AI , ML and Cybersecurity

New Delhi, India
11 October 2019

Sameer Sharma
Regional Director a.i.
ITU Regional Office for Asia-Pacific

THE SUMMIT

The Summit is **THE** leading UN platform for global and inclusive dialogue on AI

Hosted by the ITU in partnership with sister UN agencies, XPRIZE Foundation & ACM

THE GOAL

Connect **AI innovators** with **problem owners**, to identify **practical applications of AI** to **accelerate progress** towards the **UN Sustainable Development Goals**

Ensure **trusted, safe** and **inclusive** development of AI technologies and **equitable access** to their benefits

2019 SUMMIT IN NUMBERS

2300+ Participants registered

40% Women Participants

90+ Countries

37 UN Partners

375+ Speakers

50+ Exhibitors

15 Stages

275+ Developing Countries

80+ Sessions

2019 BREAKTHROUGH TEAMS

The heart of the Summit…

SDG4 Education

SDG3 Good Health and Well Being

SDG10 Human dignity

SDG7 Scaling AI for Good

AI for Space

ITU / WHO Focus Group on Artificial Intelligence for Health

AI for Health

An ITU Focus Group
In collaboration with WHO

ITU / WHO Focus Group on Artificial Intelligence for Health

Topic areas: Cardiovascular disease risk prediction (TG-Cardio)

- Dermatology (TG-Derma)
- Falls among the elderly (TG-Falls)
- Histopathology (TG-Histo)
- Neuro-cognitive diseases (TG-Cogni)
- Outbreak detection (TG-Outbreaks) New
- Ophthalmology (TG-Ophthalmo)
- Psychiatry (TG-Psy)
- Radiotherapy (TG-Radiotherapy)
- Snakebite and snake identification (TG-Snake)
- Symptom assessment (TG-Symptom)
- Tuberculosis (TG-TB)
- Volumetric chest computed tomography (TG-DiagnosticCT)

Key current **output documents**:

- FG-AI4H Whitepaper
- E-102: Updated call for proposals: use cases, benchmarking, and data
- D-103: Updated FG-AI4H data acceptance and handling policy
- C-104: Thematic classification scheme

ITU/WHO Focus Group AI for Health

Artificial Intelligence for Health (A4IH) offers substantial improvements for public and clinical health, e.g. early detection, diagnosis and risk identification, treatment decision support, self-management, improved outcomes, …

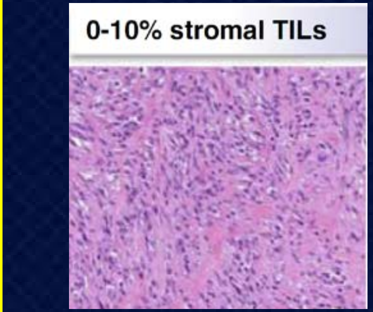
For world-wide adoption, need evaluation standards on effective AI for Health

Focus Group AI for Health (FG-AI4H) created July 2018; open platform

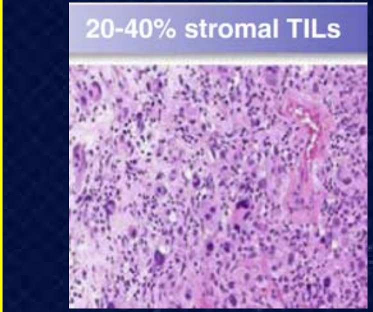
FG-AI4H goals: standardized framework for benchmarking and evaluation of AI solutions

AI for Health Use Case in Histopathology: Diagnostic Support for Breast Cancer Treatment

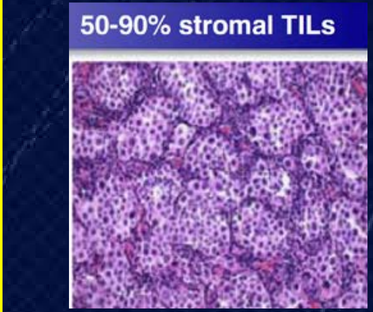
- Tumor infiltrating lymphocytes (TILs) are implicated in eliminating tumor cells
- Quantification of TILs relevant for patient prognosis estimation and therapy selection
- Replace “eye-balling” by pathologist with Machine Learning method for TIL quantification
- Focus Group: specify process on data generation and evaluate accuracy of Machine Learning method



0-10% stromal TILs



20-40% stromal TILs



50-90% stromal TILs

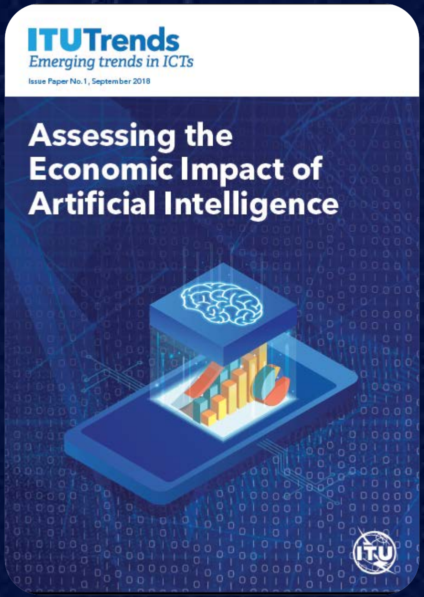
Source: Hendry, S., Salgado, R., Gevaert, T., Russell, P. A., John, T., Thapa, B., ... & Sanders, M. (2017). Assessing Tumor-Infiltrating Lymphocytes in Solid Tumors: A Practical Review for Pathologists and Proposal for a Standardized Method from the International Immuno-Oncology Biomarkers Working Group Part 2 (...). Advances in anatomic pathology, 24(6), 311-335.

