

ITU GCI OVERVIEW



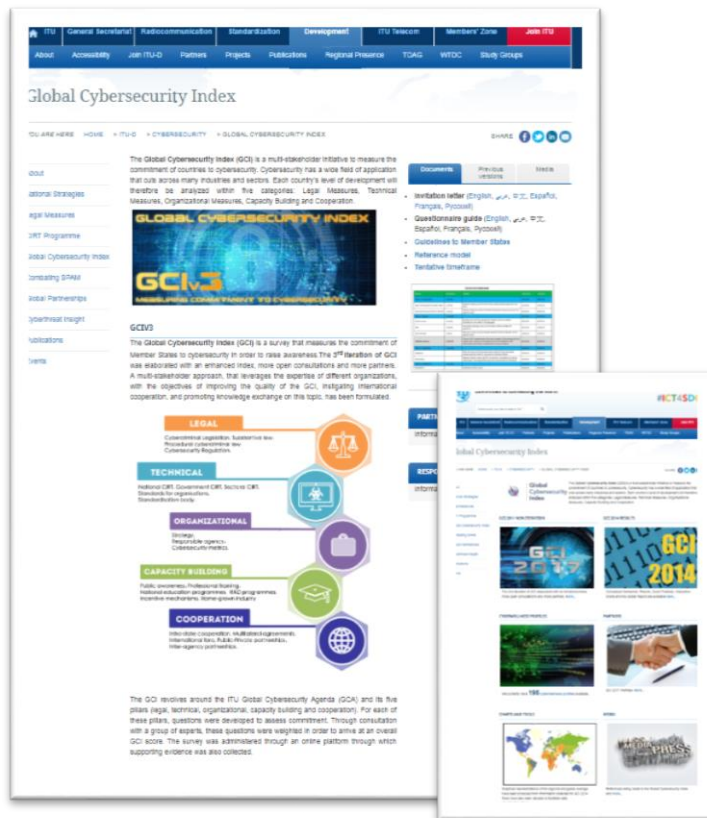
What is GCI ...

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”

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 started in March 2018**



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

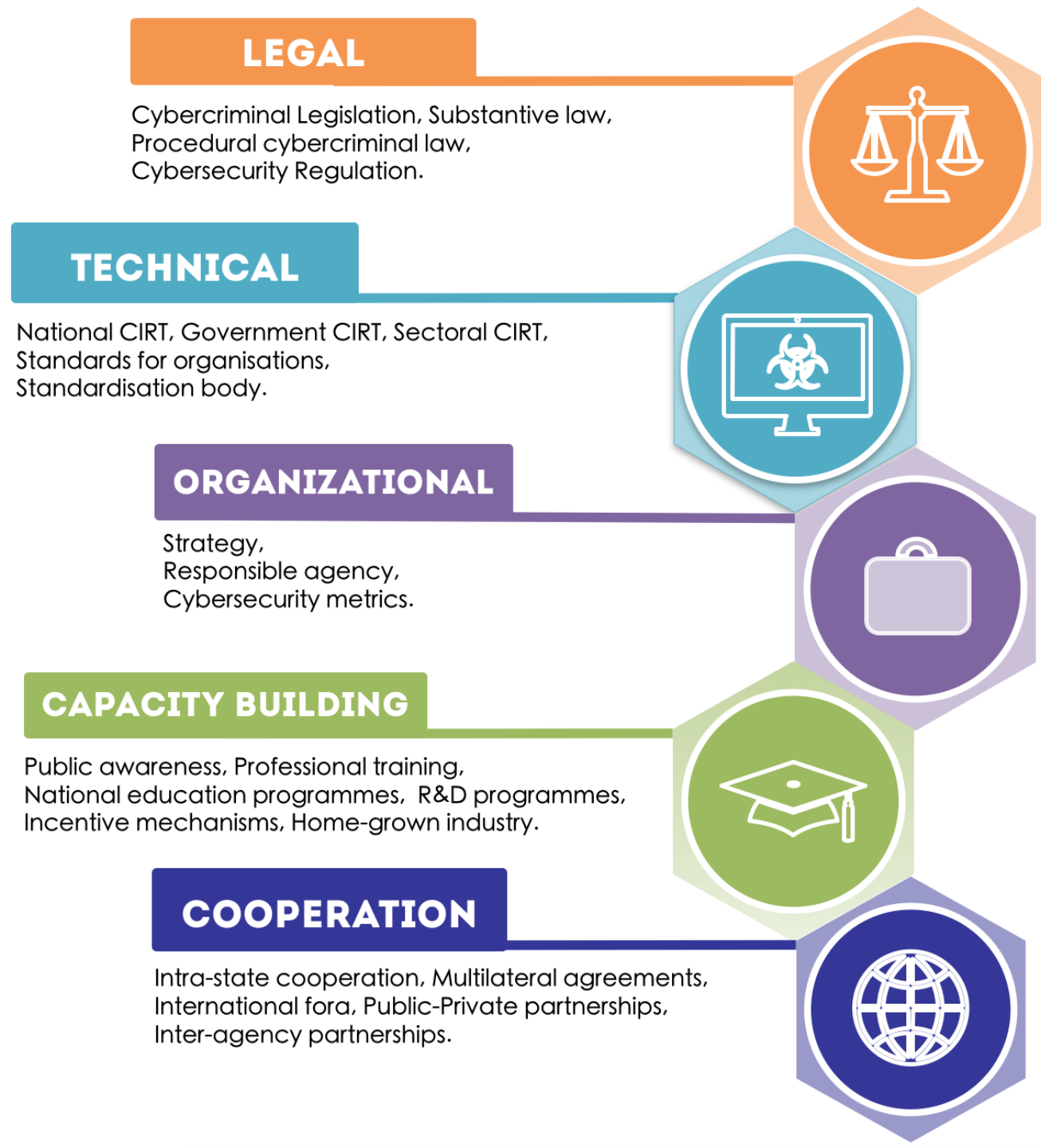
Goals

- 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.





