Cybersecurity : ITU Initiatives

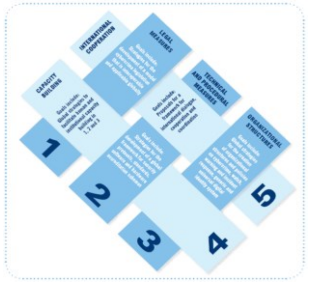
Sameer Sharma
ITU

Tehran , Iran
12-16 May 2018

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.

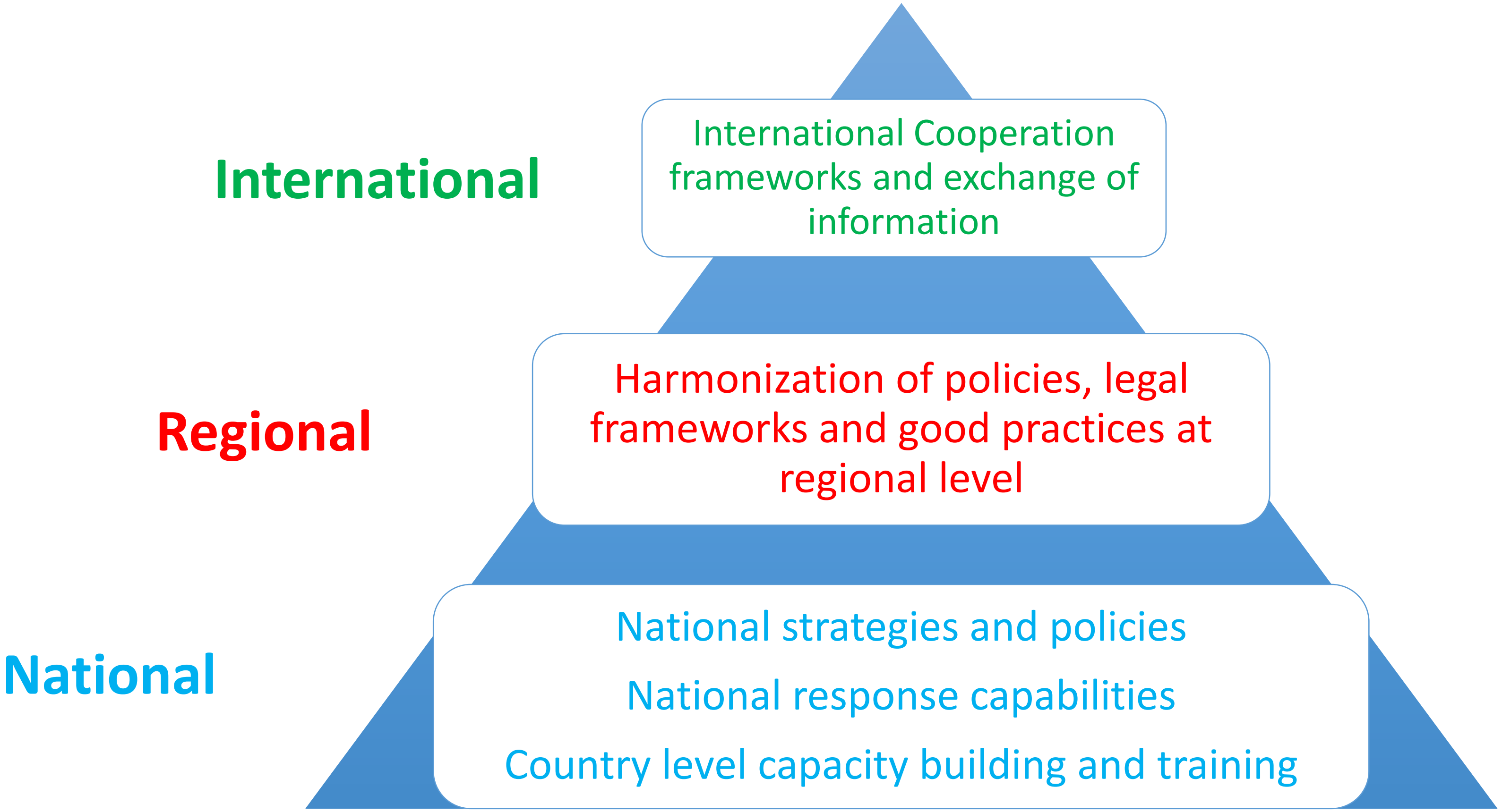
Building confidence and security in the use of ICTs is widely present in **PP and Conferences**' resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues,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

GCA Pillars

- **i. Legal Measures**
- **ii. Technical and Procedural Measures**
- **iii. Organizational Structure**
- **iv. Capacity Building**
- **v. International Cooperation**

