ITU-D

Global Cybersecurity Index (GCI) 2017

Global Cybersecurity Index 2017

Acknowledgments

This report has been produced by the International Telecommunication Union (ITU) with the support of Michael Minges. The Cybersecurity Team of the ITU would like to express its appreciation to Dr. Sherif Hashem (NTRA Egypt), Michaela Saisanna and Hedvig Norlen (Joint Research Centre of the European Commission) as well as the Rapporteurs of the Study Group 2 Question 3 Rozalin Al-Balushi (Oman) and Eliot Lear (USA) for their input to the Global Cybersecurity Index (GCI) work and report.

The online questionnaire preparation, secondary data collection, data validation and report elaboration have been carried out with the support of Mohaamed Ahmed Yousef Aly, Ahmed Abd Allah Abd El- Latif, Tymoteusz Kurpeta, Benjamin Lim, Daniela Toma, Grace Rachael Acayo, and Lena Lattion.

If you have any comments, please contact the ITU Cybersecurity Team: cybersecurity@itu.int

ISBN

978-92-61-25061-4 (paper version)

978-92-61-25071-3 (electronic version)

978-92-61-25081-2 (EPUB version)

978-92-61-25091-1 (Mobi version)

Please consider the environment before printing this report.

Foreword

The global community is increasingly embracing ICTs as key enabler for social and economic development. Governments across the world recognize that digital transformation has the power to further the prosperity and wellbeing of their citizens. In supporting this transformation, they also recognize that cybersecurity must be an integral and indivisible part of technological progress.

In 2016, nearly one percent of all emails sent were essentially malicious attacks, the highest rate in recent years. Ransomware attacks increasingly affected businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. Attackers are demanding more and more from victims, with the average ransom demand rising to over 1,000 USD in 2016, up from approximately 300 USD a year earlier. In May 2017, a massive cyberattack caused major disruptions to companies and hospitals in over 150 countries, prompting a call for greater cooperation around the world.

First launched in 2014, the goal of the Global Cybersecurity Index (GCI) is to help foster a global culture of cybersecurity and its integration at the core of ICTs. This second iteration of the GCI measures the commitment of ITU Member States towards cybersecurity in order to drive further efforts in the adoption and integration of cybersecurity on a global scale.

The GCI reaffirms ITU's commitment to build confidence and security in the use of ICTs. This report on the second iteration of the GCI continues to show the cybersecurity commitment of ITU Member States around the world, and I am pleased to note that the overall picture shows improvement and strengthening of the global cybersecurity agenda.

I wish to thank Member States for their contribution to this effort.

The collection of information for the GCI is an ongoing process, and I therefore invite all ITU Member States to continue sending and updating information on their cybersecurity efforts so that we can effectively share experiences, views and solutions in order to make the digital world a more secure and safe environment for all citizens.

Brahima Sanou

Director, Telecommunication Development Bureau

Executive Summary

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

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.

One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results reported herein cover all 193 ITU Member States.

The 2017 publication of the GCI continues to show the commitment to cybersecurity of countries around the world. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions. However, there is space for further improvement in cooperation at all levels, capacity building and organizational measures. As well, the gap in the level of cybersecurity engagement between different regions is still present and visible. The level of development of the different pillars varies from country to country in the regions, and while commitment in Europe remains very high in the legal and technical fields in particular, the challenging situation in the Africa and Americas regions shows the need for continued engagement and support.

In addition to providing the GCI score, this report also provides a set of illustrative practices that give insight into the achievements of certain countries.

Table of Contents

List of Tables, Figures and Boxes

Tables

Figures

1 Introduction

The information and communication technologies (ICT) networks, devices and services are increasingly critical for day-to-day life. In 2016, almost half the world used the Internet (3.5 billion users)[1] and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020[2]. Yet, just as in the real world, the cyber world is exposed to a variety of security threats that can cause immense damage.

Statistics on threats to computer networks are sobering and reflect a shift from the relatively innocuous spam of yesteryear to threats that are more malicious. A security company tracking incidents in 2016 found that malicious emails became a weapon of choice for a wide range of cyberattacks during the year used by everyone from state sponsored cyber espionage groups to mass-mailing ransomware gangs. One-in-131 emails sent were malicious, the highest rate in five years.

Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. In some cases, organizations can be overwhelmed by the sheer volume of ransomware-laden emails they receive. Attackers are demanding more and more from victims with the average ransom demand in 2016 rising to USD 1 077, up from USD 294 a year earlier[3]. The scale of cybercrime makes it critical for governments to have a robust cybersecurity ecosystem in place to reduce threats and enhance confidence in using electronic communications and services.