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.

0%

100%

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

Resume later

Exit and clear survey

Question index

1 Respondent Survey

2 Legal Measures

3 Technical Measures

Pages from the online survey.

[token] Token ID

[firstname] First name

[lastname] Last name

[email] Email

[submittedata] Submission date

[id] Completed

[startlanguage] Start language

[startdate] Date started

[datestamp] Date last action

[Q00] Please enter your name

[Q01] Please enter your position

[Q02] Please enter the organization you are representing

[Q1] Is there any cyber related legislation?

[Q11] Please provide links to document if available.

[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)

[Q11] Is there any cybercriminal law?

[Q11] Please provide links to document if available.

[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)

[Q111] Are there any substantive cybercriminal law

[Q111] Please provide links to document if available.

[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)

any articles on the unauthorized access of computers, systems and data?

[Q1111] Please provide links to document if available.

[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)

unauthorized interference / modification of computers, systems and data?

[Q1112] Please provide links to document if available.

[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)

articles on the unauthorized interception of computers, systems and data?

[Q1113] Please provide links to document if available.

[Q1113F(name)] File 1 - Please upload document if available, (File name)

[Q1113F(size)] File 1 - Please upload document if available, (File size)

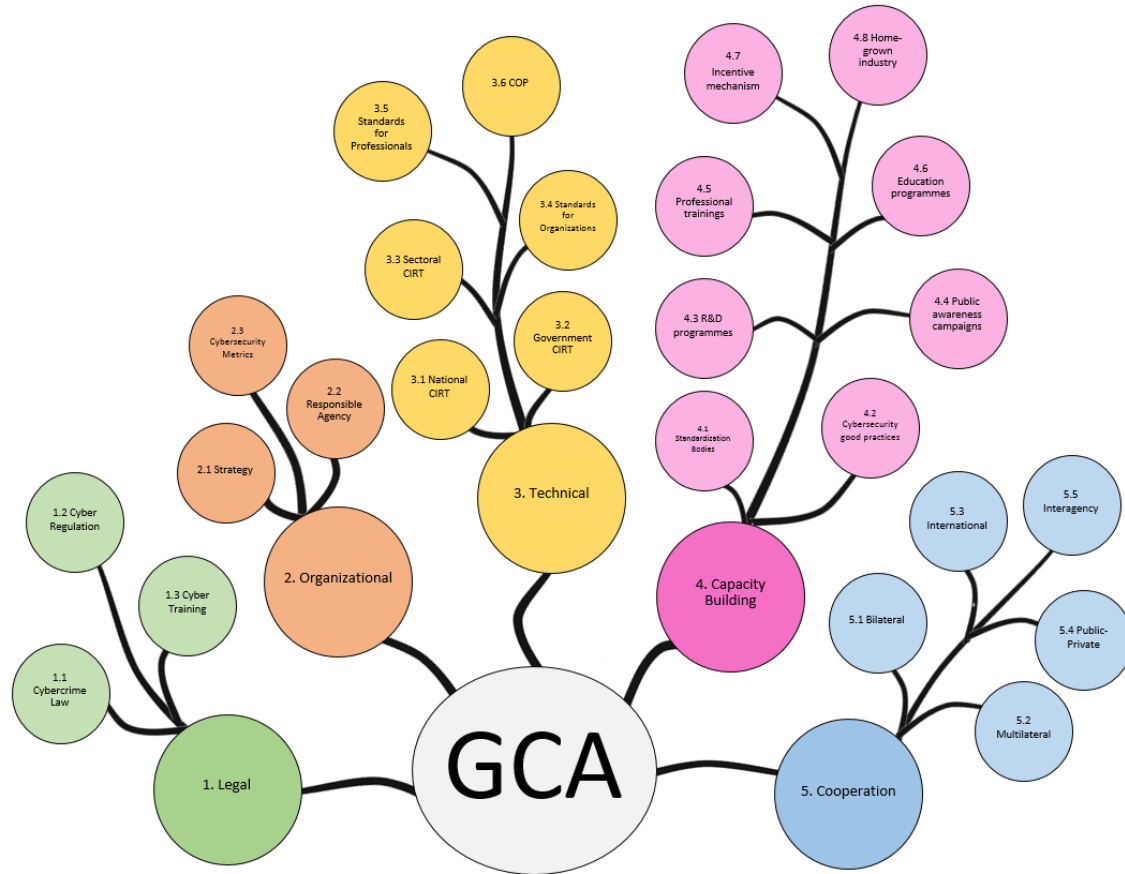
[Q1113F(name)] File 2 - Please upload document if available, (File name)

[Q1113F(size)] File 2 - Please upload document if available, (File size)