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

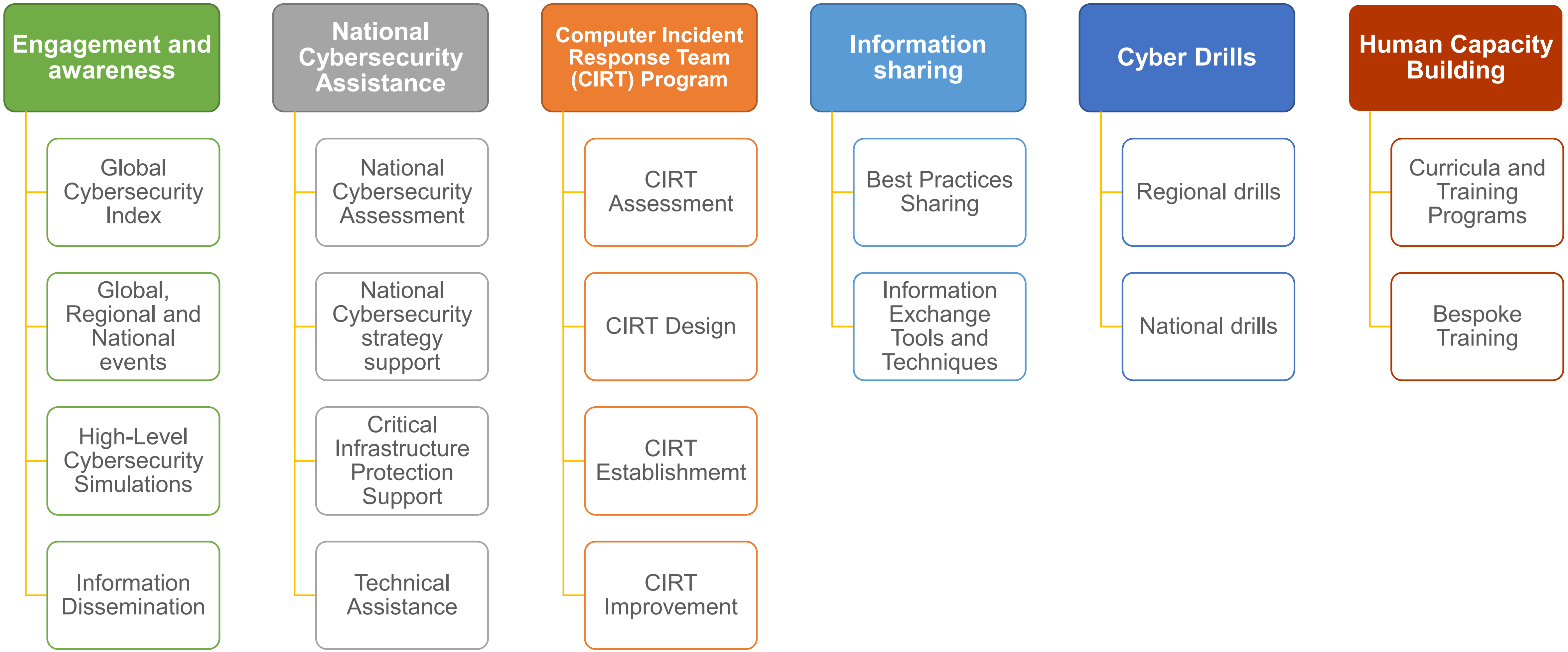
National strategies and policies

National response capabilities

Country level capacity building and training

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

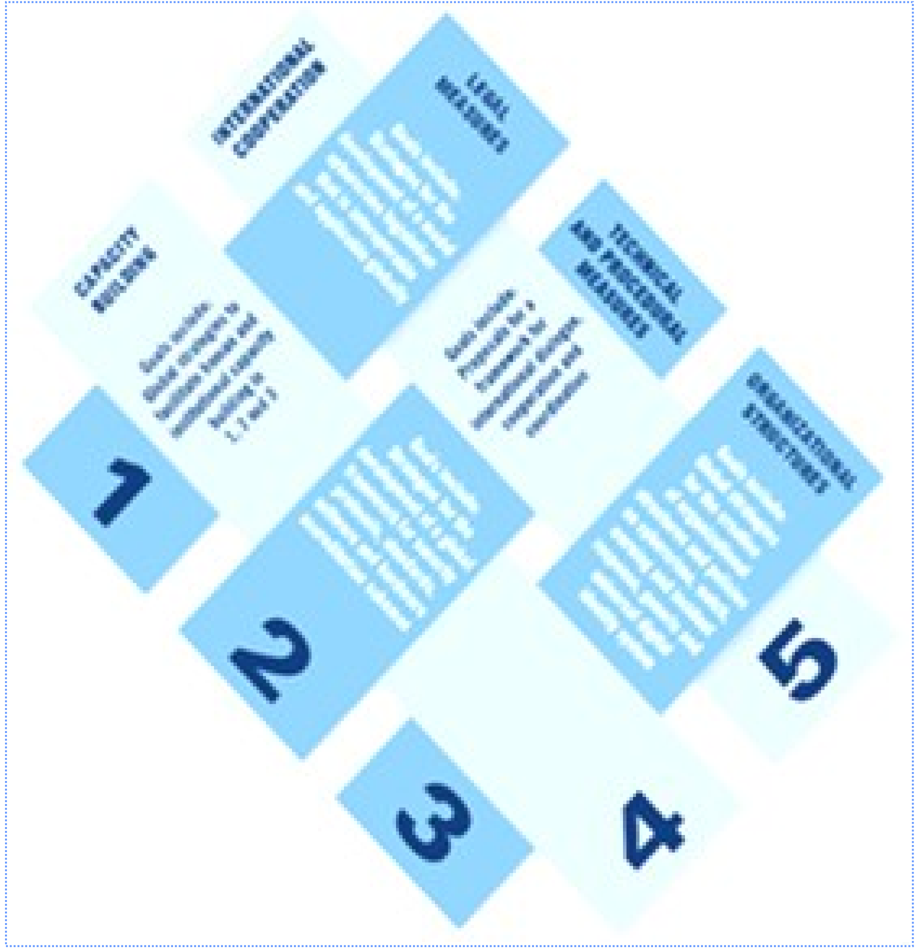
Information sharing
- Best Practices Sharing
- Information Exchange Tools and Techniques

Cyber Drills
- Regional drills
- National drills

Human Capacity Building
- Curricula and Training Programs
- Bespoke Training

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

Global Cybersecurity Index

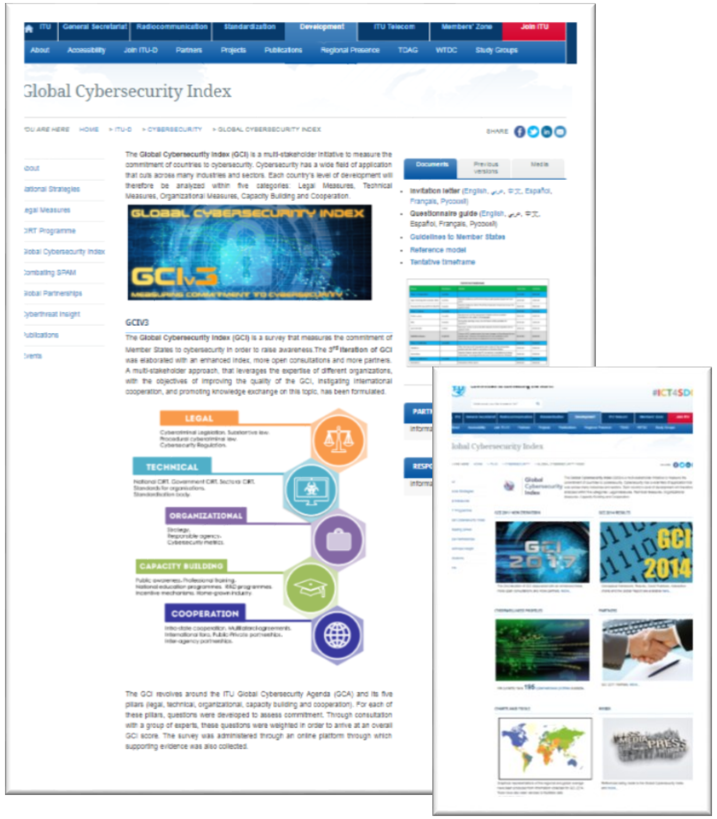
What is GCI …

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-Leve Experts and endorsed by the GCA.

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

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</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

Global Cybersecurity Index

OU ARE HERE HOME > ITU-D > CYBERSECURITY > GLOBAL CYBERSECURITY INDEX SHARE

bout
ational Strategies
egal Measures
IRT Programme
lobal Cybersecurity Index
ombating SPAM
lobal Partnerships
yberthreat Insight
ublications
vents

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.

GLOBAL CYBERSECURITY INDEX
GCIv3
MEASURING COMMITMENT TO CYBERSECURITY

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 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.

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.

Documents | Previous versions | Media

- **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

PART
informa

RESP
informa

#ICT4SDG

lobal Cybersecurity Index

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

Unique Value

What makes the GCI unique is the balanced combination of:

- The **broad geographic range** covering all Member States of ITU
- The study of cybersecurity in **five broad areas** (pillars of Global Cybersecurity Agenda)
- The **scoring and ranking** mechanisms
- The **cyberwellness** country **profiles**

GCI overall approach

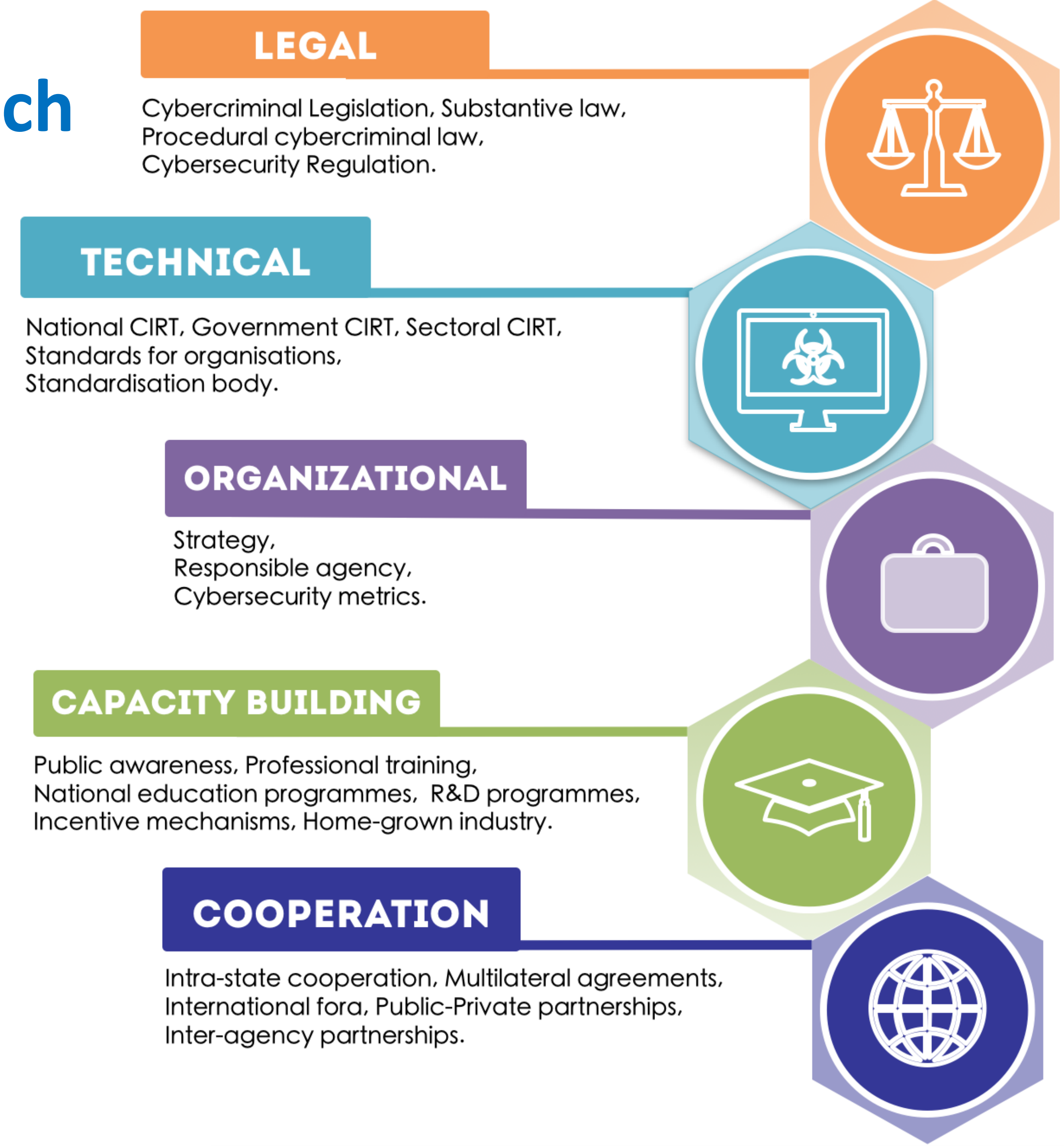
Goals

- Help countries identify areas for improvement
- Motivate action to improve relative GCI rankings
- Raise the level of cybersecurity worldwide
- Help to identify and promote best practices
- Foster a global culture of cybersecurity