ITU-T Focus Group on Machine Learning for 5G

Unified architecture for machine learning in 5G and future networks processed and approved by SG13 on 1 of July “Architectural framework for machine learning in future networks including IMT-2020"

ITU's ML-Aware Network Architecture: Bringing Intelligence to Verticals
March 2019
Upcoming: Machine learning in 5G and future networks: use cases and basic requirements
Upcoming: Framework for data handling to enable Machine Learning in future networks including IMT 2020
Upcoming: Method for evaluating mobile network intelligence level

Source: https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx



ITUTrends
Emerging trends in ICTs
Issue Paper No.1, September 2018

Assessing the Economic Impact of Artificial Intelligence

Assessing the economic impact of Artificial Intelligence

Contributed by the McKinsey Global Institute (MGI), the economic and business research arm of McKinsey & Company, this paper offers a framework for thinking about how to model the economic impact of AI

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.

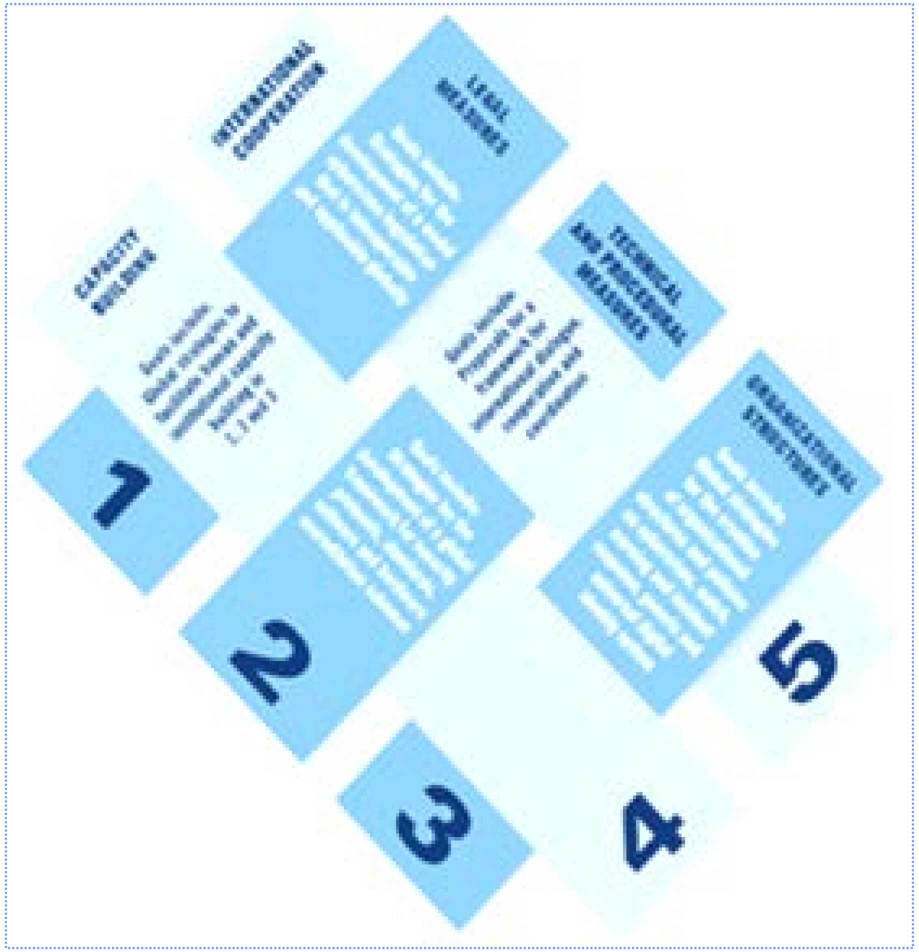
GCA GLOBAL CYBERSECURITY AGENDA

Child Online Protection

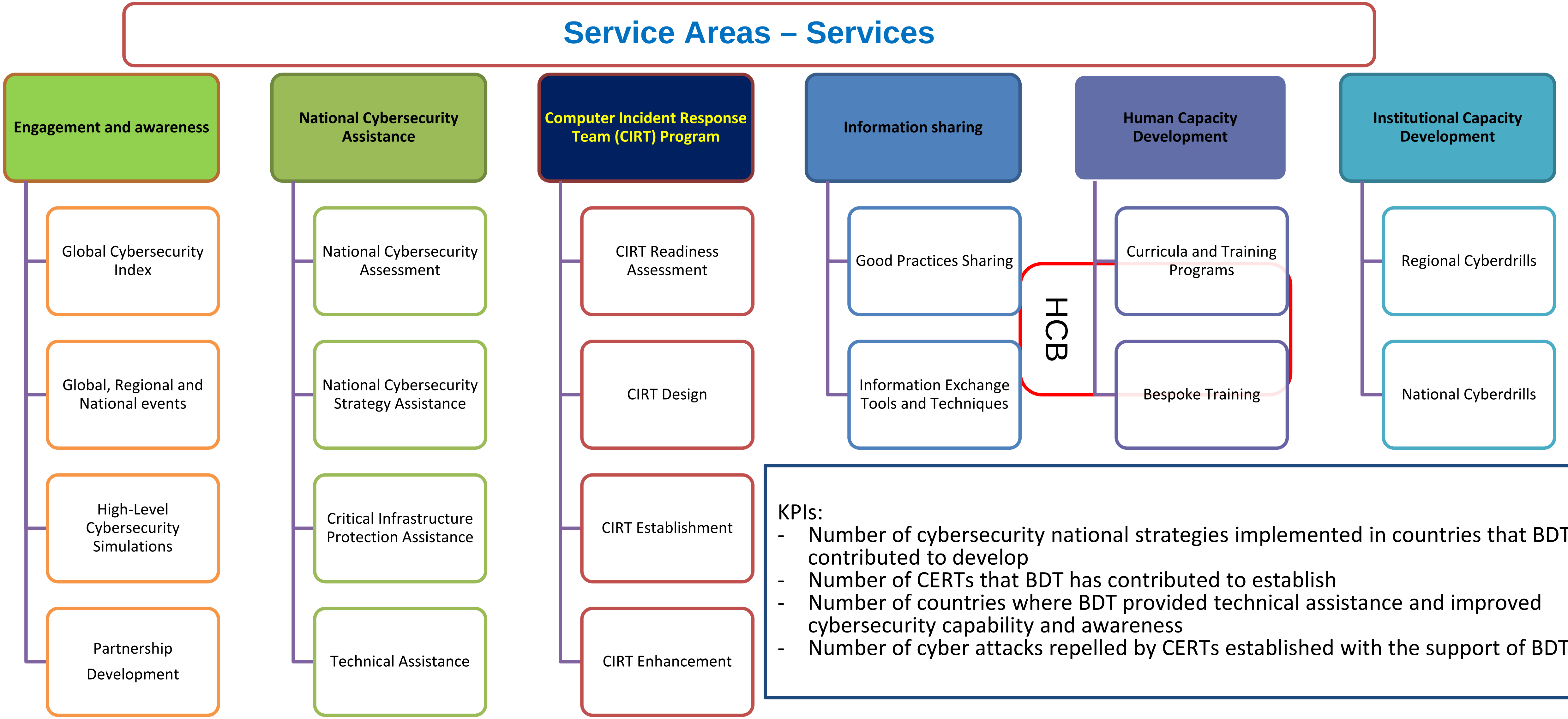
Building confidence and security in the use of ICTs is widely present in **PP and Conferences**’ resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues,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