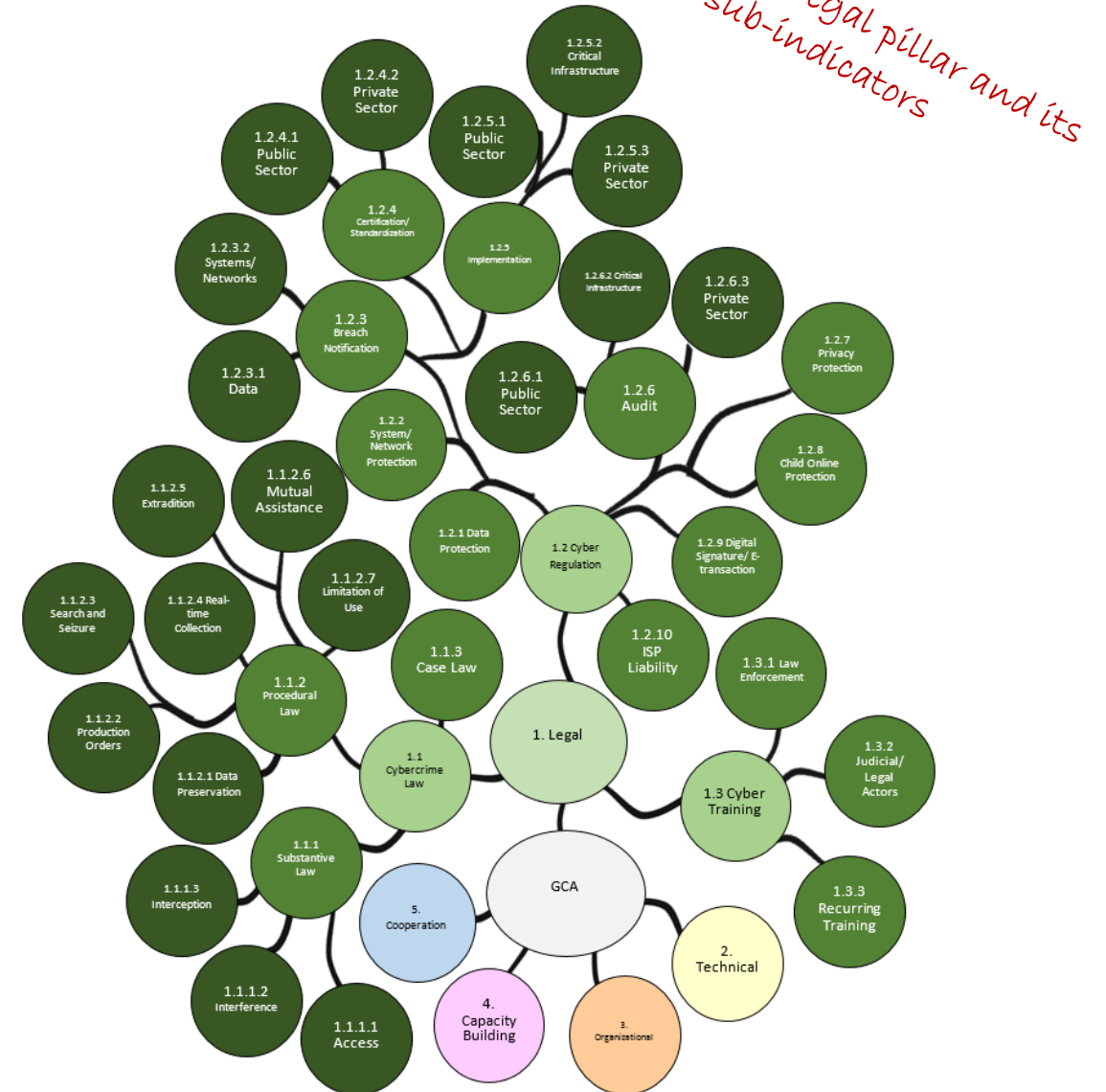
[Q1113F(name)] File 3 - Please upload document if available, (File name)

[Q1113F(size)] File 3 - Please upload document if available, (File size)

GCI and GCA correlation

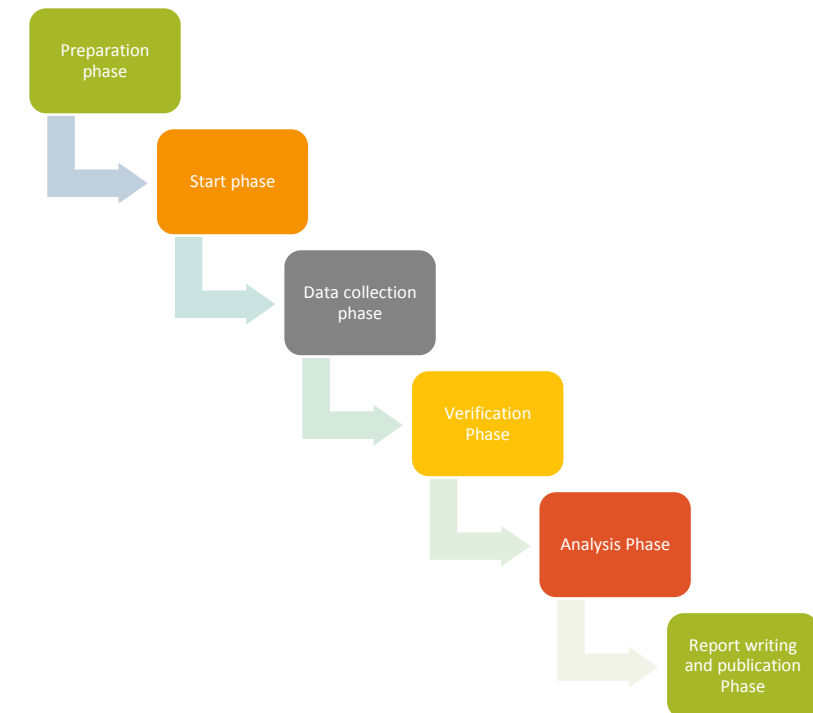


□



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 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!**

JOIN US

- As a partner
 - Add to this body of knowledge under construction
 - Your expertise on thematic to help enhance the GCI process and deliverables
 - Connect better with ITU and Member States
- As a respondent to questionnaire
 - Reflect your Country's achievements and plans for enhancing Cybersecurity
 - Share best practices
 - Position your country on the cybersecurity commitment scale

Media Uptake on GCI

GCI Media

YOU ARE HERE [HOME](#) > [ITU-D](#) > [CYBERSECURITY](#) > [GCI MEDIA](#)

SHARE [f](#) [t](#) [in](#) [L](#)