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

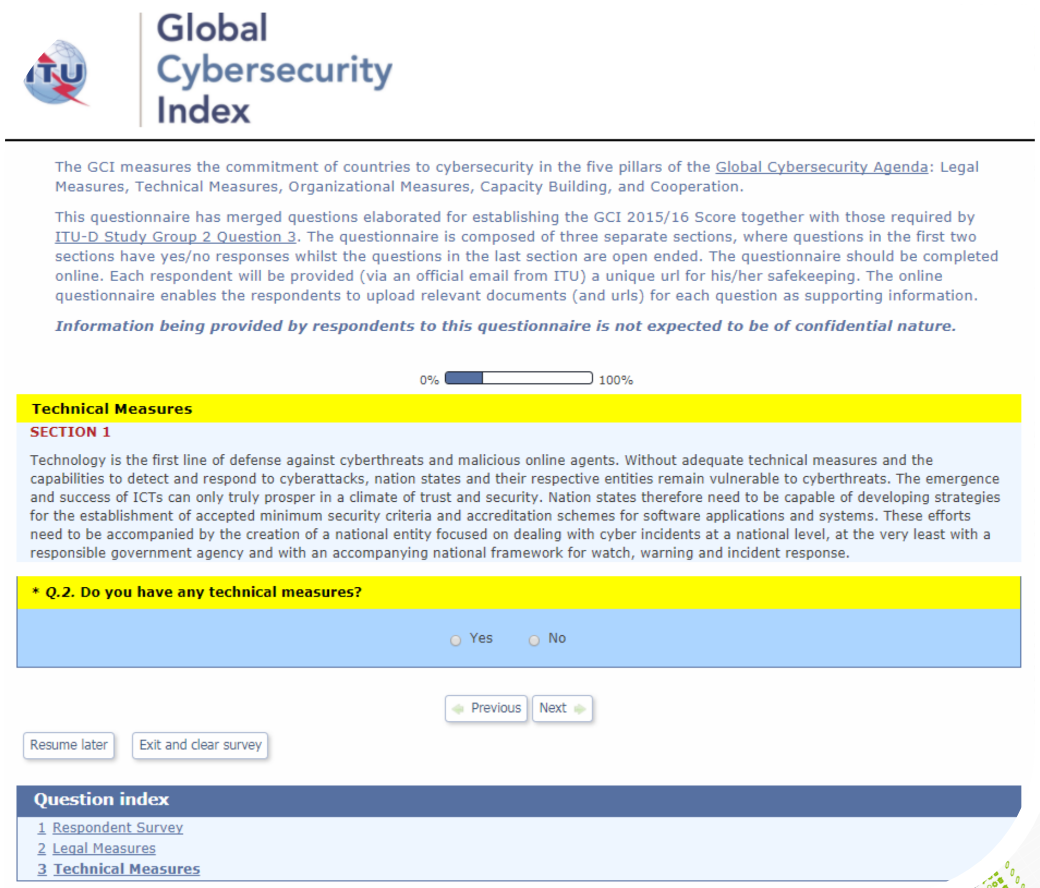
Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.

Online Survey

GCIv3

50

questions



Global Cybersecurity Index

The GCI measures the commitment of countries to cybersecurity in the five pillars of the Global Cybersecurity Agenda: Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation.

This questionnaire has merged questions elaborated for establishing the GCI 2015/16 Score together with those required by ITU-D Study Group 2 Question 3. The questionnaire is composed of three separate sections, where questions in the first two sections have yes/no responses whilst the questions in the last section are open ended. The questionnaire should be completed online. Each respondent will be provided (via an official email from ITU) a unique url for his/her safekeeping. The online questionnaire enables the respondents to upload relevant documents (and urls) for each question as supporting information.

Information being provided by respondents to this questionnaire is not expected to be of confidential nature.

Technical Measures

SECTION 1

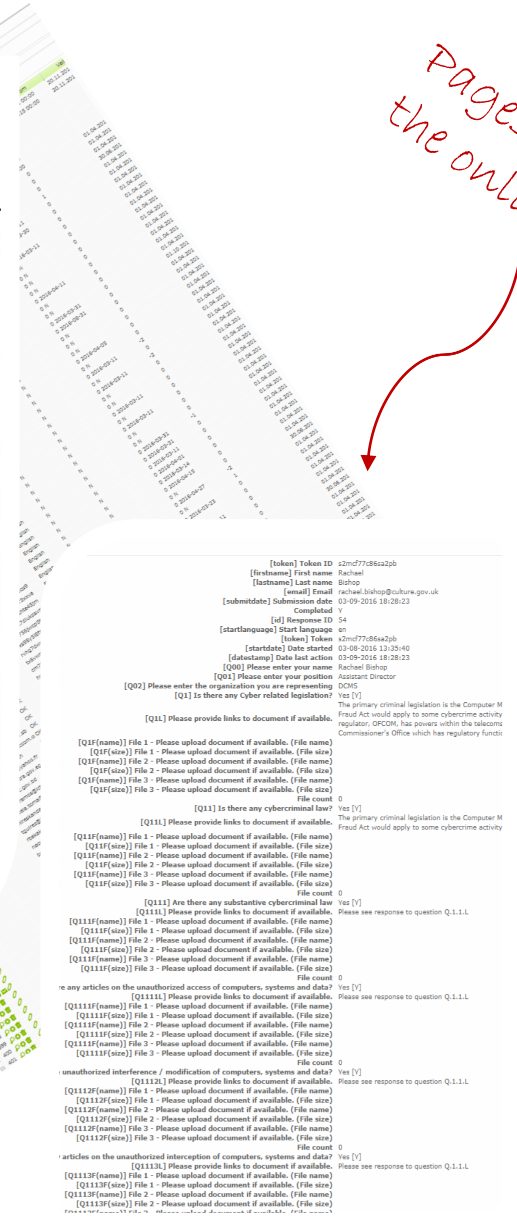
Technology is the first line of defense against cyberthreats and malicious online agents. Without adequate technical measures and the capabilities to detect and respond to cyberattacks, nation states and their respective entities remain vulnerable to cyberthreats. The emergence and success of ICTs can only truly prosper in a climate of trust and security. Nation states therefore need to be capable of developing strategies for the establishment of accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be accompanied by the creation of a national entity focused on dealing with cyber incidents at a national level, at the very least with a responsible government agency and with an accompanying national framework for watch, warning and incident response.

*** Q.2. Do you have any technical measures?**

○ Yes ○ No

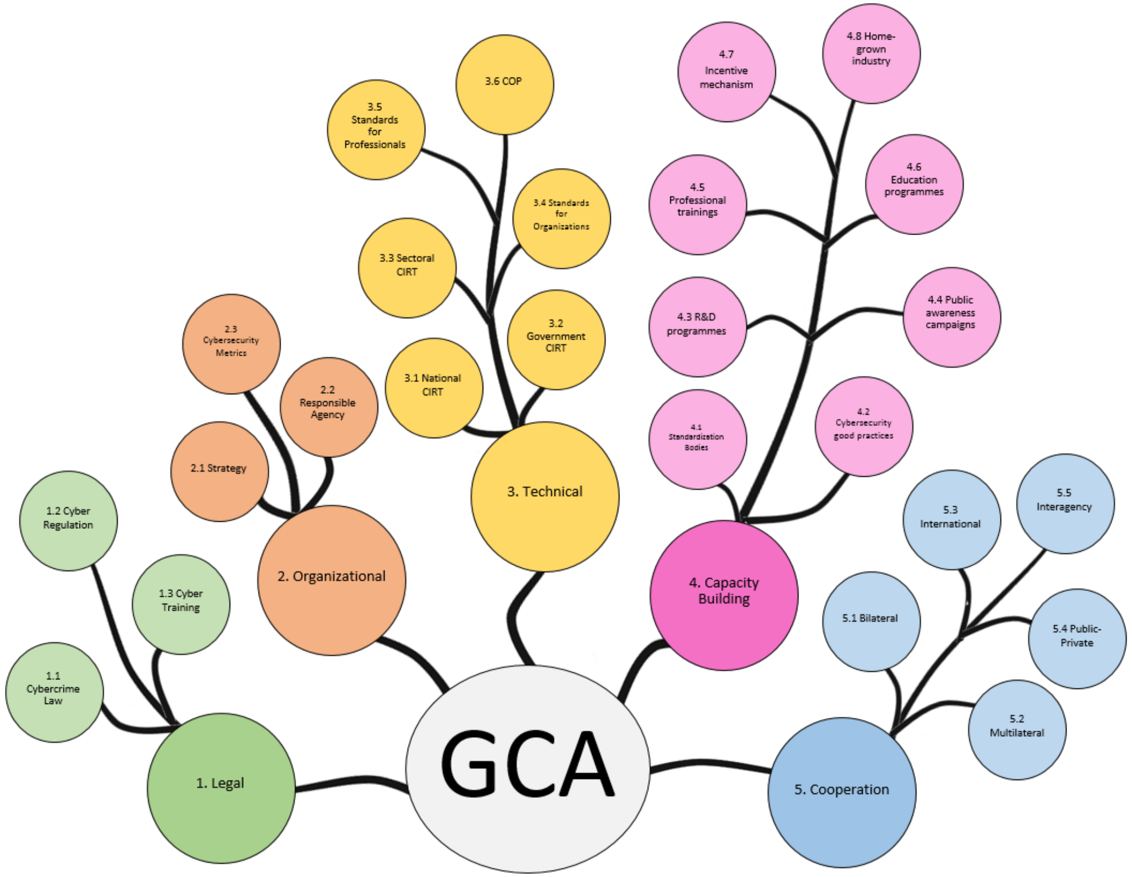
Question index

Pages from the online survey.