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

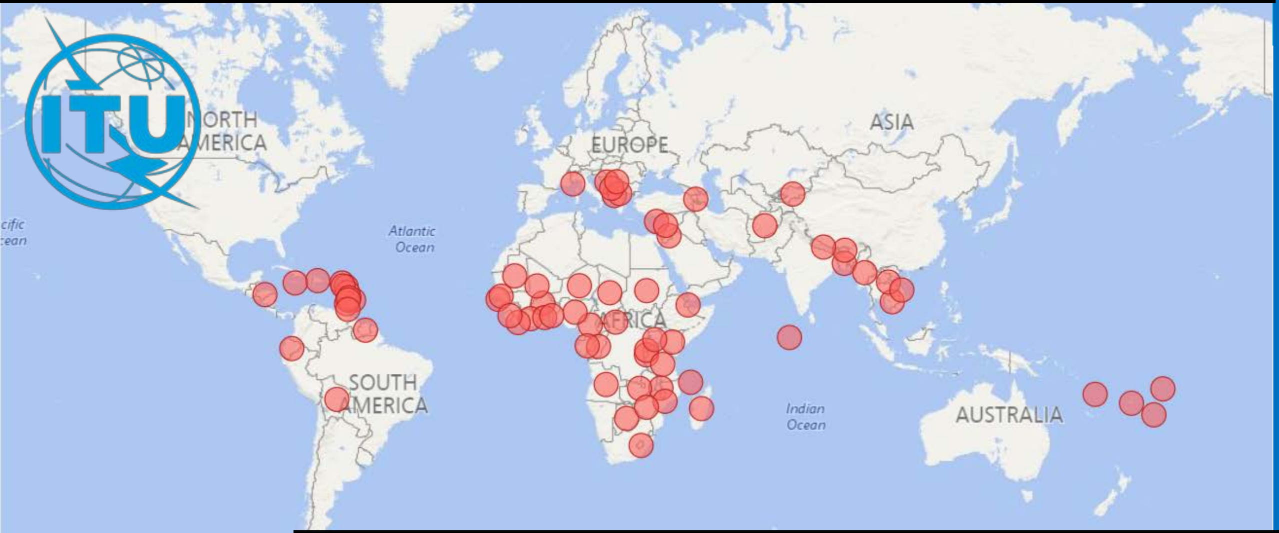
HCB

Human Capacity Development
- Curricula and Training Programs
- Bespoke Training

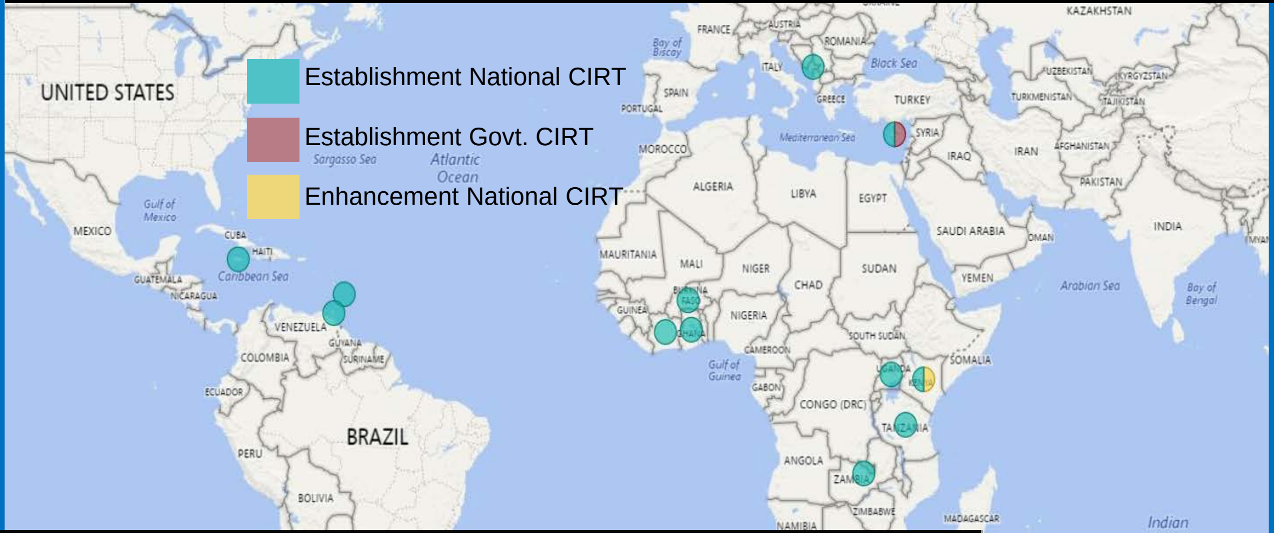
Institutional Capacity Development
- Regional Cyberdrills
- National Cyberdrills