About

National Strategies

Legal Measures

CIRT Programme

Global Cybersecurity Index

Combating SPAM

Global Partnerships

Cyberthreat Insight

Publications

Events

GCI 2017

- What Can We Learn From the 'Global State of Information Security Survey 2018'?
- The state of PH cybersecurity
- Global Cybersecurity Index 2017 reveals that 50% of countries have no cybersecurity strategy in place
- India ranks 23rd among 165 nations in cybersecurity index
- ITU Global Cybersecurity Index 2017 shows improvements and strengthening of global cybersecurity agenda
- Singapore tops ITU's Global Cybersecurity Index 2017
- Rwanda, Mauritius top Africa in 2017 global cyber security index
- Netherlands Ranks Top-15 in ITU Global Cyber Security Index 2017
- UN cyber security index 2017: At 23rd, India ahead of Germany, China, but Singapore on top
- U.N. survey finds cybersecurity gaps everywhere except Singapore
- VN falls in world cyber security index
- How CyberSecurity Malaysia industry certification helped win 3rd place ranking: Global CyberSecurity Index 2017
- Thailand ranks 20th in global cybersecurity ranking

GCI 2014

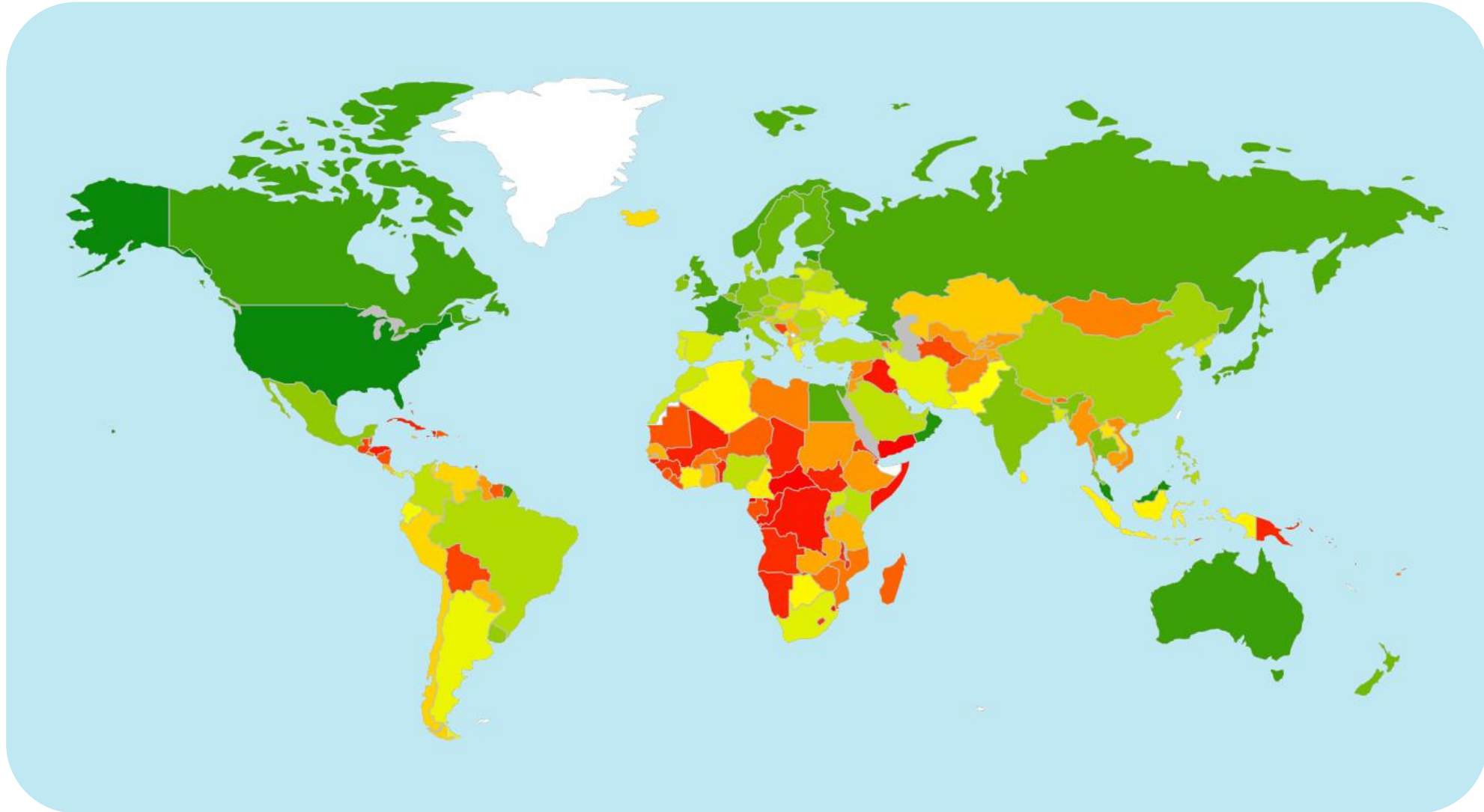
- Canada ranks 2nd in the Global Cybersecurity Index (GCI)
- How do you work out a country's level of cybersecurity?
- Measuring the Information Society Report 2015, Chapter 1
- Cybersecurity Indexes in Cybersecurity Experts Blog at National Cybersecurity Institute
- UK ranks fifth in global cyber security rankings
- Oman third best prepared in world to thwart cyber attacks
- Malaysia ranks third in Global Cybersecurity Index
- Estonia ranks fifth in the global cybersecurity index
- United Nations Launches Global Cybersecurity Index
- US has greatest commitment to cybersecurity, global index reveals
- Egypt Ranked Ninth at Global Cybersecurity Index
- ITU starts Global Cybersecurity Index
- Latvia Takes 7th Place in Global Cyber Security Index
- Uruguay es el segundo país de América Latina y octavo del mundo en seguridad informática (Spanish only)
- Top countries best prepared against cyberattacks
- Η Νορβηγία, η πιο "ετοιμοπόλεμη" ευρωπαϊκή χώρα στην αντιμετώπιση ψηφιακών απειλών (Greek only)