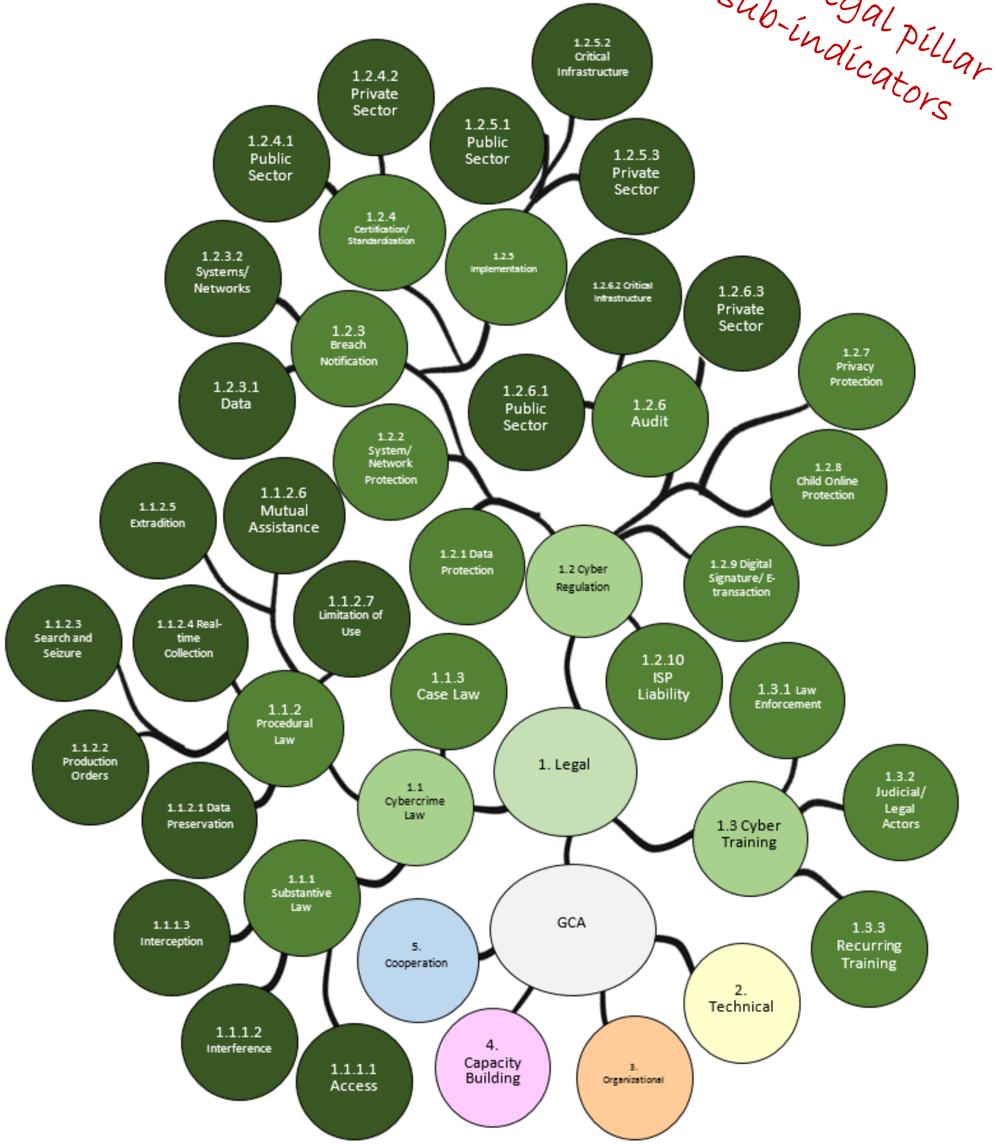


[token] Token ID	s2mcf77c86sa2pb
[firstname] First name	Rachael
[lastname] Last name	Bishop
[email] Email	rachael.bishop@culture.gov.uk
[submitdate] Submission date	03-09-2016 18:28:23
Completed	Y
[id] Response ID	54
[startlanguage] Start language	en
[token] Token	s2mcf77c86sa2pb
[startdate] Date started	03-08-2016 13:35:40
[datestamp] Date last action	03-09-2016 18:28:23
[Q00] Please enter your name	Rachael Bishop
[Q01] Please enter your position	Assistant Director
[Q02] Please enter the organization you are representing	DCMS
[Q1] Is there any Cyber related legislation?	Yes [Y]
[Q1L] Please provide links to document if available.	The primary criminal legislation is the Computer M Fraud Act would apply to some cybercrime activity regulator, OFCOM, has powers within the telecoms Commissioner's Office which has regulatory functic
[Q1F(name)] File 1 - Please upload document if available. (File name)	
[Q1F(size)] File 1 - Please upload document if available. (File size)	
[Q1F(name)] File 2 - Please upload document if available. (File name)	
[Q1F(size)] File 2 - Please upload document if available. (File size)	
[Q1F(name)] File 3 - Please upload document if available. (File name)	
[Q1F(size)] File 3 - Please upload document if available. (File size)	
File count	0
[Q11] Is there any cybercriminal law?	Yes [Y]
[Q11L] Please provide links to document if available.	The primary criminal legislation is the Computer M Fraud Act would apply to some cybercrime activity
[Q11F(name)] File 1 - Please upload document if available. (File name)	
[Q11F(size)] File 1 - Please upload document if available. (File size)	
[Q11F(name)] File 2 - Please upload document if available. (File name)	
[Q11F(size)] File 2 - Please upload document if available. (File size)	
[Q11F(name)] File 3 - Please upload document if available. (File name)	
[Q11F(size)] File 3 - Please upload document if available. (File size)	
File count	0
[Q111] Are there any substantive cybercriminal law	Yes [Y]
[Q111L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q111F(name)] File 1 - Please upload document if available. (File name)	
[Q111F(size)] File 1 - Please upload document if available. (File size)	
[Q111F(name)] File 2 - Please upload document if available. (File name)	
[Q111F(size)] File 2 - Please upload document if available. (File size)	
[Q111F(name)] File 3 - Please upload document if available. (File name)	
[Q111F(size)] File 3 - Please upload document if available. (File size)	
File count	0
re any articles on the unauthorized access of computers, systems and data?	Yes [Y]
[Q1111L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q1111F(name)] File 1 - Please upload document if available. (File name)	
[Q1111F(size)] File 1 - Please upload document if available. (File size)	
[Q1111F(name)] File 2 - Please upload document if available. (File name)	
[Q1111F(size)] File 2 - Please upload document if available. (File size)	
[Q1111F(name)] File 3 - Please upload document if available. (File name)	
[Q1111F(size)] File 3 - Please upload document if available. (File size)	
File count	0
unauthorized interference / modification of computers, systems and data?	Yes [Y]
[Q1112L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q1112F(name)] File 1 - Please upload document if available. (File name)	
[Q1112F(size)] File 1 - Please upload document if available. (File size)	
[Q1112F(name)] File 2 - Please upload document if available. (File name)	
[Q1112F(size)] File 2 - Please upload document if available. (File size)	
[Q1112F(name)] File 3 - Please upload document if available. (File name)	
[Q1112F(size)] File 3 - Please upload document if available. (File size)	
File count	0
articles on the unauthorized interception of computers, systems and data?	Yes [Y]
[Q1113L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q1113F(name)] File 1 - Please upload document if available. (File name)	
[Q1113F(size)] File 1 - Please upload document if available. (File size)	
[Q1113F(name)] File 2 - Please upload document if available. (File name)	
[Q1113F(size)] File 2 - Please upload document if available. (File size)	

