5 Assisting Member States to develop and implement operational procedures to respond better to various cyber incidents, identify improvements for future planning CIRT processes and operational procedures

Regional Cyberdrills - Programme



1

Days 1 and 2 are dedicated to the organization of capacity building sessions, case studies or other themes-related training requirements, as well as COP-related issues, etc.

2

Day 3 is a conference day that includes presentations and panel discussions on current issues, latest assessment and current and emerging trends in cybersecurity threats and solutions.

3

Days 4 and 5 are structured around scenarios that consist of several incidents involving the most common types of attacks and possible resolutions.

ITU Asia-Pacific and CIS Inter-Regional Cyberdrill

Date : 23-27 September 2019, Kuala Lumpur, Malaysia

Hosted by

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

The Ministry of Communications and Multimedia Malaysia

The National Cyber Security Agency Malaysia

Child Online Protection (COP)

Online Threats to Children

Threats & Risks

Cybergrooming

Child abuse materials

Pornography

Sexual solicitation

Disclosure private information

Child pornography

Racism

Online Fraud

Cyber Bullying

Anorexia, self-harm or suicide

Online Gaming & Addiction

Violence

Cyberstalking

Phishing attacks

Spam

Youth-to-youth cybercrimes

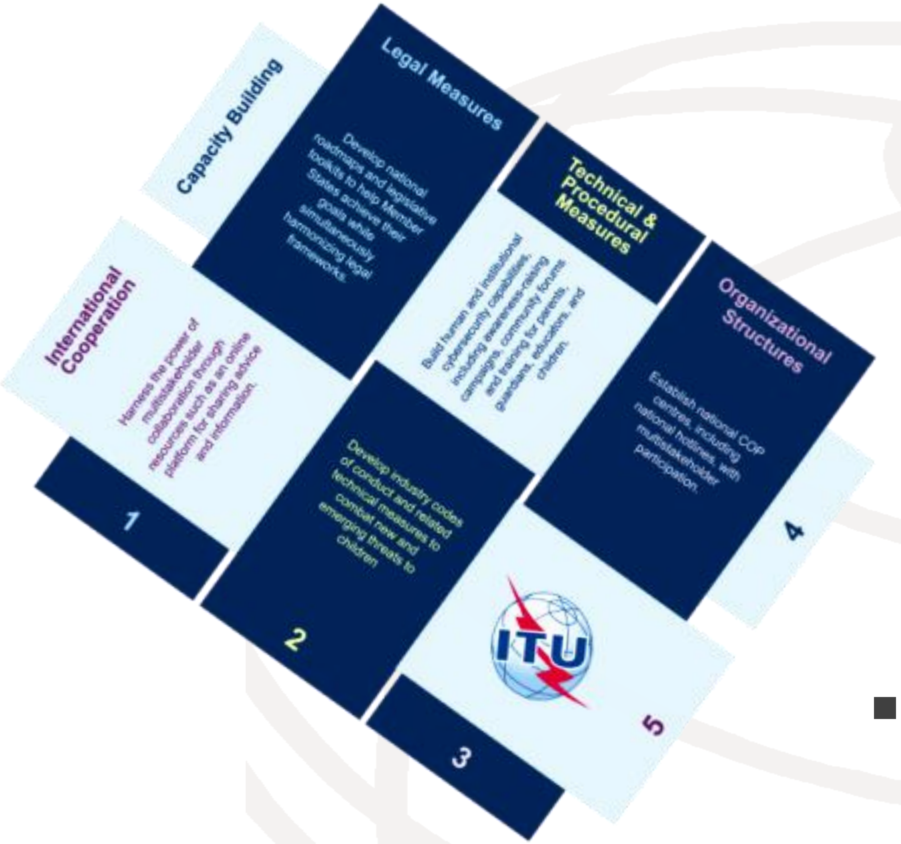
Child Online Protection (COP) Initiative

The COP Initiative aims at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere.

Objectives

- Identify risks and vulnerabilities to children in cyberspace;
- Create awareness of the risks and issues through multiple channels;
- Develop practical tools to help governments, organizations and educators minimize risk; and
- Share knowledge and experience while facilitating international strategic partnership to define and implement concrete initiatives

COP Five Strategic Pillars



Capacity Building

Legal Measures

Develop national roadmaps and legislative toolkits to help Member States achieve their goals while simultaneously harmonizing legal frameworks.