Results

GCIv2 World Heat Map



Commitment levels

High

Medium

Low

GCIv2 results

2017 GCI Participants

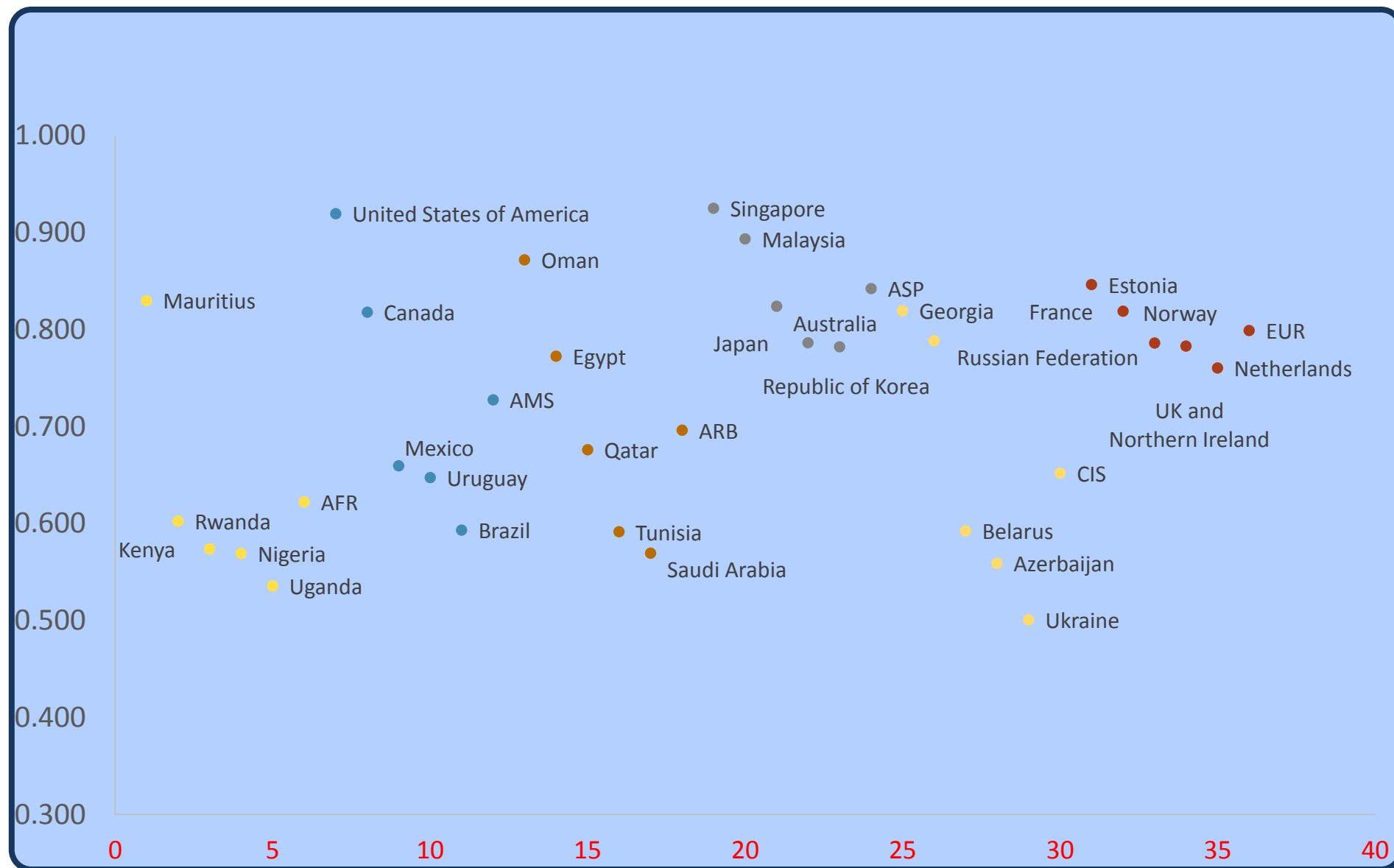
Region	AFR	AMS	ARB	ASP	CIS	EUR	GLO
Responses	29	23	16	25	7	34	134
Non responses	15	12	5	13	5	9	59
Total of participants	44	35	21	38	12	43	193