GCI and GCA correlation

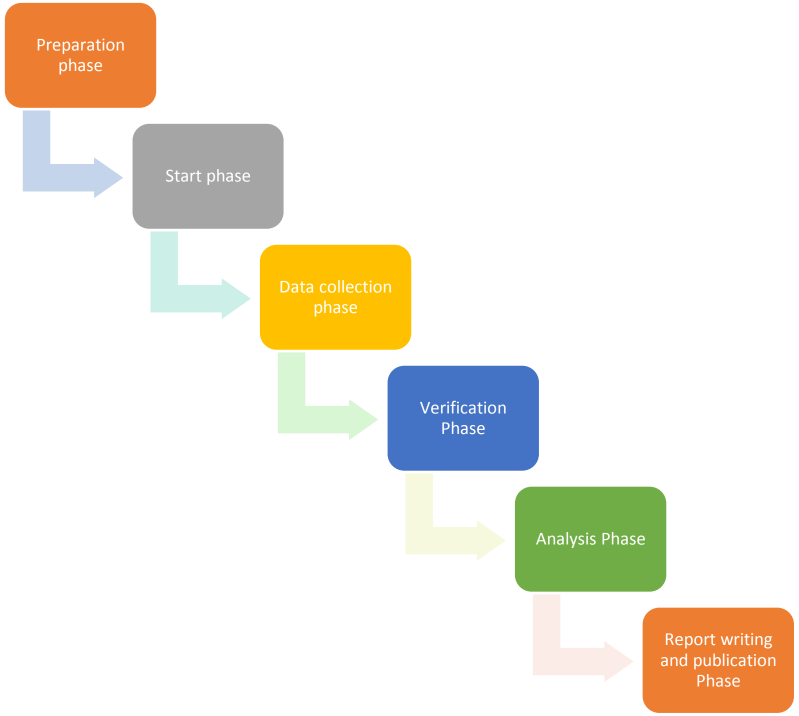


Example of the Legal pillar and its indicators, sub-indicators



How it functions. Main steps.

- Preparation phase
  - Elaboration of the survey in collaboration with experts an 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 and 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

Panel of Expert: an average for each question weightage provided by GCI Partners

2. Do you have any technical measures?	19.12
2.1. Is there a CIRT, CSIRT or CERT with national responsibility?	4.65
2.1.1. Does it have a government mandate?	1.33
2.1.2. Does the CIRT, CSIRT or CERT conduct recurring cybersecurity exercise?	1.23
2.1.3. Is the CIRT, CSIRT or CERT affiliated with FIRST?	1.04
2.1.4. Is the CIRT, CSIRT or CERT affiliated with any other CERT communities? (regional CERT)	1.06
2.2. Is there a Government CERT?	3.03
2.3. Are there any sectoral CERTs?	2.71

1. Is there any Cyber related legislation?	20.94
2. Do you have any technical measures?	19.12
3. Do you have any organizational measures?	19.67
4. Do you have any capacity building activities?	18.93
5. Do you have any cooperative measures?	21.34

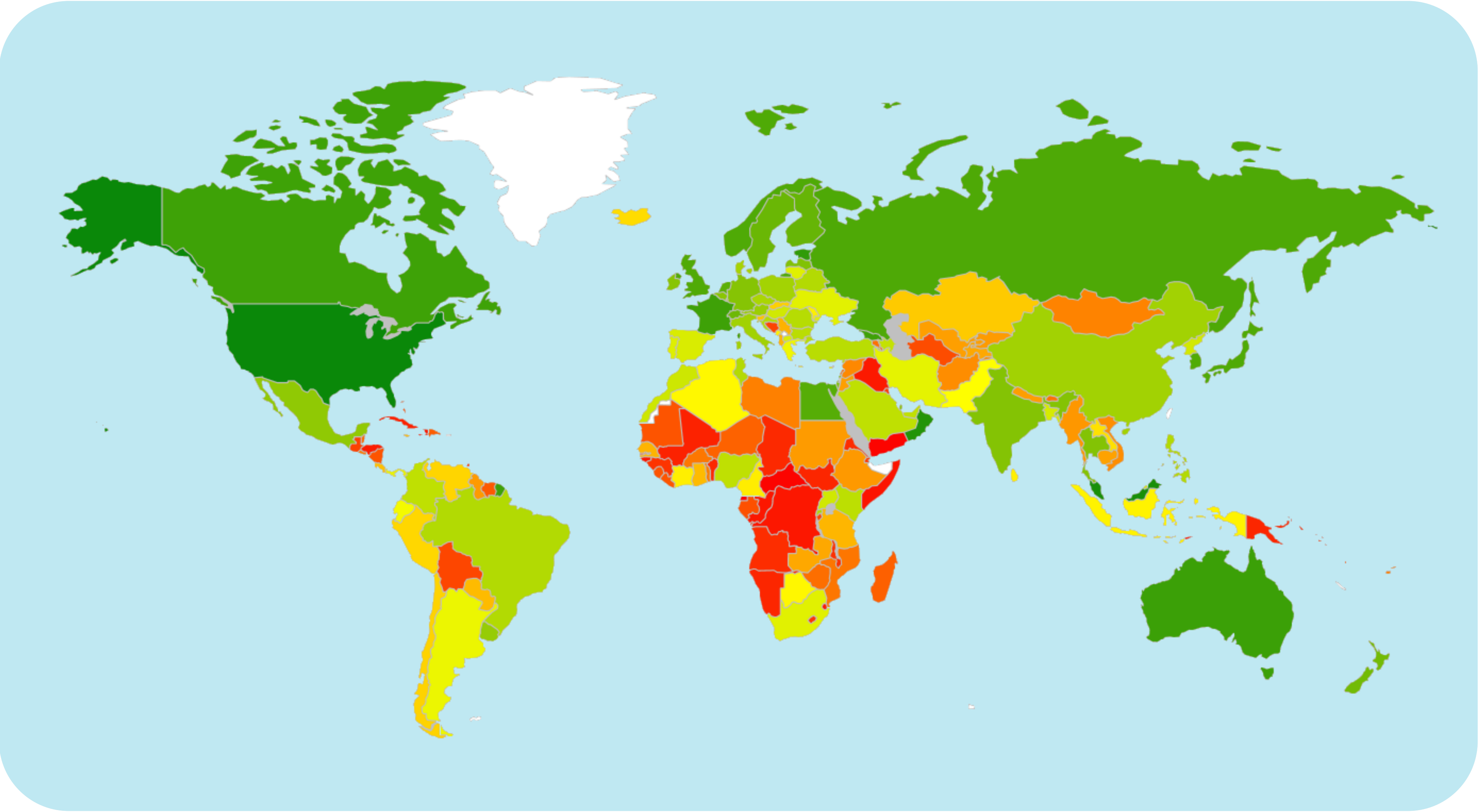
Total of all weightages = 100

How to improve GCI score and position

1. Commit to Cybersecurity!
2. Make continuous progress in all 5 pillars!
3. Make all relevant data available!
4. Cooperate when and where possible!
5. **Actively participate in GCI!**

Results

GCIv2 World Heat Map



Commitment levels 🟩 High 🟨 Medium 🟥 Low

GCIv2 results

2017 GCI Participants

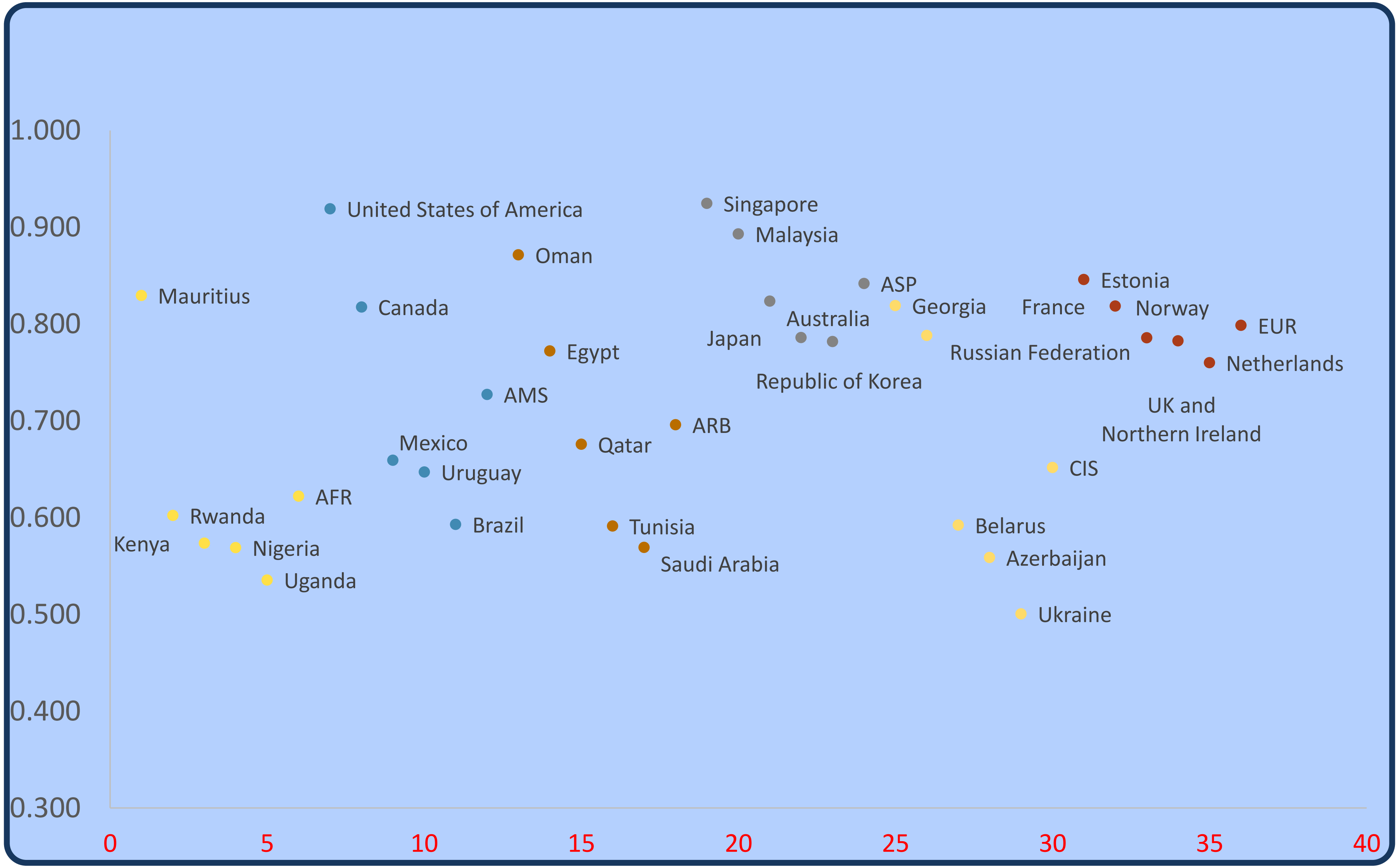
Region	AFR	AMS	ARB	ASP	CIS	EUR	GLO
Responses	29	23	16	25	7	34	134
Non responses	15	12	5	13	5	9	59
Total of participants	44	35	21	38	12	43	193