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

75 CIRT READINESS ASSESSMENTS

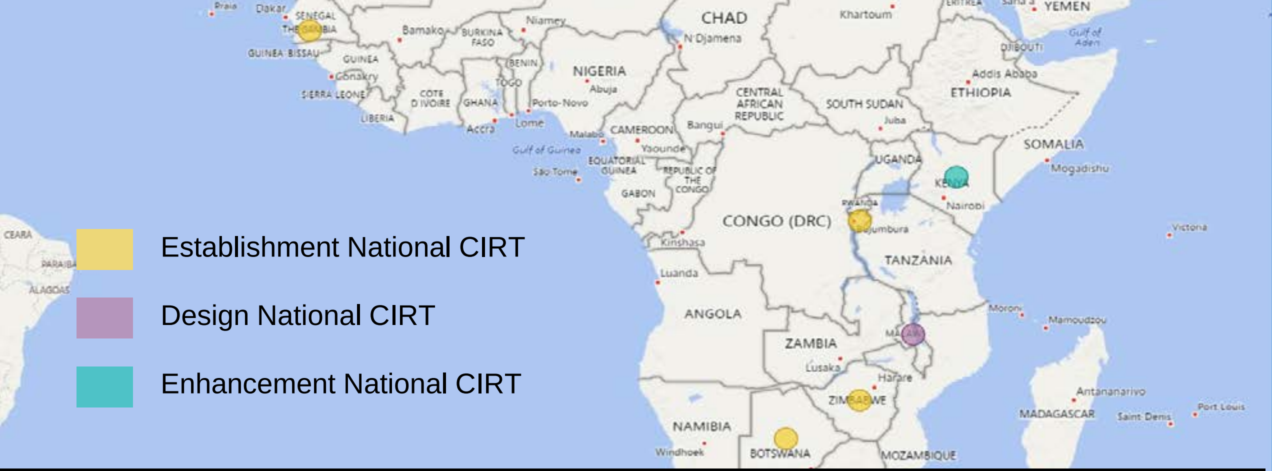


13 CIRT ESTABLISHMENT + 1 ENHANCEMENT

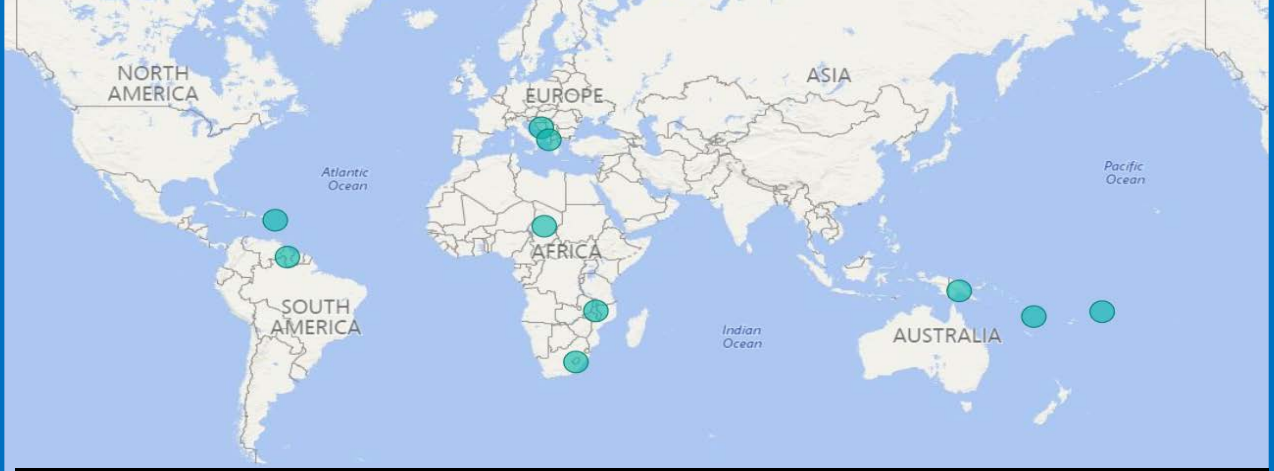


SCALE-UP & DELIVER MORE

CIRT PROGRAMME EXAMPLE

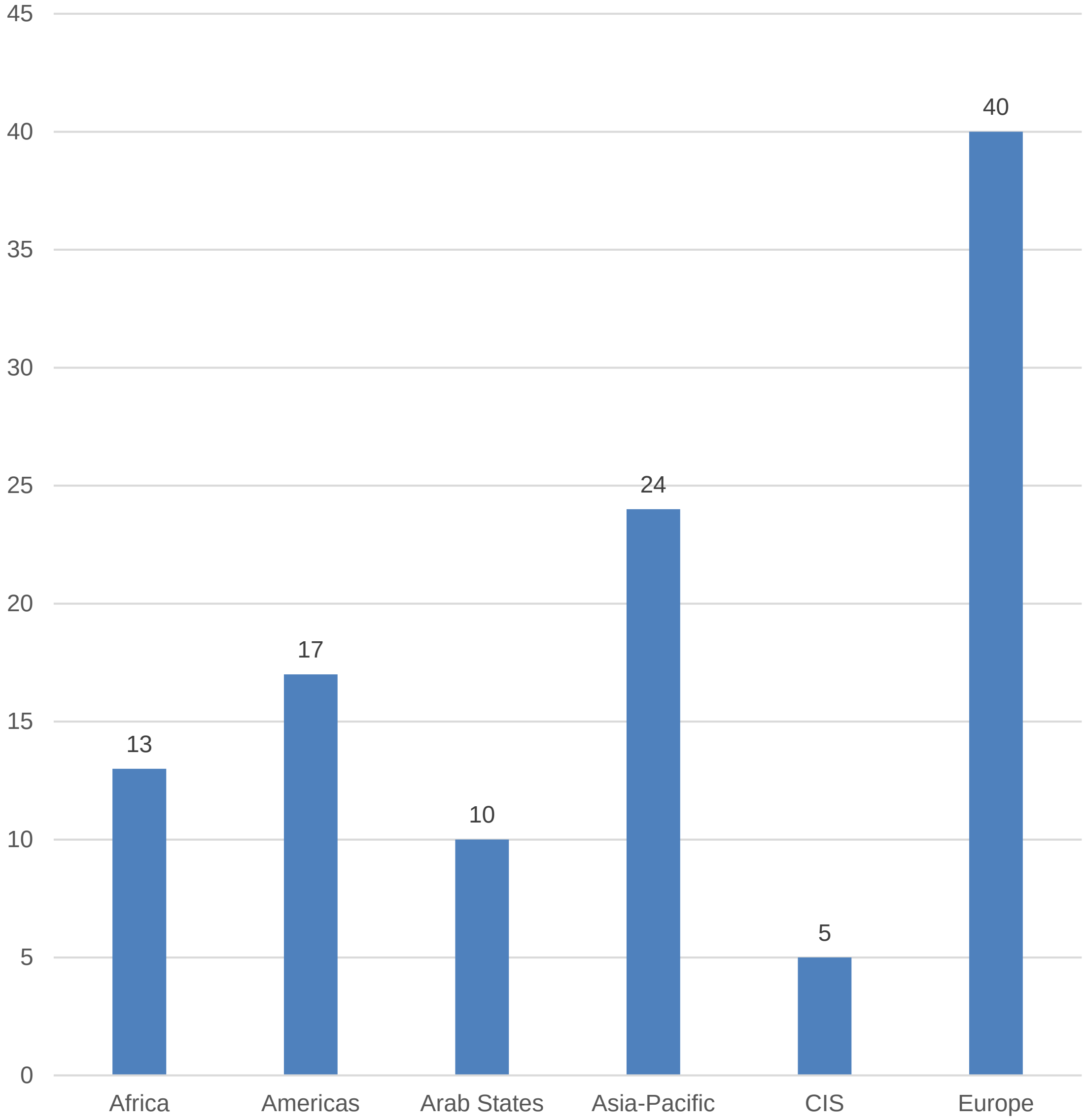


CIRT ESTBLISHMENT IN 2019



CIRT ESTABLISHMENT– INTERESTS

Number of CIRT activities around the world



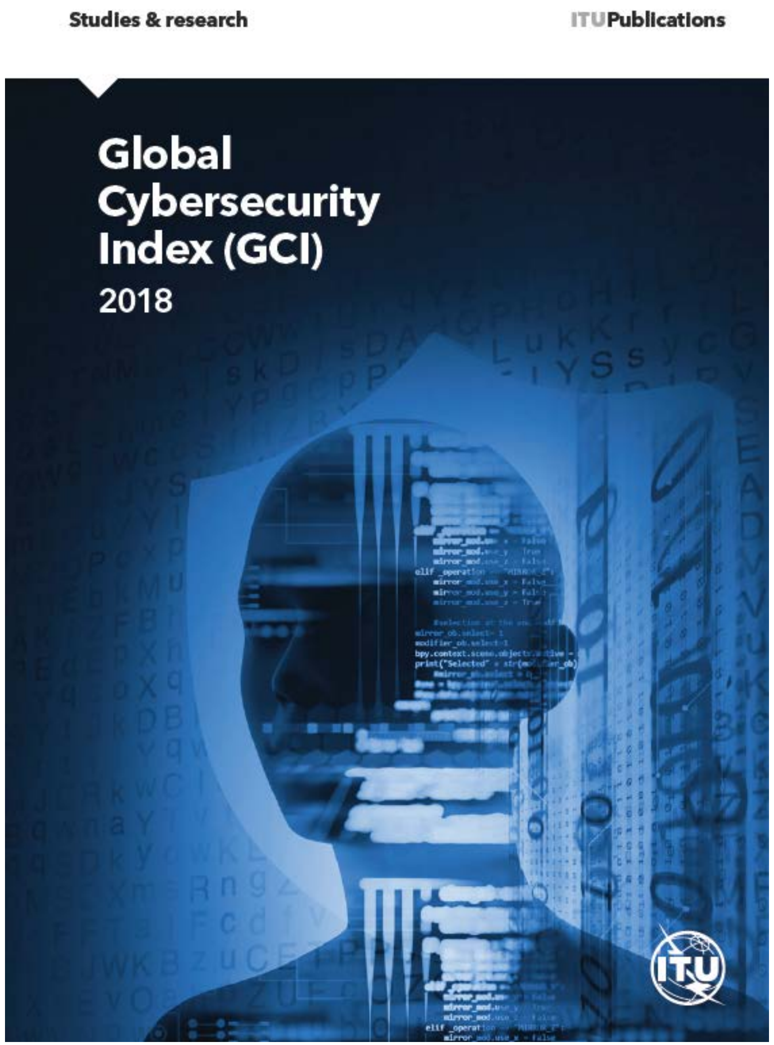
CIRTs in Asia-Pacific:

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