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

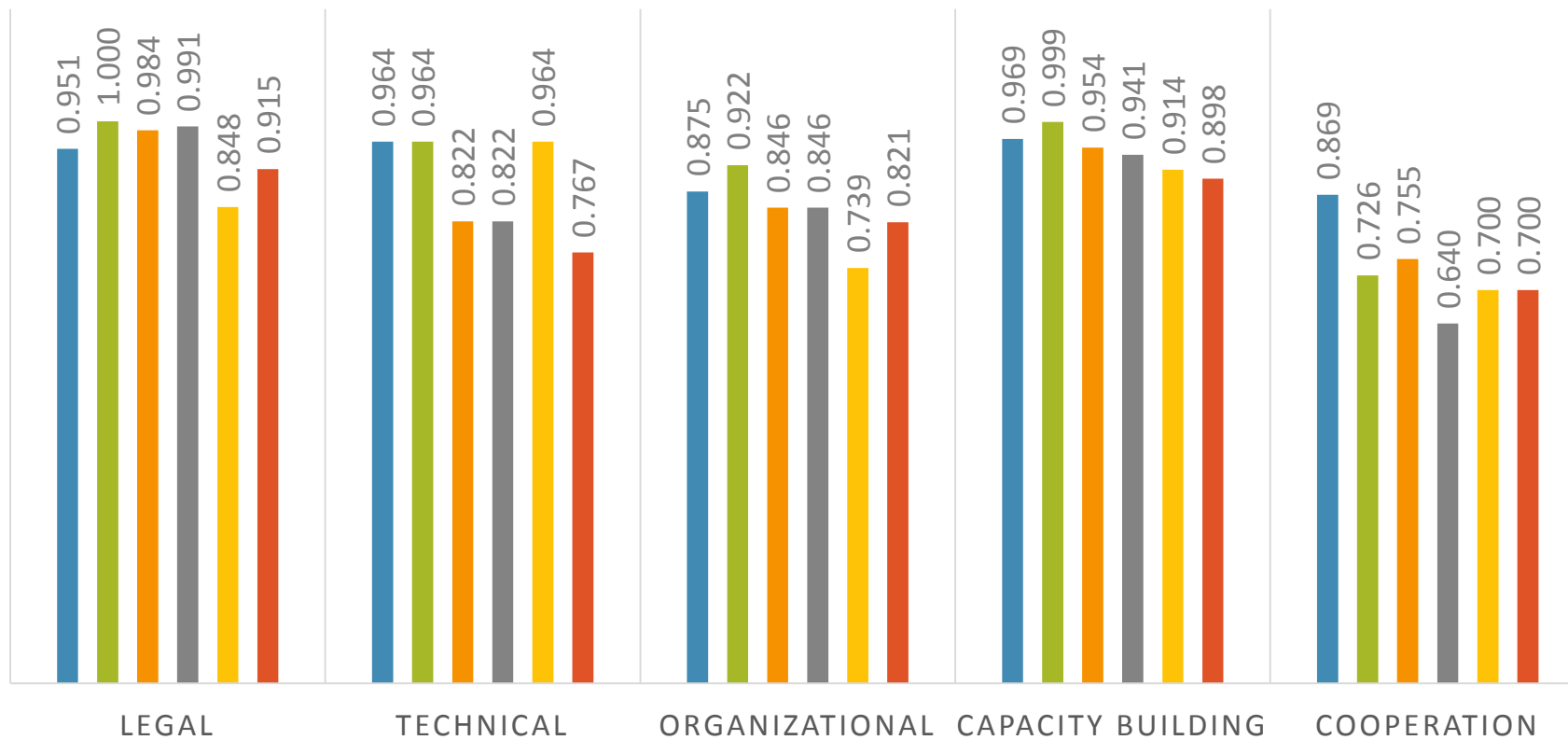
Country	Index	Global Rank
United States of America	0.824	1
Canada	0.794	2
Australia	0.765	3
Malaysia	0.765	3
Oman	0.765	3
New Zealand	0.735	4
Norway	0.735	4
Brazil	0.706	5
Estonia	0.706	5
Germany	0.706	5
India	0.706	5
Japan	0.706	5
Republic of Korea	0.706	5
United Kingdom	0.706	5

134 responses

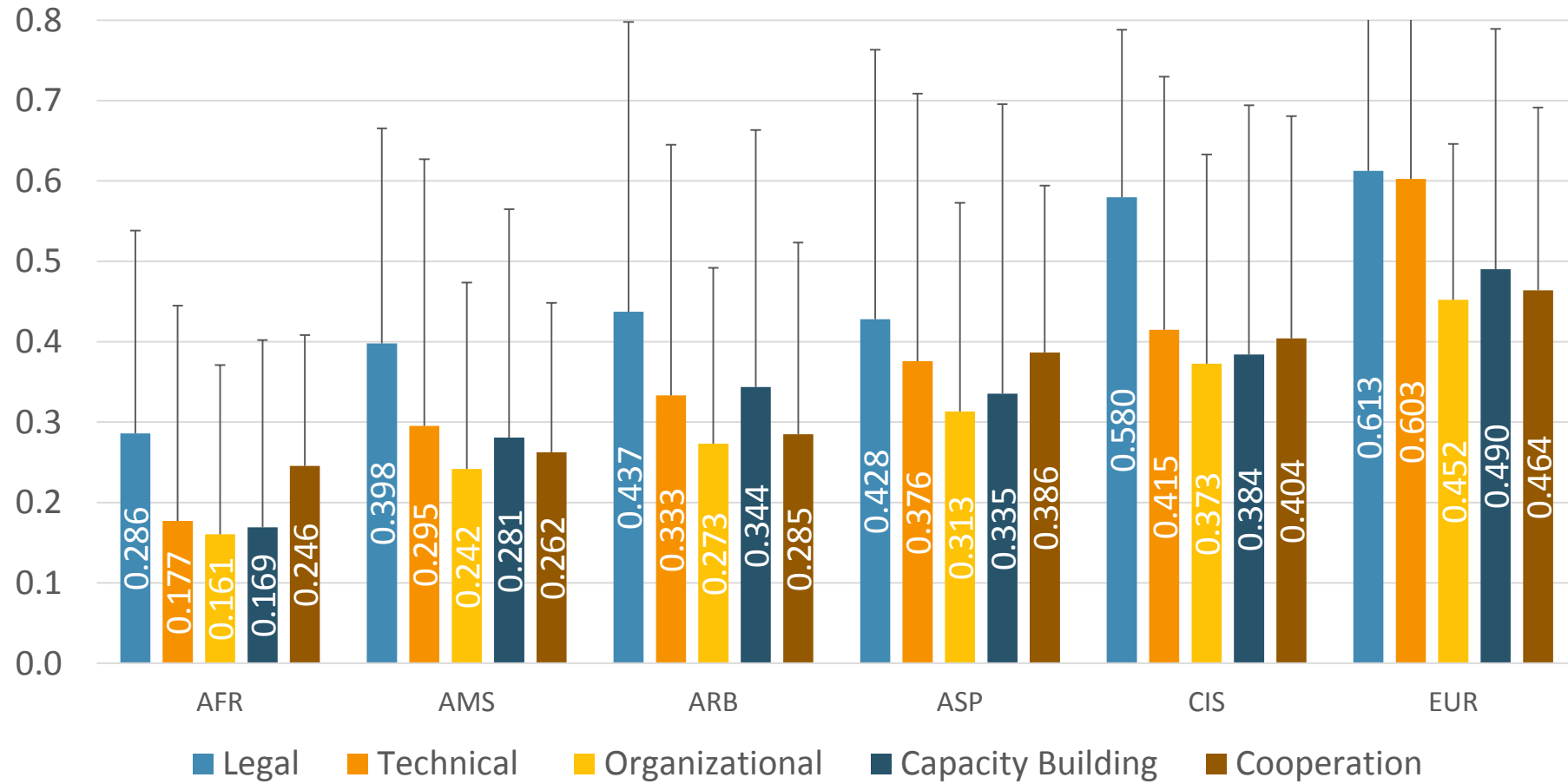
Country	Index	Global ranking
Singapore	0.92	1
United States	0.91	2
Malaysia	0.89	3
Oman	0.87	4
Estonia	0.84	5
Mauritius	0.82	6
Australia	0.82	7
Georgia	0.81	8
France	0.81	8
Canada	0.81	9
Russian Federation	0.78	10