GCIv2 Global Top Ten

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

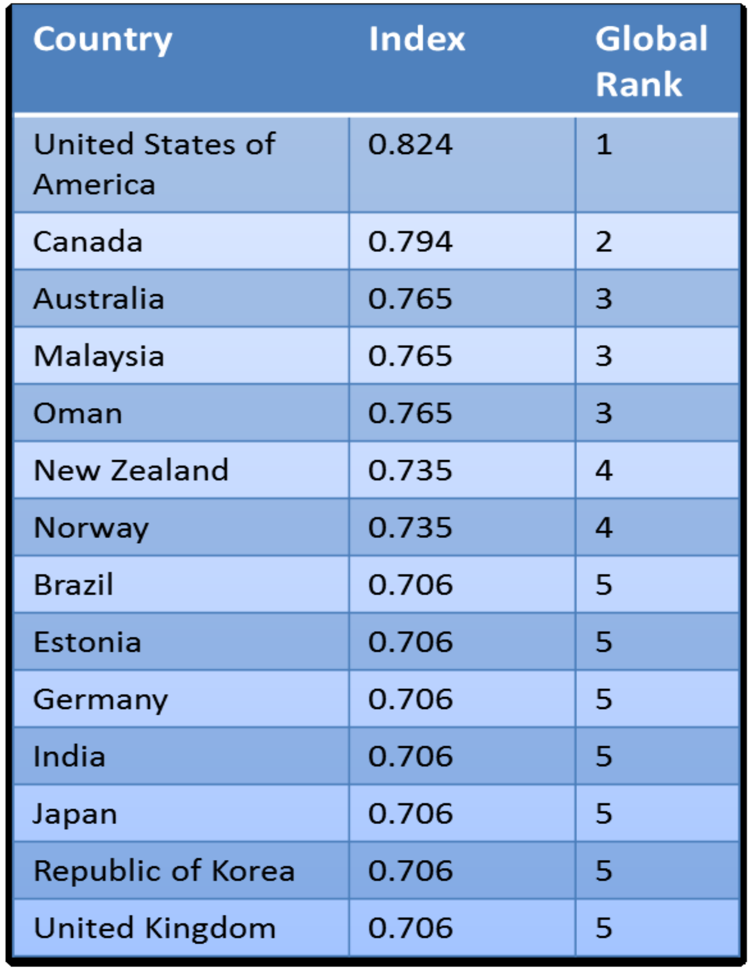
Maximum score is 1

GCIv2 top five for each region



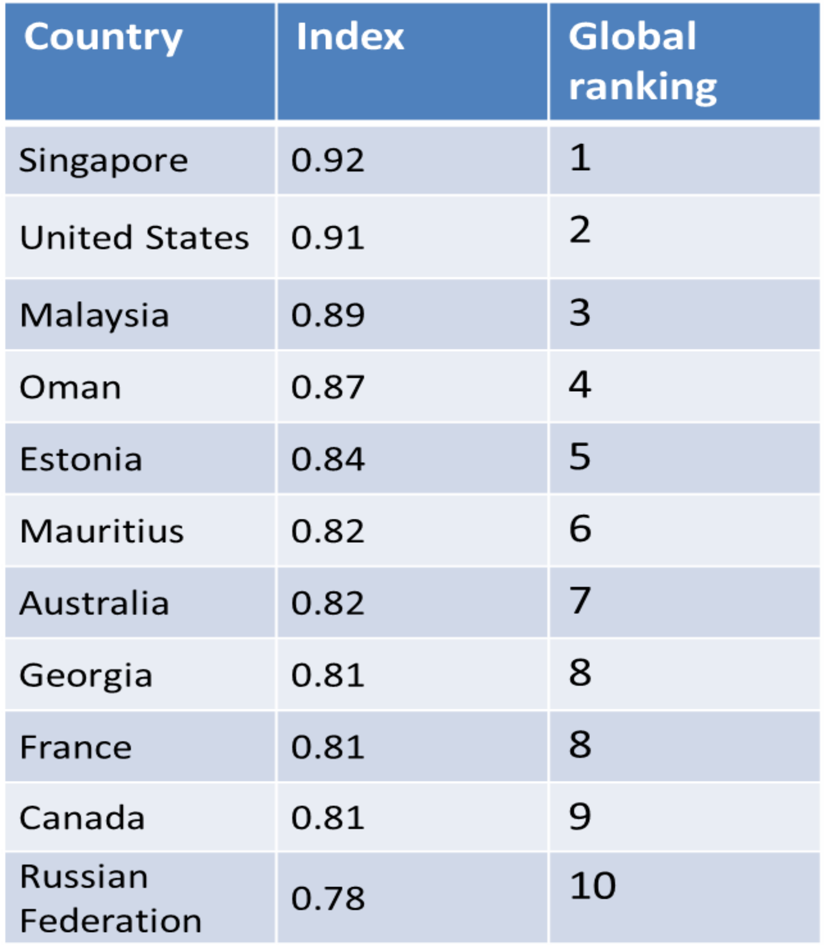
GCI results Version 1 vs Version 2

105 responses



Country	Index	Global Rank
United States of America	0.824	1
Canada	0.794	2
Australia	0.765	3
Malaysia	0.765	3
Oman	0.765	3
New Zealand	0.735	4
Norway	0.735	4
Brazil	0.706	5
Estonia	0.706	5
Germany	0.706	5
India	0.706	5
Japan	0.706	5
Republic of Korea	0.706	5
United Kingdom	0.706	5

134 responses



Country	Index	Global ranking
Singapore	0.92	1
United States	0.91	2
Malaysia	0.89	3
Oman	0.87	4
Estonia	0.84	5
Mauritius	0.82	6
Australia	0.82	7
Georgia	0.81	8
France	0.81	8
Canada	0.81	9
Russian Federation	0.78	10

Cybersecurity Standards

ITU-T Recommandations on Security

Work item	Question	Status	Subject / Title
X.1126 (ex X.msec-11)	Q6/17	Approved 2017-03-30	Guidelines on mitigating the negative effects of infected terminals in mobile networks
X.1127 (ex X.msec-9)	Q6/17	Approved 2017-09-06	Functional security requirements and architecture for mobile phone anti-theft measures
X.1362 (ex X.iotsec-1)	Q6/17	Approved 2017-03-30	Simple encryption procedure for Internet of things (IoT) environments
X.1373 (ex X.itssec-1)	Q6/17	Approved 2017-03-30	Secure software update capability for intelligent transportation system communication devices
X.1331 (ex X.sgsec-2)	Q6/17	Determined 2017-09-06	Security guidelines for home area network (HAN) devices in smart grid systems
X.ibc-iot	Q6/17	Under study	Security Requirements and Framework of Using Identity-Based Cryptography Mechanism in Internet of Things
X.iotsec-2	Q6/17	Under study	Security framework for Internet of things
X.iotsec-3	Q6/17	Under study	Technical framework of PII (Personally Identifiable Information) handling system in IoT environment