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”



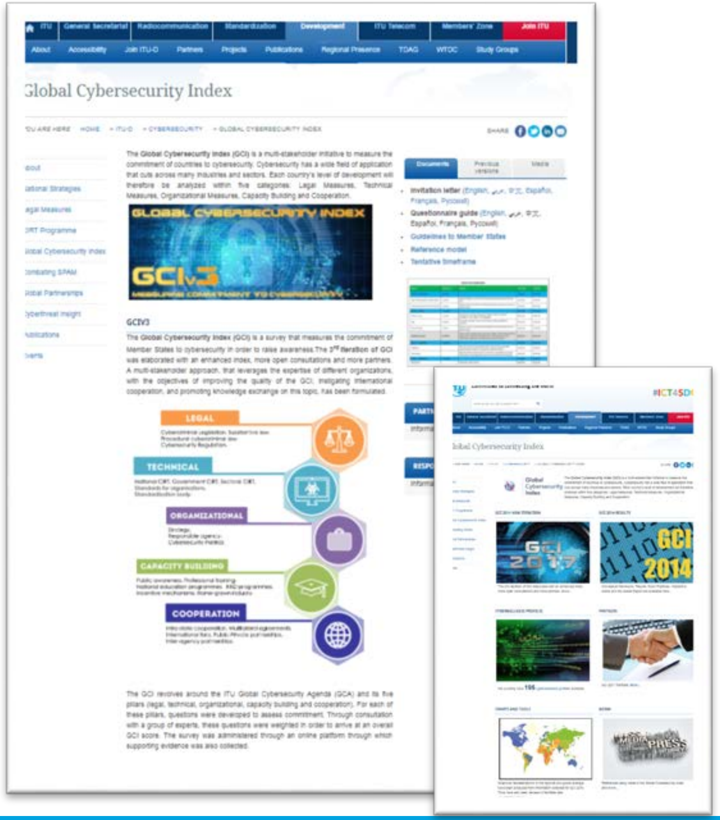
Studies & research

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>**



Global Cybersecurity Index

YOU ARE HERE HOME > ITU-D > CYBERSECURITY > GLOBAL CYBERSECURITY INDEX

About
National Strategies
Legal Measures
CIRT Programme
Global Cybersecurity Index
Combating SPAM
Global Partnerships
Cyberthreat insight
Publications
Events

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.