TOP 5 ITU MEMBERS: BEST COMMITMENT BY PILLARS

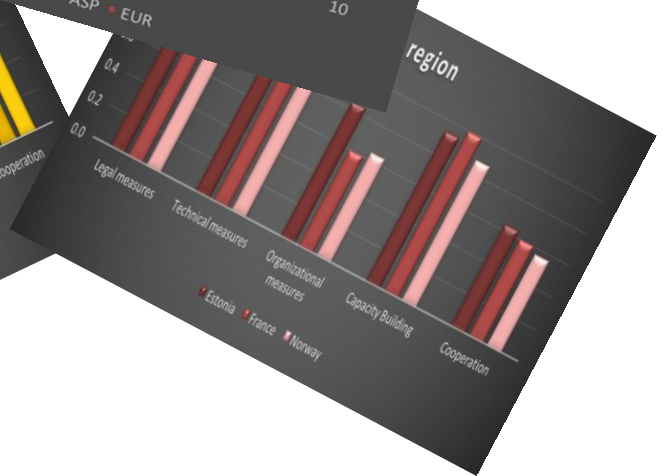
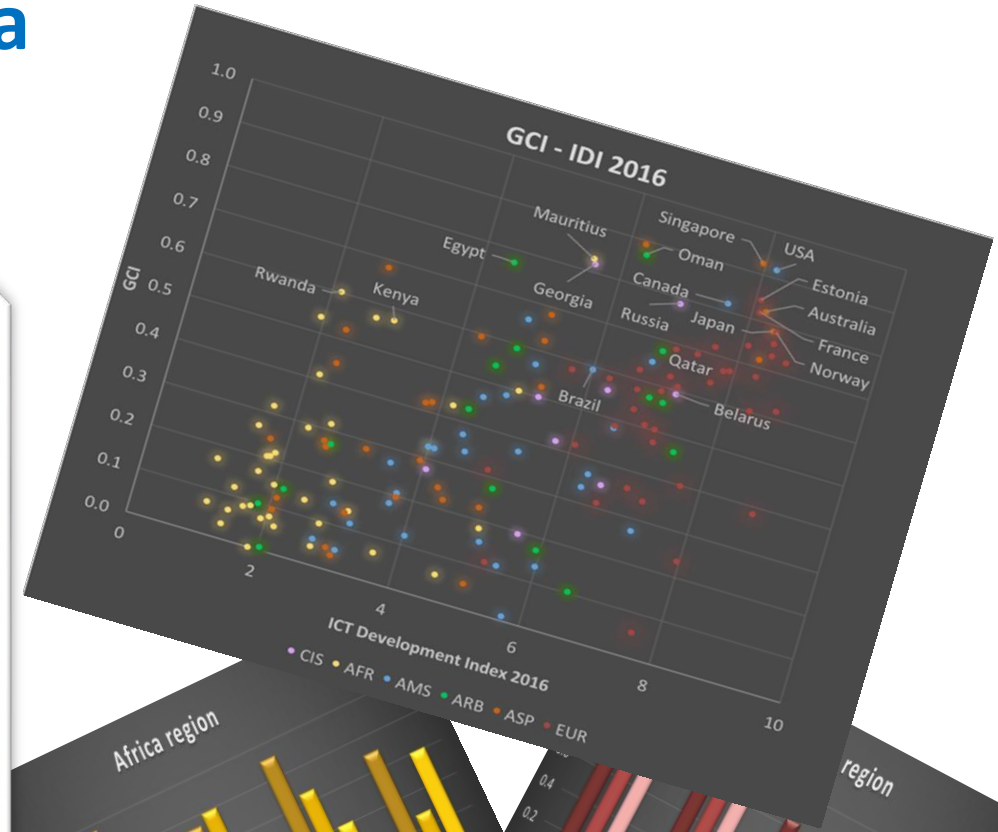
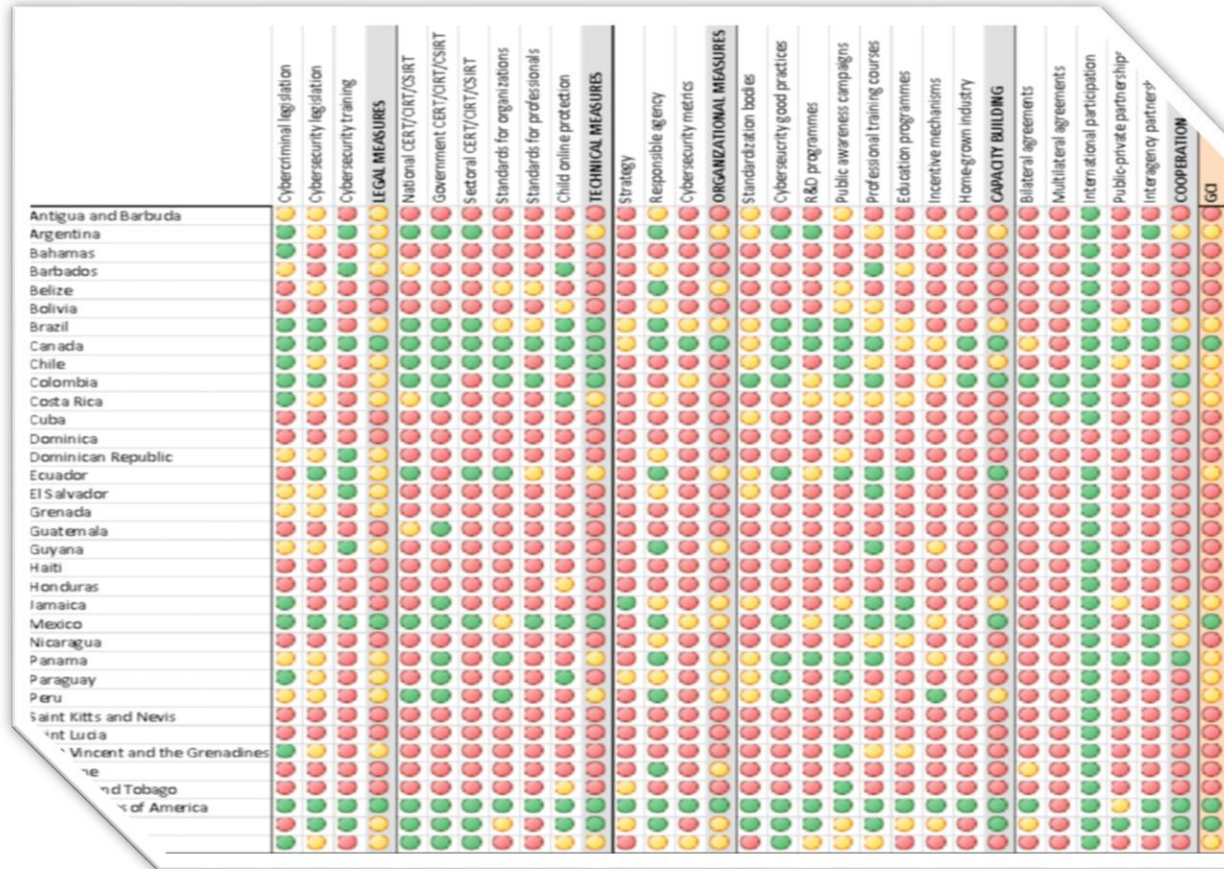
■ Singapore ■ USA ■ Oman ■ Estonia ■ Mauritius ■ Georgia