Work item	Question	Status	Subject / Title
X.1126 (ex X.msec-11)	Q6/17	Approved 2017-03-30	Guidelines on mitigating the negative effects of infected terminals in mobile networks
X.1127 (ex X.msec-9)	Q6/17	Approved 2017-09-06	Functional security requirements and architecture for mobile phone anti-theft measures
X.1362 (ex X.iotsec-1)	Q6/17	Approved 2017-03-30	Simple encryption procedure for Internet of things (IoT) environments
X.1373 (ex X.itssec-1)	Q6/17	Approved 2017-03-30	Secure software update capability for intelligent transportation system communication devices
X.1331 (ex X.sgsec-2)	Q6/17	Determined 2017-09-06	Security guidelines for home area network (HAN) devices in smart grid systems
X.ibc-iot	Q6/17	Under study	Security Requirements and Framework of Using Identity-Based Cryptography Mechanism in Internet of Things
X.iotsec-2	Q6/17	Under study	Security framework for Internet of things
X.iotsec-3	Q6/17	Under study	Technical framework of PII (Personally Identifiable Information) handling system in IoT environment

Security Standardization

- National laws and regulations are often very generic so as to withstand time and technological evolvement, thus must be complimented with **standards**, i.e., specification on technical, procedural and administrative (organizational) details.
- Cyberspace doesn't recognize national boundaries, therefore security needs **international** standards.
- SG17 is a major venue where such international security standards can be, and are being, developed.
- SG17 collaborates with ISO/IEC JTC 1, ETSI, IETF, …

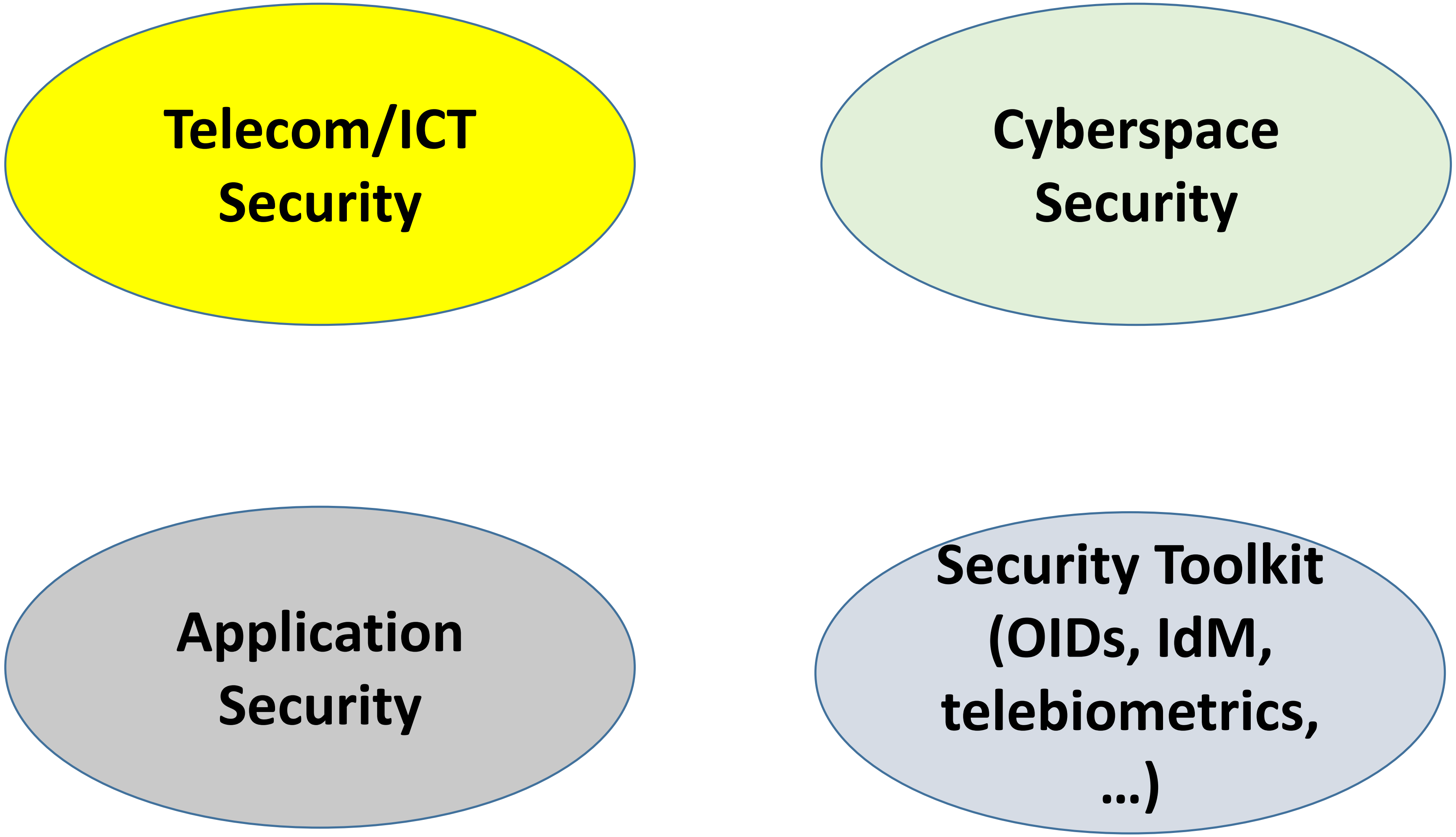
ITU-T SG17 ‘Security’ mandate

Responsible for building confidence and security in the use of information and communication technologies (ICTs).

This includes studies relating to **cybersecurity**, **security management**, **countering spam** and **identity management**.

It also includes **security architecture and framework**, **protection of personally identifiable information**, and **security of applications and services** for the Internet of things (IoT), smart grid, smartphone, software defined networking (SDN), Internet Protocol television (IPTV), web services, social network, cloud computing, big data analytics, mobile financial system and telebiometrics.

Security subjects within Study Group 17



Telecom/ICT Security

Cyberspace Security

Application Security

Security Toolkit (OIDs, IdM, telebiometrics, …)

Key SG17 standards

- X.800-series on OSI Security Architecture
  - X.800|ISO/IEC 7498-2:1989 OSI security architecture
  - X.805 Security architecture for end-to-end communications
- X.500-series on OSI Directory
  - X.509 Public-key and attribute certificate frameworks
- X.1051-X.1058 on information security management for teleco industry
- X.1205-1213 on Cybersecurity
- X.1231, 1240-1248 on Countering spam
- X.1250-1258, 1275 on Identity management
- X.1500-series on Cybersecurity information exchange

Current hot topics - 1

- Q13/17 security aspects of Intelligent Transport Systems

Security guidelines for V2X communication systems

Security requirements for vehicle accessible external devices

Methodologies for intrusion detection system on in-vehicle systems

Security guidelines for vehicular edge computing

Current hot topics - 2

- Q14/17 security aspects of Distributed Ledger Technology

Privacy and security considerations for using DLT data in Identity Management

Security assurance for Distributed Ledger Technology

Security capabilities and threats of Distributed Ledger Technology

Security architecture for Distributed Ledger Technology

Security Services based on Distributed Ledger Technology

Security threats to online voting using distributed ledger technology

Security threats and requirements for digital payment services based on distributed ledger technology

Current hot topics - 3

- Q8/17 cloud computing security
- Data analytics (middlebox security)

Data security requirements for the monitoring service of cloud computing

Guidelines on security of Big Data as a Service

Security guidelines of lifecycle management for telecom Big Data

Security requirements for Communication as a Service application environments

Security requirements of public infrastructure as a service (IaaS) in cloud computing

Security requirements of Network as a Service (NaaS) in cloud computing

Current hot topics - 4

- Q6/17 IoT security
- Identity management for IoT

Security Requirements and Framework of Using Identity-Based Cryptography Mechanism in IoT environment

Security framework for Internet of things

Technical framework of PII (Personally Identifiable Information) handling system in IoT environment

Security Requirements and Framework for Narrow Band Internet of Things

Secure Software Update for IoT devices

Cybersecurity in Asia-Pacific region

- Cybercrime Legislation and ITU –UNODC- INTERPOL Workshop (2017)
- National Cybersecurity Strategy & Cybersecurity Awareness : Nepal (2016-2015)
- Readiness Assessment to Establish a National CIRT for Fiji (2014-2015)
- Workshop on Cybersecuirty and Cybercrime Legislation & Cybersecurity Incident Simulation Bangkok 23 March 2015
- INTERPOL-ITU Cybercrime Investigation Seminar,19-21 Feb 2014, Malaysia
- First Pacific Islands Capacity Building Workshop on Child Online Protection and Commonwealth National Cybersecurity Framework Regional Workshop, 22-24 September 2014, Vanuatu
- Establishment of Pac CIRT, Fiji
- Readiness assessment National Cybersecurity Strategy, Bangladesh (2013)
- ITU Cyber Security Forum & Cyber Drill, 9-11 Dec 2013, Vientiane, Lao P.D.R
- Enhancement of cybersecurity capabilities (CIRT) Bhutan (2013)
- CIRT Capacity Building for Afghanistan (2014 and 2015)

Cybersecurity in Pacific Island Countries 2018

PROJECT OBJECTIVE

- The objectives of this proposed project are:
- To establish and strengthen of national CIRTS and enhancing coordination, collaboration and information exchange between national CIRTs and with other relevant players;
- To strengthen national cybersecurity policy frameworks that will include assessment and design of national CIRTs from civilian usage perspective;
- To build human and institutional capacity for efficient and effective use of capabilities of CIRTs .