It is therefore clear that there is a direct cause-effect principle between the growth of ICTs and their illicit and malicious use. To counter this effect, cybersecurity is becoming more and more relevant in the minds of countries' decision makers, and cybersecurity related doctrines have been established in almost all countries in the world.

However, there is still an evident gap between countries in terms of awareness, understanding, knowledge and finally capacity to deploy the proper strategies, capabilities and programmes to ensure a safe and appropriate use of ICTs as enablers for economic development.

In this context, ITU, together with international partners from private-public and private sector as well as academia, has established the GCI with the key objective of building capacity at the national, regional and international level, through assessing the level of engagement of countries on cybersecurity, and, with the data gathered, producing a list of good practices that can be used by countries in need.

[1] www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2] www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

[3] www.symantec.com

2 GCI Scope and Framework

2.1 Background

The GCI is included under Resolution 130 (Rev. Busan, 2014) on strengthening the role of ITU in building confidence and security in the use of ICT. Specifically, Member States are invited "to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors".

A first iteration of the GCI was conducted in 2013-2014 in partnership with ABI Research[1], and the final results have been published[2].

Following feedback received from various communities, a second iteration of the GCI was planned and undertaken. This new version was formulated around an extended participation from Member States, experts and industry stakeholders as contributing partners (namely World Bank and Red Team Cyber as new GCI partners joining the Australia Strategic Policy Institute, FIRST, Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet & Security Agency, NTRA Egypt, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica and UNODC) who all provided support with the provision of secondary data, response activation, statistical analysis, qualitative appreciation amongst other.

The data collected via GCI 2017 for ITU-D Study Group 2 Question 3 (SG2Q3) surveys have been analysed by the Rapporteur and co-Rapporteur for inclusion in the SG2Q3 final report. GCI partners have been active in providing expertise and secondary data as appropriate, while the UN office of ICT (New York) has also initiated collaborative work. ITU is also working in a multi-stakeholder collaboration led by the World Bank to elaborate a toolkit on "Best practice in Policy/Legal enabling Framework and Capacity Building in Combatting Cybercrime". ITU is providing support on the component on capacity building from a cybersecurity perspective based on GCI 2017 data.

An enhanced reference model was thereby devised. Throughout the steps of this new version, Member States were consulted using various vehicles including ITU-D Study Group 2 Question 3/2, where the overall project was submitted, discussed and validated.

2.2 Reference model

The 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 Group and endorsed by the GCA. These pillars form the five pillars of GCI.

The main objectives of the GCI are to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- the progress in cybersecurity commitment of all countries from a global perspective;
- the progress in cybersecurity commitment from a regional perspective;
- the cybersecurity commitment divide, i.e. the difference between countries in terms of their level of engagement in cybersecurity programmes and initiatives.

[1] https://www.abiresearch.com/

[2] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx

The objective of the GCI as an initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of commitment to cybersecurity worldwide.

Through the information collected, the GCI aims to illustrate the practices of other countries so that Member States can implement selected aspects suitable to their national environment, with the added benefits of helping harmonize practices and fostering, a global culture of cybersecurity.