Technical & Procedural Measures

Build human and institutional cybersecurity capabilities, including awareness-raising campaigns, community forums and training for parents, guardians, educators, and children.

International Cooperation

Harness the power of multistakeholder collaboration through resources such as an online platform for sharing advice and information.

Develop industry codes of conduct and related technical measures to combat new and emerging threats to children

Organizational Structures

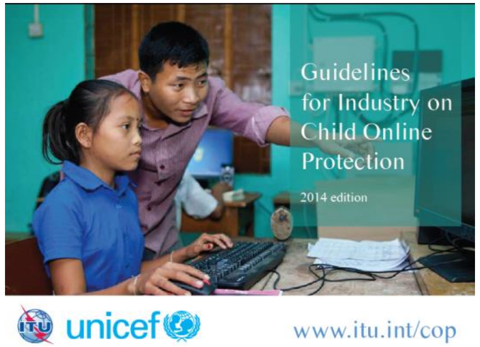
Establish national COP centres, including national hotlines, with multistakeholder participation.

- COP high-level deliverables across the five strategic pillars are designed to be achieved by ITU and COP members in collaboration.
  - Legal Measures
  - Technical & Procedural Measures
  - Organizational Structures
  - Capacity Building
  - International Cooperation
- It is designed to transform the COP Guidelines into concrete activities by leveraging the active support provided by COP partners.

4 Set of COP Guidelines

مبادئ توجيهية
للأطفال بشأن حماية
الأطفال على الخط

www.itu.int/cop


Guidelines for Industry on Child Online Protection

2014 edition

unicef

www.itu.int/cop

父母、监护人和教育者保护在线儿童指南

www.itu.int/cop

Directrices sobre Protección de la Infancia en Línea para los encargados de formular políticas

www.itu.int/cop

Руководящие указания для детей по защите ребенка в онлайновой среде

www.itu.int/cop

Guidelines for Industry on Child Online Protection

www.itu.int/cop

- Developed in cooperation with COP partners, is the first set of guidelines addressing different stakeholders. Available in the six UN languages

The COP Guidelines in details

Guidelines for Children on Child Online Protection

www.itu.int/cop

Update version

COP Guidelines for Children

Children and young people need to be aware of risks online. The guidelines advise them on possible harmful activities online, such as bullying and harassment, identity theft, and online abuse. The guidelines also include advice to children seeing and experiencing harmful and illegal content online, or young people being exposed to grooming for sexual purposes, the production, distribution and collection of child abuse material.