LEGAL
Cybercriminal Legislation, Substantive law, Procedural cybercriminal law, Cybersecurity Regulation.

TECHNICAL
National CIRT, Government CIRT, Sectoral CIRT, Standards for organizations, 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.

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.

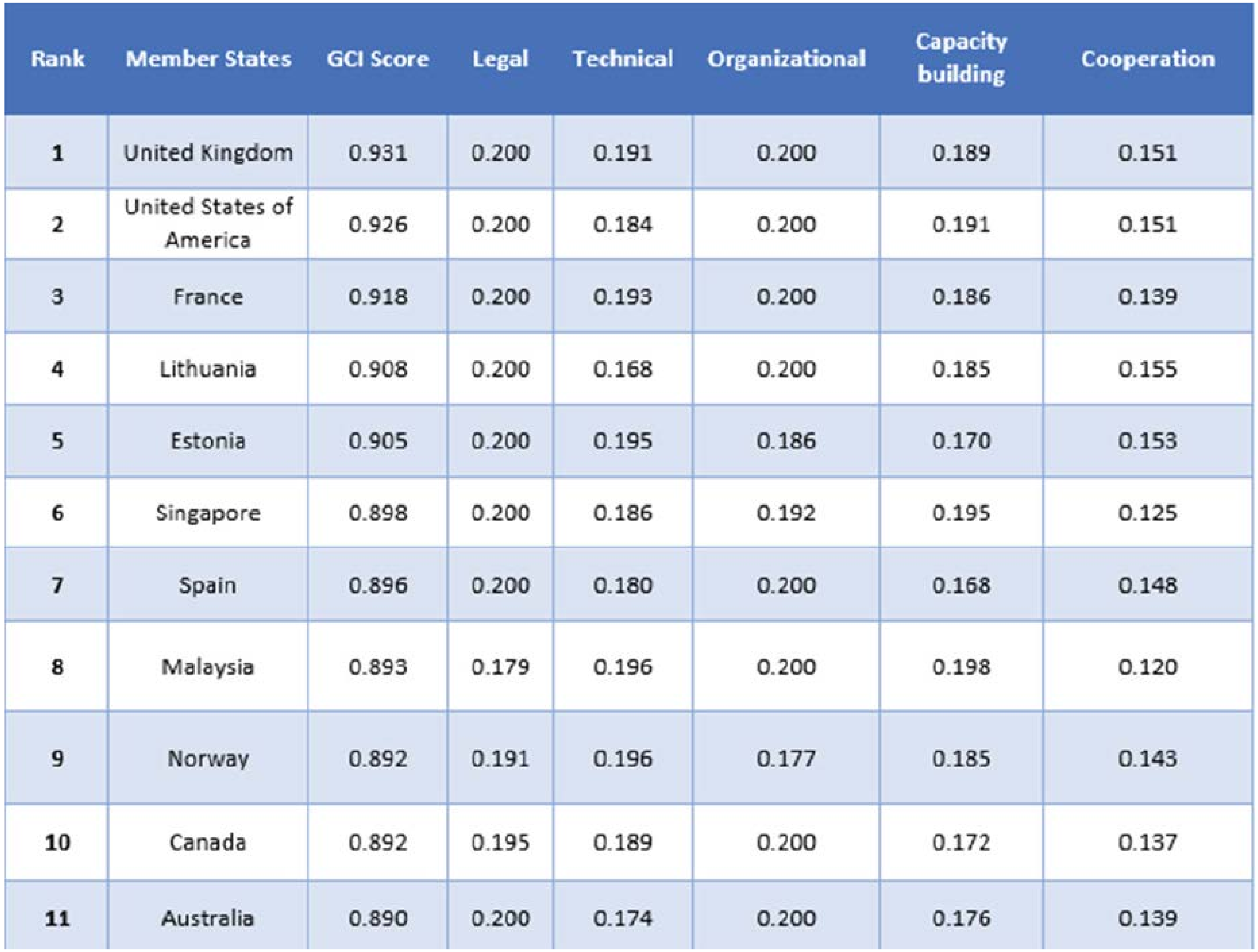
Global Cybersecurity Index

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

GCI most committed countries globally in 2018

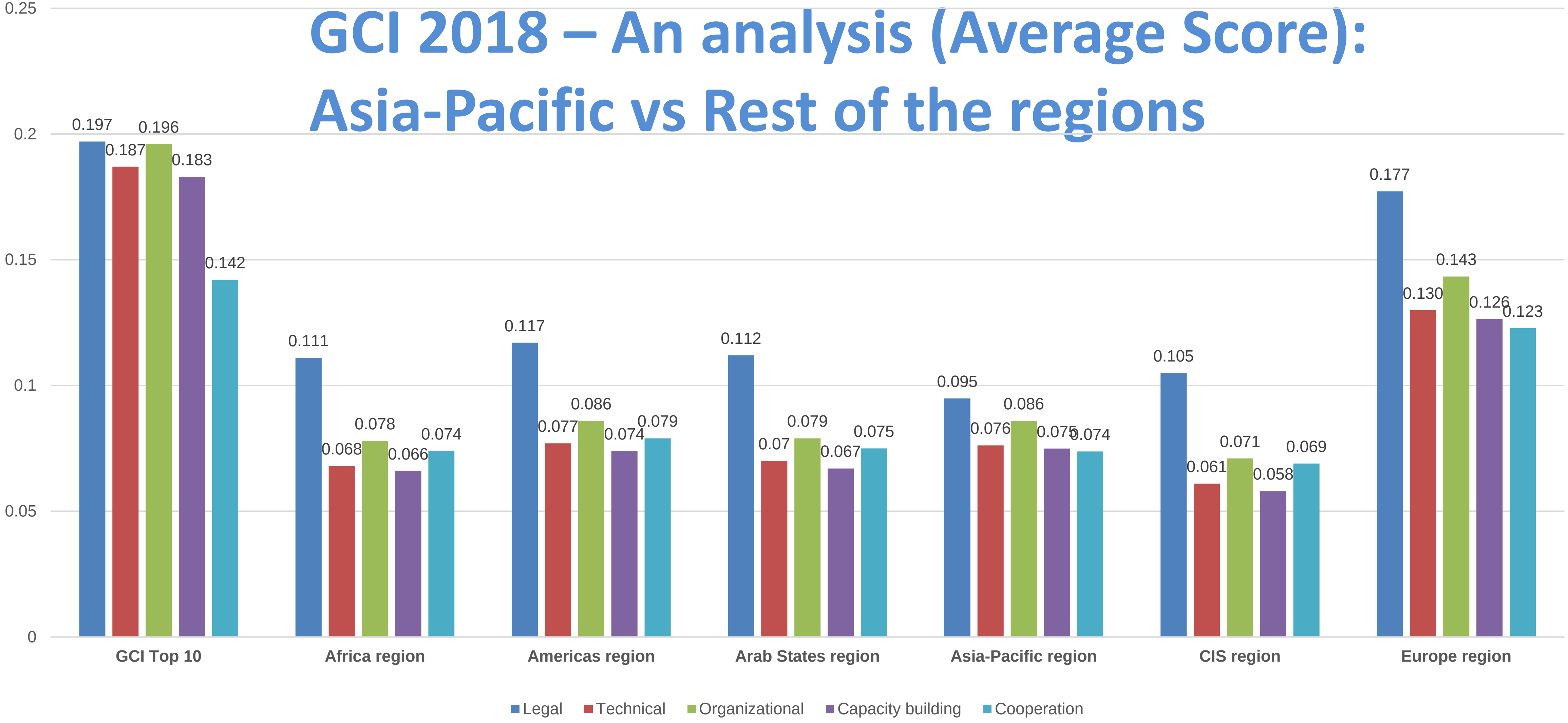
In 2018, only three regions are represented with countries having the most level of commitment: six countries from the Europe region, three from the Asia-Pacific region, and two from the Americas region