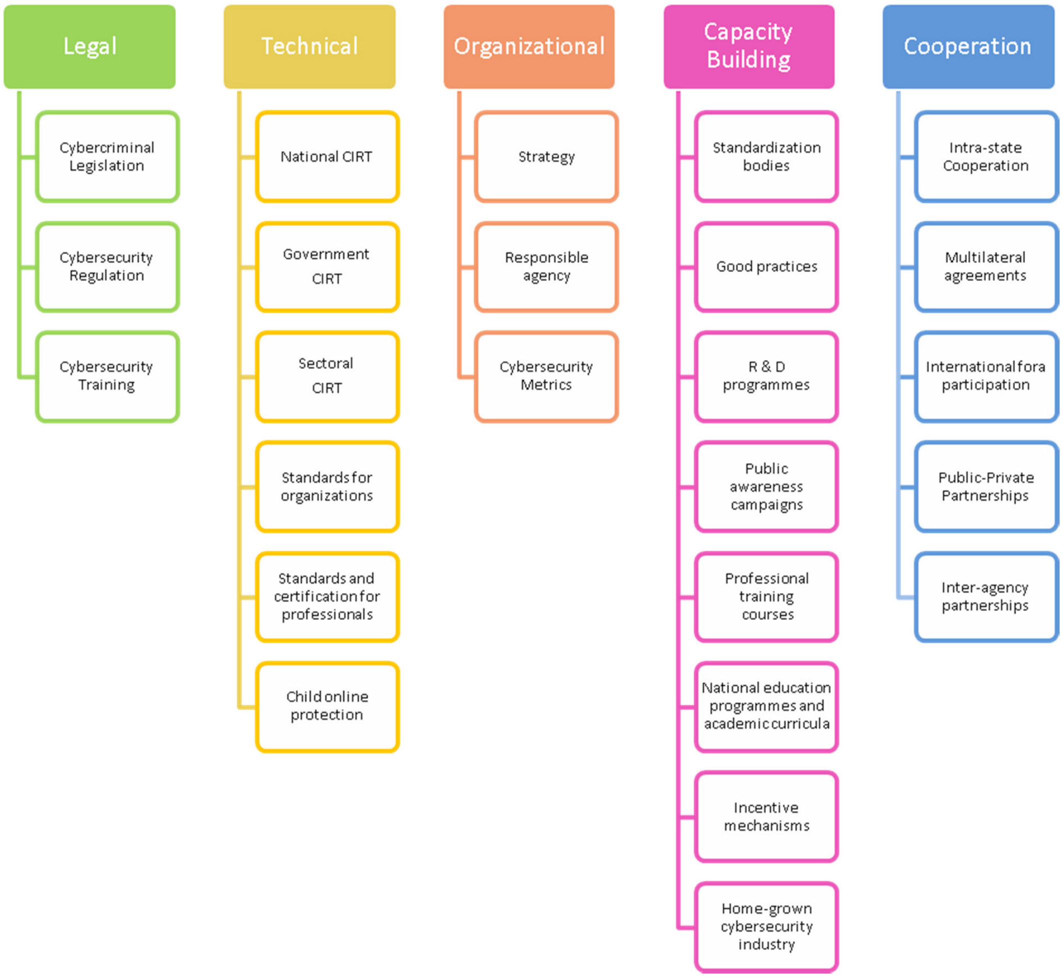
2.3 Conceptual framework

The five pillars of the GCI are briefly explained below:

1. **Legal:** Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. **Technical:** Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.
3. **Organizational:** Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
4. **Capacity Building:** Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.
5. **Cooperation:** Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Each pillar was then further divided in sub-pillars (Figure 2.3.1).

Figure 2.3.1: GCI pillars and sub-pillars



The questionnaire was elaborated on the basis of these sub-pillars[3]. The values for the 25 indicators were therefore constructed through 157 binary questions. This was done in order to achieve the required level of granularity and ensure accuracy and quality on the answers.

[3] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf

Figure 2.3.2 below represents all the five pillars from GCA with their indicators.

Figure 2.3.2: GCA tree structure illustrating all pillars (simplified)