The COP Guidelines in details

Guidelines for Parents, Guardians and Educators on Child Online Protection

www.itu.int/cop

Update version

COP Guidelines for Parents, Guardians and Educators

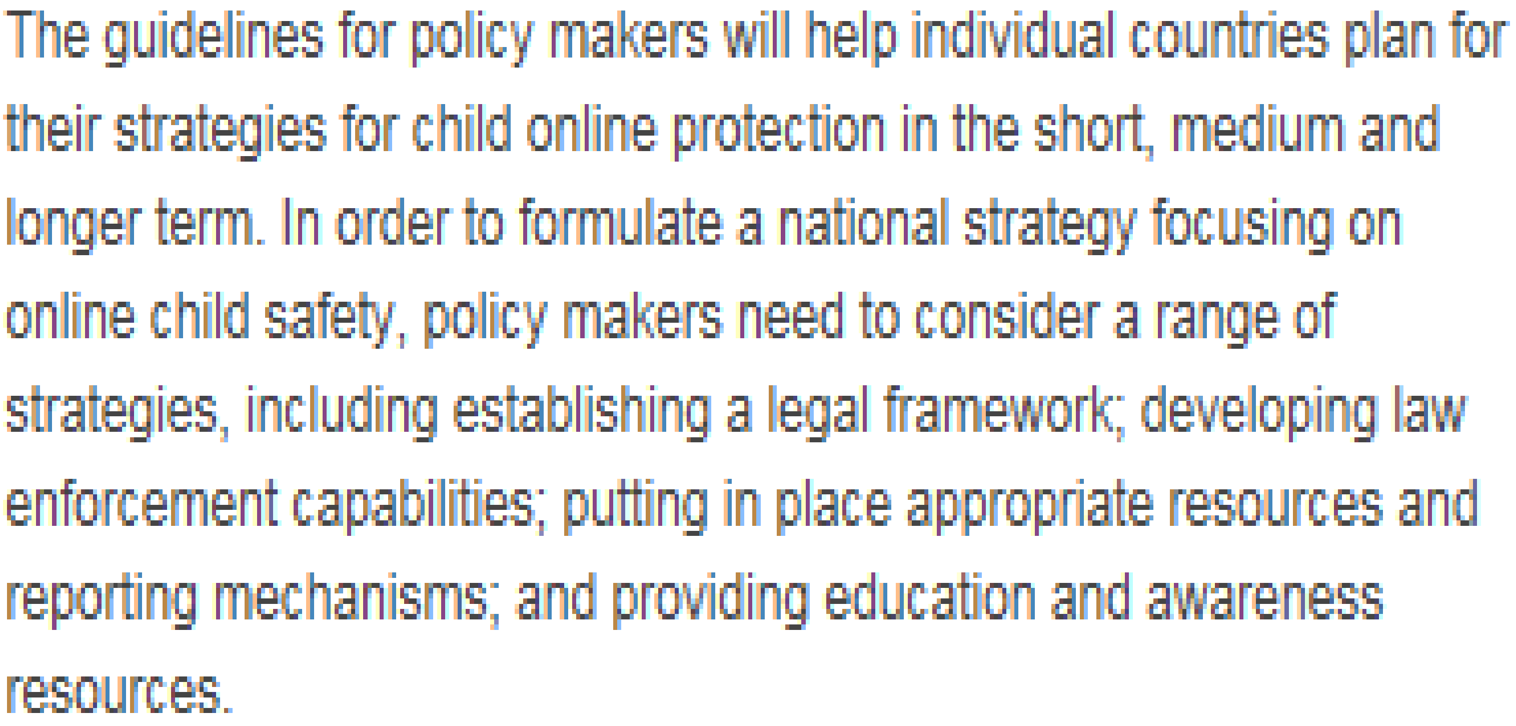
Research shows that more and more children are connecting to the Internet using game consoles and mobile devices, yet many adults are not even aware that these activities include internet connectivity. The guidelines for parents, guardians and educators provide recommendations on what they can do to make their child's online experience a positive one.

The COP Guidelines in details

COP Guidelines for Policy Makers

Guidelines for Policy Makers on Child Online Protection

www.itu.int/cop



The guidelines for policy makers will help individual countries plan for their strategies for child online protection in the short, medium and longer term. In order to formulate a national strategy focusing on online child safety, policy makers need to consider a range of strategies, including establishing a legal framework; developing law enforcement capabilities; putting in place appropriate resources and reporting mechanisms; and providing education and awareness resources.

The COP Guidelines in details

New COP Guidelines for Industry

The updated guidelines for Industry on Child Online Protection provide advice on how the ICT industry can help promote safety for children using the Internet or any technologies or devices that can connect to it. **An online platform of COP case studies from the broader ICT Industry further complements the content of these Guidelines.**

5 key areas for protecting and promoting children's rights in the online environment

Policies and management processes	Child sexual abuse content	Safer and age appropriate environment	Educate children, parents and teachers	Promote positive use of ICTS
Integrate children's rights in policies and management processes	Develop processes for handling child sexual abuse content	Develop safer and age appropriate online environments	Educate children, parents and teachers on children's safety	Promote digital technology as a mode to further good citizenship

Purpose of the Guidelines is to provide:

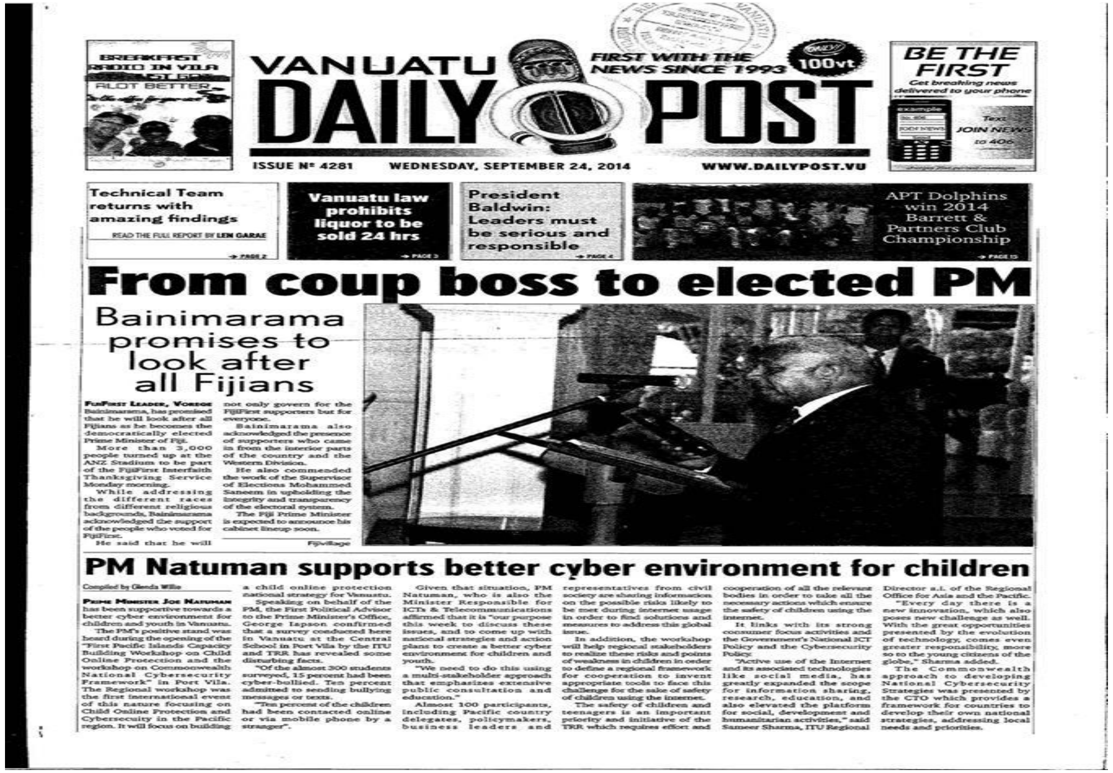
- ✓ A blueprint that can be adapted locally for various industry players
- ✓ Establish a benchmark for recommended actions
- ✓ Guidance on identifying, prevent and mitigating risks
- ✓ Guidance on supporting children's rights

Initiative of Australia on Cyberbullying https://www.youtube.com/watch?v=TtEGAcLBTTA

ITU Work on Child Online Protection in Asia-Pacific

- ITU Regional Workshop , Vanuatu
- Partners : CTO, Regulator, OGCIO
- Outcome: COP Guidelines for Vanuatu

- COP Guidelines for Brunei : 2014
- COP Awareness in Nepal (2015)
- COP ongoing work in Philippines , Bhutan, Kiribati (2018)



VANUATU DAILY POST
FIRST WITH THE NEWS SINCE 1993
100vt
ISSUE Nº 4281 WEDNESDAY, SEPTEMBER 24, 2014 WWW.DAILYPOST.VU

Technical Team returns with amazing findings
READ THE FULL REPORT BY LEN GARAE
→ PAGE 2

Vanuatu law prohibits liquor to be sold 24 hrs
→ PAGE 3

President Baldwin: Leaders must be serious and responsible
→ PAGE 4

APT Dolphins win 2014 Barrett & Partners Club Championship
→ PAGE 15

From coup boss to elected PM

Bainimarama promises to look after all Fijians

FijiFirst Leader, Voreqe Bainimarama, has promised that he will look after all Fijians as he becomes the democratically elected Prime Minister of Fiji.

More than 3,000 people turned up at the ANZ Stadium to be part of the FijiFirst Interfaith Thanksgiving Service Monday morning.

While addressing the different races from different religious backgrounds, Bainimarama acknowledged the support of the people who voted for FijiFirst.

He said that he will not only govern for the FijiFirst supporters but for everyone.

Bainimarama also acknowledged the presence of supporters who came in from the interior parts of the country and the Western Division.

He also commended the work of the Supervisor of Elections Mohammed Saneem in upholding the integrity and transparency of the electoral system.

The Fiji Prime Minister is expected to announce his cabinet lineup soon.

Fijivillage

PM Natuman supports better cyber environment for children

Compiled by Glenda Willie

Prime Minister Joe Natuman has been supportive towards a better cyber environment for children and youth in Vanuatu.

The PM's positive stand was heard during the opening of the "First Pacific Islands Capacity Building Workshop on Child Online Protection and the workshop on Commonwealth National Cybersecurity Framework" in Port Vila. The Regional workshop was the first international event of this nature focusing on Child Online Protection and Cybersecuity in the Pacific region. It will focus on building a child online protection national strategy for Vanuatu.