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



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

ITU Asia-Pacific and CIS Inter-Regional Cyberdrill

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

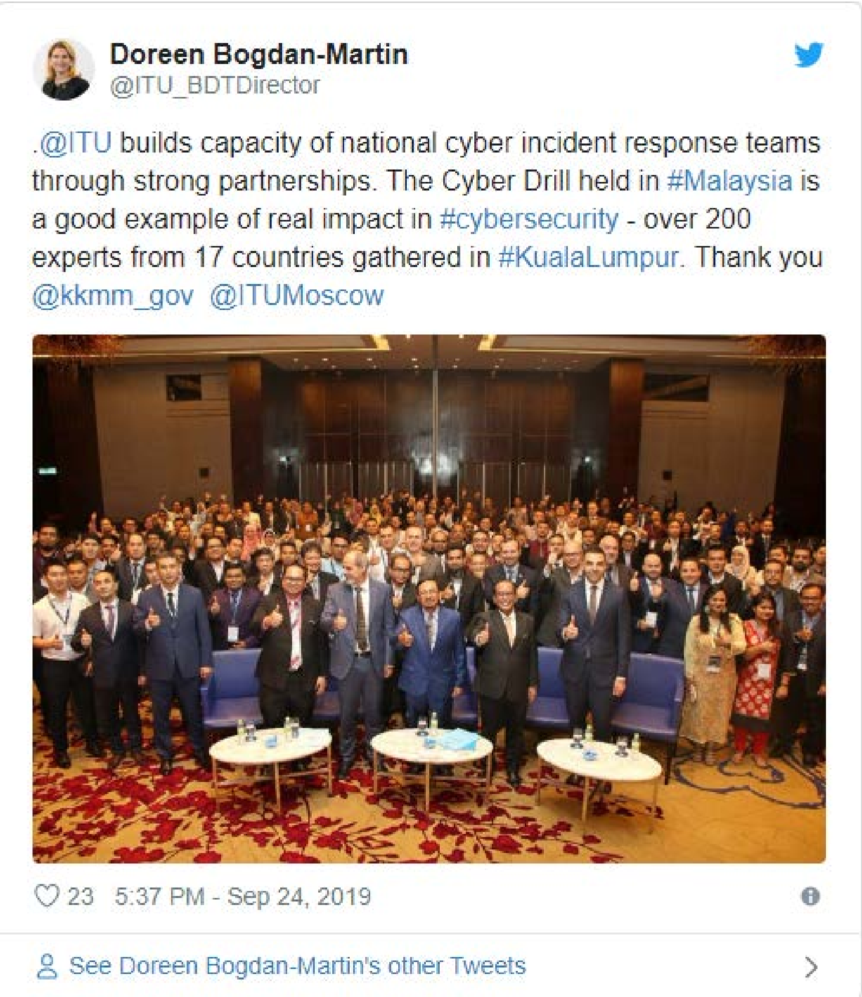
Hosted by

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



Doreen Bogdan-Martin
@ITU_BDTDirector

.@ITU builds capacity of national cyber incident response teams through strong partnerships. The Cyber Drill held in #Malaysia is a good example of real impact in #cybersecurity - over 200 experts from 17 countries gathered in #KualaLumpur. Thank you @kkmm_gov @ITUMoscow