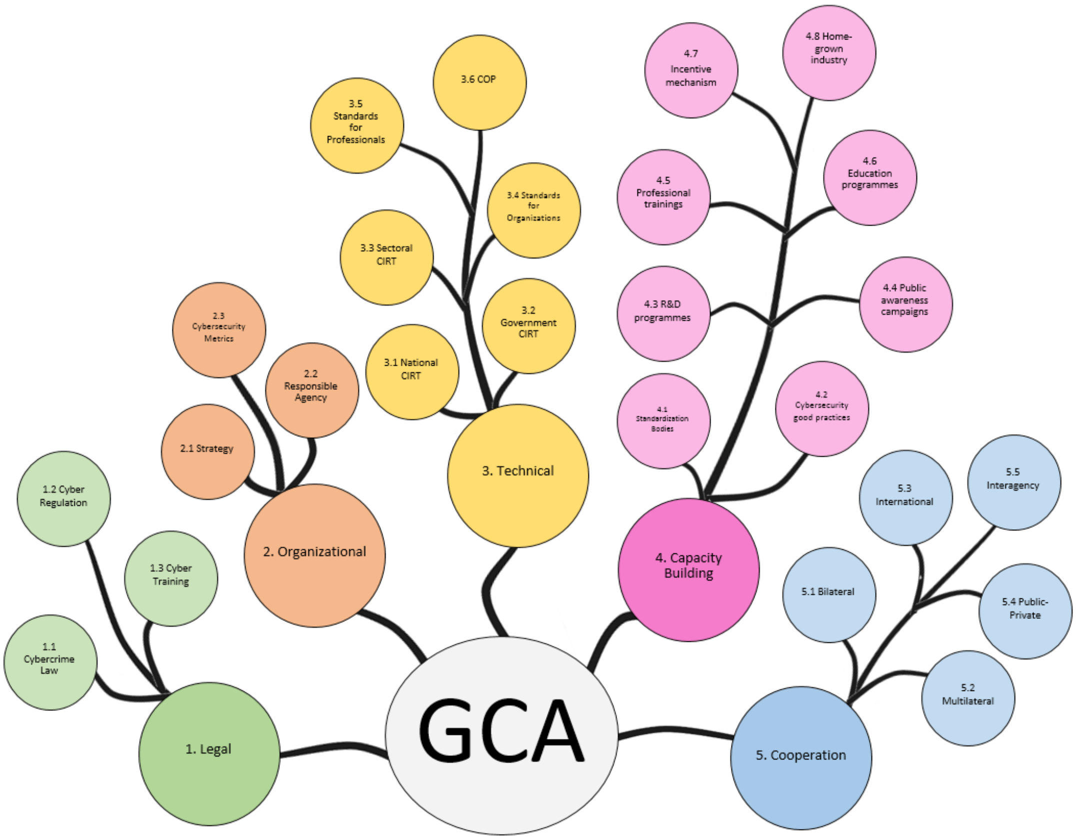
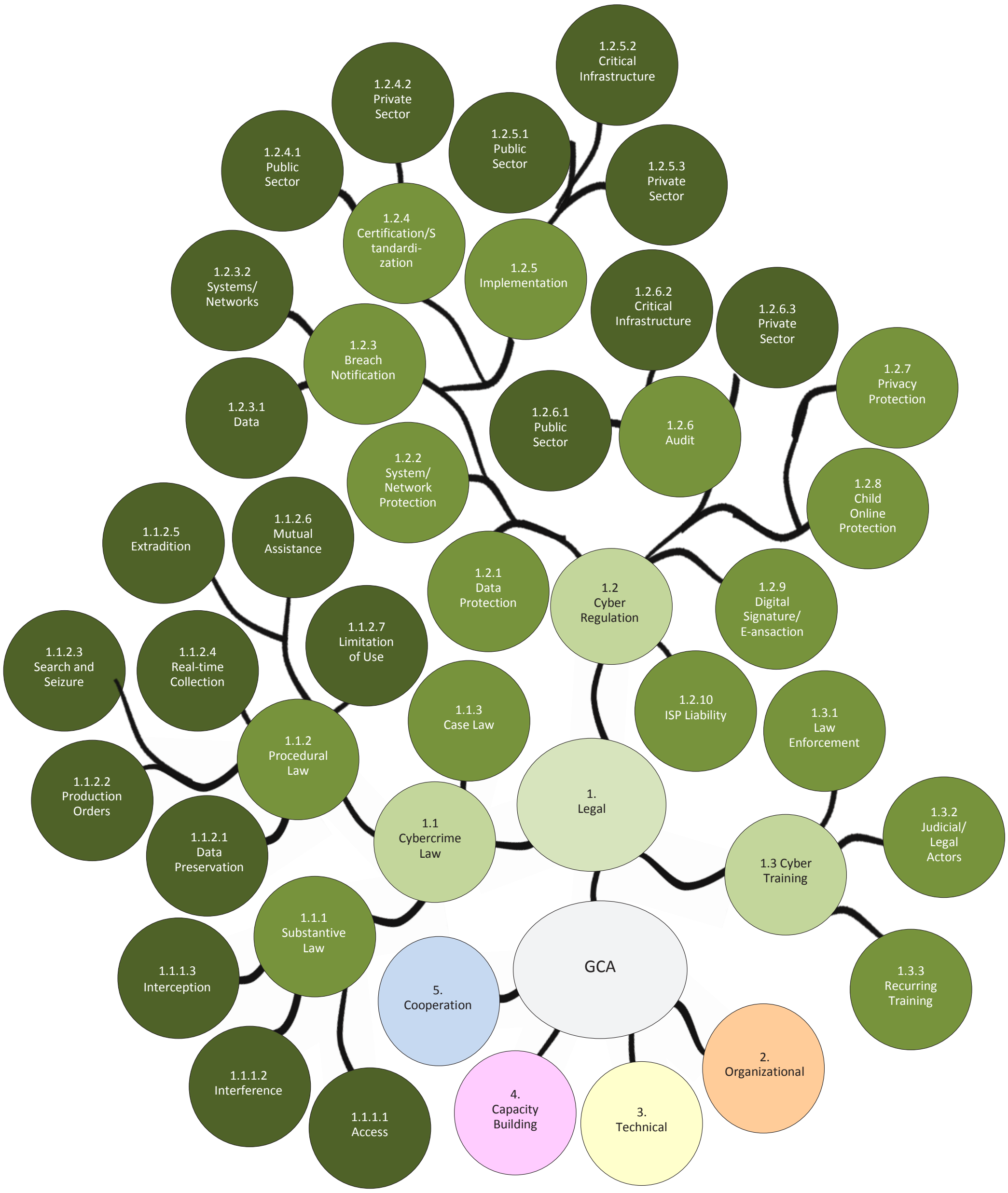


Figure 2.3.3 below illustrates the relationship between the GCA, the pillars, sub-pillars and questions (expanded only for the legal pillar due to space considerations).