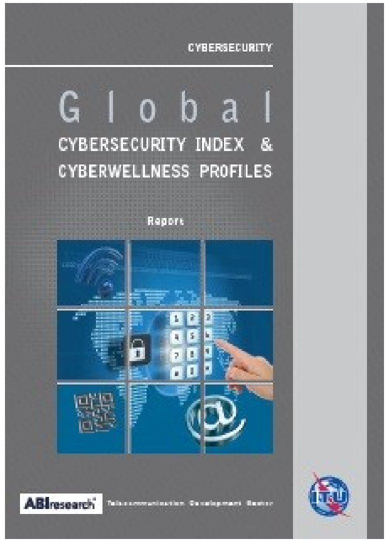
EXPECTED RESULTS

- Stronger coordination, collaboration and information sharing between CIRTS and other relevant players;
- Readiness assessments for national CIRT establishment for selected Pacific Island countries namely Tonga, Samoa, Papua New Guinea and Vanuatu;
- Design and implementation plan for each national CIRT;
- Stocktaking of activities being undertaken in the selected countries by national, regional, and international organisations, and in the region in general; and
- Awareness and hands-on training workshops aimed at building and strengthening human capacity in cybersecurity related matters in general and CIRTs in particular.

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 Resources / Publications on Cybersecurity

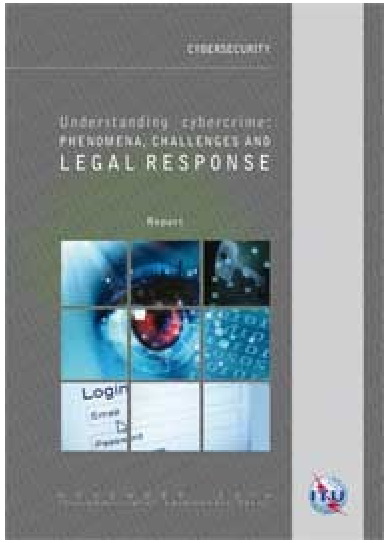


CYBERSECURITY

Global
CYBERSECURITY INDEX & CYBERWELLNESS PROFILES

Report

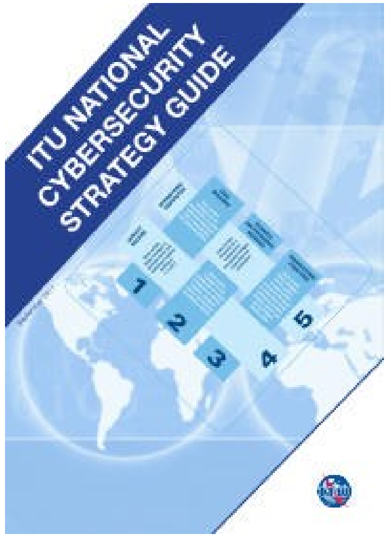
ABIresearch Telecommunication Development Sector



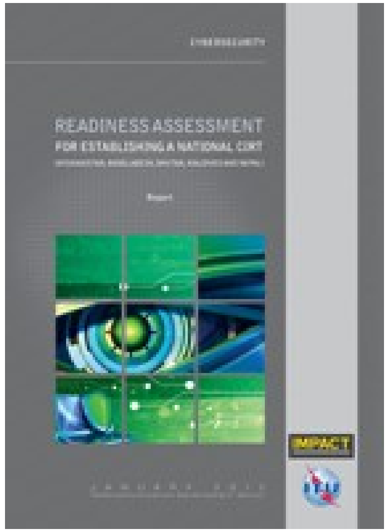
CYBERSECURITY

Understanding cybercrime:
PHENOMENA, CHALLENGES AND
LEGAL RESPONSE

Report



ITU NATIONAL
CYBERSECURITY
STRATEGY GUIDE

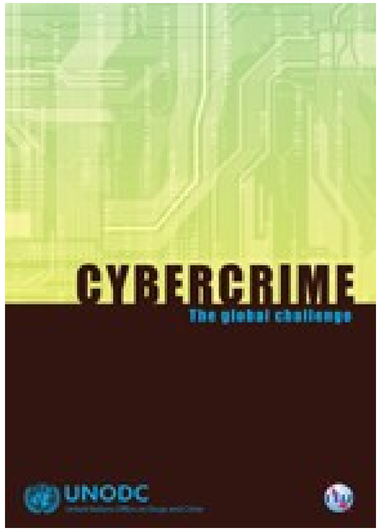


CYBERSECURITY

READINESS ASSESSMENT
FOR ESTABLISHING A NATIONAL CIRT

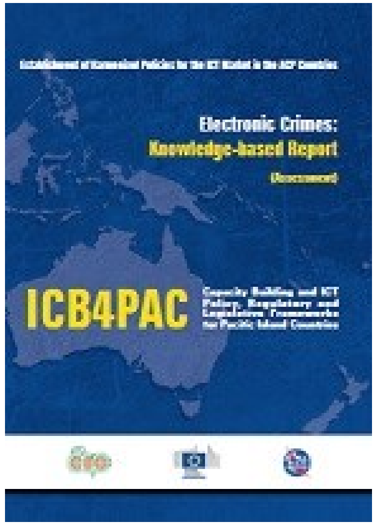
Report

IMPACT



CYBERCRIME
The global challenge

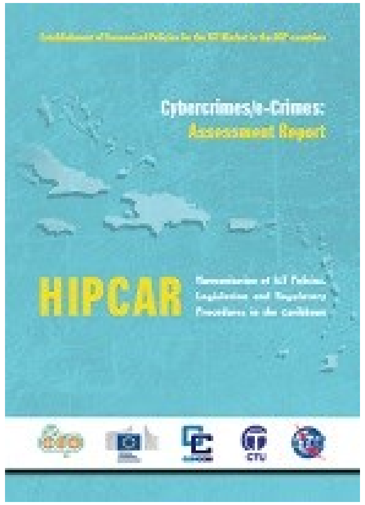
UNODC



Electronic Crimes:
Knowledge-based Report

ICB4PAC

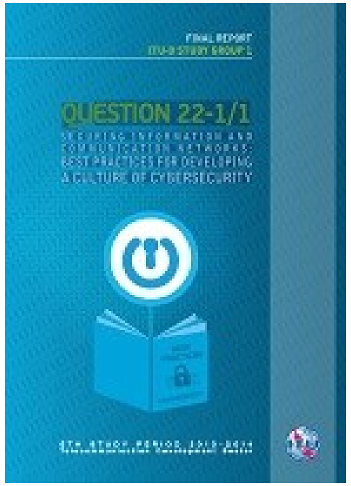
Capacity Building and ICT Policy, Regulatory and Legislative Frameworks for Pacific Island Countries



Cybercrimes/e-Crimes:
Assessment Report

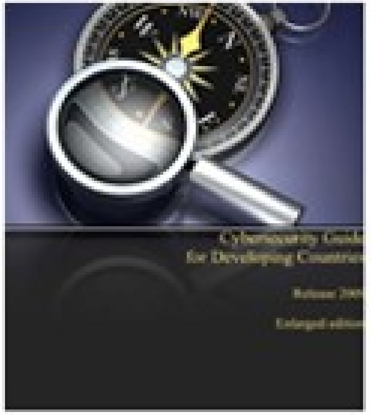
HIPCAR

CTU



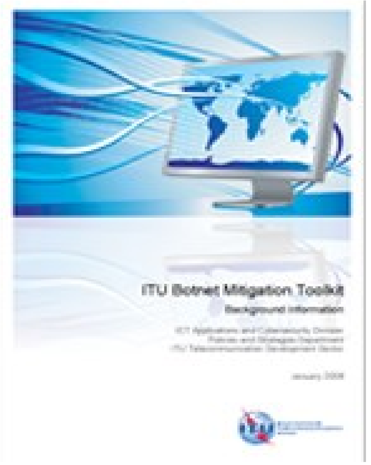
FINAL REPORT
ITU-D STUDY GROUP 1

QUESTION 22-1/1
SECURING INFORMATION AND COMMUNICATION NETWORKS: BEST PRACTICES FOR DEVELOPING A CULTURE OF CYBERSECURITY



Cybersecurity Guide
for Developing Countries

Enlarged edition



ITU Botnet Mitigation Toolkit
Background information

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

ITU : I Thank U