♡ 23 5:37 PM - Sep 24, 2019

See Doreen Bogdan-Martin's other Tweets

Online Threats to Children

Cybergrooming

Child abuse materials

Pornography

Sexual solicitation

Disclosure private information

Child pornography

Threats & Risks

Violence

Cyberstalking

Racism

Online Fraud

Phishing attacks

Spam

Cyber Bullying

Youth-to-youth cybercrimes

Online Gaming & Addiction

Anorexia, self-harm or suicide

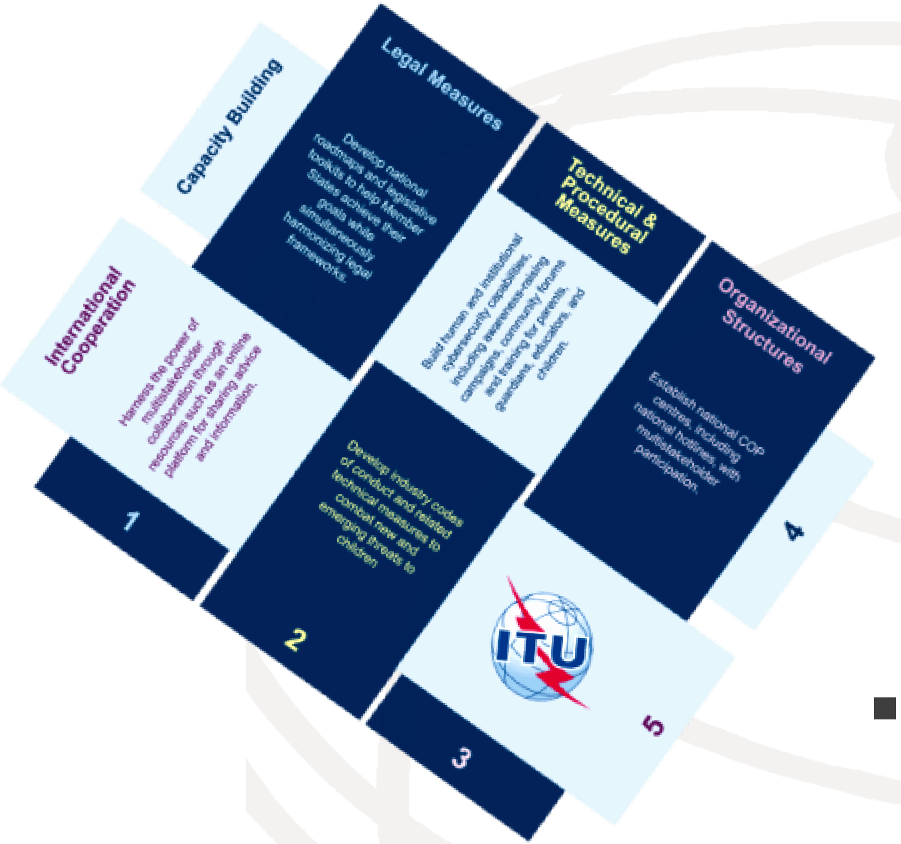
Child Online Protection (COP) Initiative

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



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

Capacity Building

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

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

Technical & Procedural Measures: 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

ITU

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

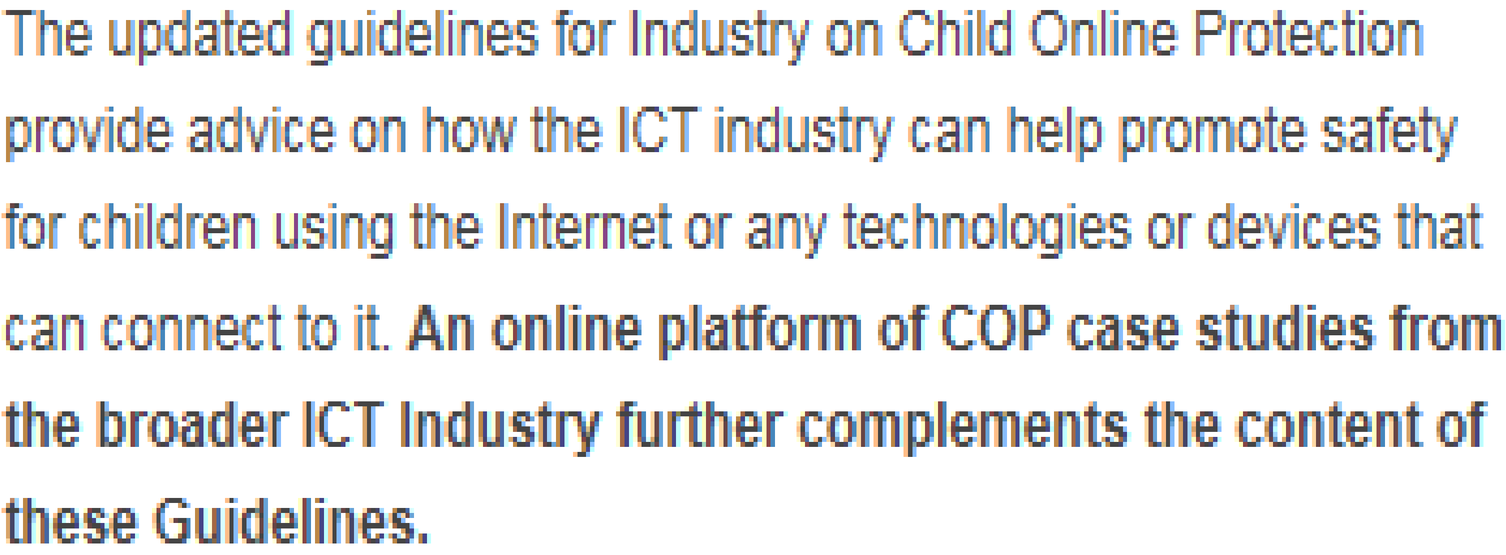
New COP Guidelines for Industry

Guidelines for Industry on Child Online Protection

2014 edition

ITU unicef

www.itu.int/cop



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

Integrate children’s rights in policies and management processes

Child sexual abuse content

Develop processes for handling child sexual abuse content

Safer and age appropriate environment

Develop safer and age appropriate online environments

Educate children, parents and teachers

Educate children, parents and teachers on children’s safety

Promote positive use of ICTS

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

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