Speaking on behalf of the PM, the First Political Advisor to the Prime Minister's Office, George Iapson confirmed that a survey conducted here in Vanuatu at the Central School in Port Vila by the ITU and TRR has revealed some disturbing facts.

"Of the almost 300 students surveyed, 15 percent had been cyber-bullied. Ten percent admitted to sending bullying messages or texts.

"Ten percent of the children had been contacted online or via mobile phone by a stranger".

Given that situation, PM Natuman, who is also the Minister Responsible for ICTs & Telecommunications affirmed that it is "our purpose this week to discuss these issues, and to come up with national strategies and action plans to create a better cyber environment for children and youth.

"We need to do this using a multi-stakeholder approach that emphasizes extensive public consultation and education."

Almost 100 participants, including Pacific country delegates, policymakers, business leaders and representatives from civil society are sharing information on the possible risks likely to be met during internet usage in order to find solutions and measures to address this global issue.

In addition, the workshop will help regional stakeholders to realize these risks and points of weakness in children in order to define a regional framework for cooperation to invent appropriate tools to face this challenge for the sake of safety of children using the internet.

The safety of children and teenagers is an important priority and initiative of the TRR which requires effort and cooperation of all the relevant bodies in order to take all the necessary actions which ensure the safety of children using the internet.

It links with its strong consumer focus activities and the Government's National ICT Policy and the Cybersecurity Policy.

"Active use of the Internet and its associated technologies like social media, has greatly expanded the scope for information sharing, research, education, and also elevated the platform for social, development and humanitarian activities," said Sameer Sharma, ITU Regional Director a.i. of the Regional Office for Asia and the Pacific.

"Every day there is a new innovation, which also poses new challenge as well. With the great opportunities presented by the evolution of technology, comes even greater responsibility, more so to the young citizens of the globe," Sharma added.

The Commonwealth approach to developing National Cybersecurity Strategies was presented by the CTO which provides a framework for countries to develop their own national strategies, addressing local needs and priorities.

COP Activities with ASEAN (2016-18)

ASEAN Strategy Framework on Child Online Protection

- Survey and its findings presented at the ITU-ASEAN Forum on COP (Sep 2016; Manila, Philippines)

- ITU-ASEAN Forum/workshops on Child Online Protection
  - ✓ Manila, Philippines, Sept. 2016
  - ✓ Jakarta, Indonesia, March 2018
  - ✓ Nay Pyi Taw, Myanmar, December 2018

- Framework finalized and will be shared with ASEAN
- ITU Paper for ASEAN on “Improving child online protection measures in ASEAN: Partnering with industry”

Child Sexual Abuse Domestic Legislation Summary

Country	Expressly criminalizes ‘child pornography’	Clear definition of ‘child pornography’	Criminalizes simple possession	Reporting obligation for ISPs	Criminalizes sexual grooming
Brunei Darussalam	✓	✓	✓	✗	✓
Cambodia	✓	✓	✗	✗	✗
Indonesia	✓	✗	✓	✗	✗
Lao PDR	✓	✗	✗	✗	✗
Malaysia	✓	✓	✓	✗	✓
Myanmar	✓	✗	✗	✗	✗
Philippines	✓	✓	✓	✓	✓
Singapore	✓	✗	✓	✗	✓
Thailand	✓	✓	✓	✗	✗
Vietnam	✓	✗	✗	✗	✗

3D Multiuser Virtual Learning Environment to increase awareness about online risks for children

- The prototype will have different scenarios where a child is confronted with a cyber abuse situation by a predator approaching the child via social media

- The game shows an island with different kinds of games for children. Once they are engaged, they will be confronted by a social media screen insert, offering interesting challenges by a K-Pop star lookalike.

- The child will be represented by a child avatar

- https://www.youtube.com/watch?v=SymYlZq5v1k&feature=youtu.be.

Conclusions

- While it will never be possible to completely remove all risks, drawing together an effective policies and practices, infrastructure & technology, awareness and communication can do a great deal to help.
- Cybersecurity and Critical National Information Infrastructure requiring political will and commitment to have clear National Cybersecurity Strategy , Cyber Crime Legislation , Child Online Protection, establishment / strengthening the CIRTs/ regular national / regional Cyber Drills
- Human and institutional capacity building critical to understand and take reactive / proactive response to address cyberthreats
- International cooperation, based on a multi-stakeholder approach, is the key and by working together with ITU and its partners, together we can realize Safe and Secure Cyber-space!

ITU : I Thank U