Global pillars' average by region



GCIv2 presentation of data



Presentation of data

Reports (including regional reports)
and Cyberwellness Profiles



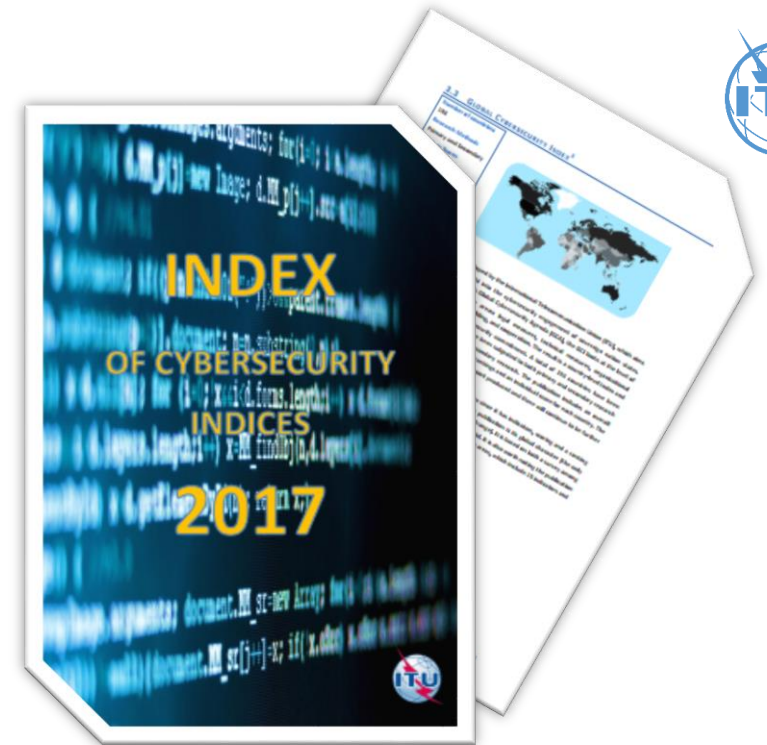
Factual information on cybersecurity
achievements on each country **based**
on the GCA pillars over 194 profiles
to date



Index of Indices



	Metrics						Content								Presentation Format				
	Score	Ranking	Information Society Development Score (ISD) score)	Cyber Maturity	Cyber Threats	Cyber Vulnerabilities	Organizational	Technical	Economical	Legal Framework	Cooperation	Capacity Building	Recommendations	Profiles	Website	PDF	Visualization	No. of Iterations	
Cyber Maturity in the Asia-Pacific Region	x			x					x	x	x			x	x	x		2	
National Cyber Security Index	x	x	x	x	x		x	x		x	x	x			x	x	x	1	
Global Cybersecurity Index	x	x					x	x		x	x	x		x	x	x	x	2	
Kaspersky Cybersecurity Index	x				x				x					x	x	x	x	1	
Asia-Pacific Cybersecurity Dashboard		x		x			x			x	x	x		x	x	x		2	
Cyber Readiness Index 2.0	x	x		x		x	x		x	x	x			x	x	x		2	
Cybersecurity Poverty Index	x			x			x	x							x		x	1	
CyberGreen Index	x	x			x			x							x		x	1	
The Accenture Security Index	x	x			x		x	x	x		x		x		x	x	x	1	
Global Cybersecurity Assurance Report Cards	x				x	x		x							x		x	1	
Index of Cybersecurity					x			x							x	x	x	73	
Cybersecurity Capability Maturity Model				x			x	x		x	x	x			x	x		2	
Cyber Power Index	x	x		x			x	x		x		x			x	x	x	1	
IBM X-force Threat Intelligence Index					x			x							x			3	



Index of Indices from different organizations and companies using different indicators is also compiled

GCI v2 Partners



More information



GCI Website :

<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>

Mr. Maxim kushtuev

maxim.kushtuev@itu.int

For technical support and special requests on GCI

Thank you!

cybersecurity@itu.int