Figure 2.3.3: GCI tree structure illustrating Legal pillar



3 Methodology

The GCI includes 25 indicators and 157 questions. The indicators used to calculate the GCI were selected on the basis of the following criteria:

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

The whole concept of a new iteration of the GCI is based on a cybersecurity development tree map and binary answer possibilities.

The tree map concept, which is illustrated in Figures 2.3.2 and 2.3.3, is an example of different possible paths that might be taken by countries in order to enhance their cybersecurity commitment.

Each of the five pillars are associated with a specific colour. The deeper the path taken, indicating a more developed level of commitment, the deeper the colour depicting it becomes.

The various levels of cybersecurity development among countries, as well as the different cybersecurity needs reflected by a country’s overall ICT development status, were taken into consideration. The concept is based on the assumption that the more developed cybersecurity is, the more complex the solutions observed will be. Therefore, the further a country goes along the tree map by confirming the presence of pre-identified cyber solutions, the more complex and sophisticated the cybersecurity commitment is within that country, allowing it to obtain a higher score with the GCI.

The rationale behind using binary answer possibilities is the elimination of opinion-based evaluation and of any possible bias towards certain types of answers.

Moreover, the simple binary concept will allow quicker and more complex evaluation as it will not require lengthy answers from countries. This, in turn, is assumed to accelerate and streamline the process of providing answers and further evaluation. The idea is that the respondent will only confirm the presence or lack of certain pre-identified cybersecurity solutions. An online survey mechanism, which was used for gathering answers and uploading all relevant materials, enabled the extraction of good practices.

The key difference in methodology between GCI 2014 and GCI Version 2017 is the use of a binary system instead of a three-level system. The binary system evaluates the existence or absence of a specific activity, department or measure. Unlike GCI Version 2014, it does not take 'partial' measures into consideration. The facility for respondents to upload supporting documents and URLs is a way of providing more information to substantiate the binary response. Furthermore, a number of new questions have been added in each of the five pillars in order to refine the depth of research.

The GCI 2014 and GCI 2017 are not directly comparable due to a change in methodology. While the 2014 index used a simple average methodology, the 2017 index employs a weighting factor for each pillar.

The questionnaire, made available through an online survey from January to September 2016, was administered to the 193 ITU Member States (plus State of Palestine) in the regions of Africa, Americas, Arab States, Asia and the Pacific, the Commonwealth of Independent States, and Europe. 134 countries responded to the online survey while 59 countries did not provide primary data.

Table 3.1: Numbers of responses received from all Members States regionally

Region	Africa	Americas	Arab States	Asia and the Pacific	CIS	Europe	Global
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

The data collection process was implemented as follows:

1. A ***Letter of Invitation*** was sent by the ITU Secretariat to all Member States, informing them on the initiative and requesting the identification of a country level GCI focal point with whom ITU could liaise and who would be responsible for collecting all relevant data for completing the online GCI questionnaire. A guideline to the online questionnaire which provided explanations and examples for each question, was attached to the letter[1].
2. ***Primary data collection*** (for countries who responded to the questionnaire):
    - Verification of the responses received by the specific Member State to identify possible missing elements (no or missing responses, no or missing supporting documents, no or missing links, etc.).
        - For instance, if a Member State answered "No", ITU researched to prove that they do not have any documents in the ITU database or online.
        - If a Member State answered "Yes", ITU researched to verify that answers provided were correct and corresponded to the question.
    - The focal point identified by the concerned Member State was contacted and provided with indications on how to improve the accuracy of the responses. Where necessary ITU provided comments and guidance to improve the completed questionnaire.
    - After the necessary rounds of iterations, the pre-final questionnaire was sent back to the concerned Member State for final approval.
    - Once formal approval was received, the questionnaire was considered validated and used for the analysis, scoring and ranking.
3. ***Secondary data collection*** (for countries that did not respond to the questionnaire):
    - ITU elaborated an initial draft of the response to the questionnaire using publicly available data and online research.
    - The draft was then sent to the concerned Member State for review.
    - The reviewed response received, the focal point identified by the concerned Member State was contacted and provided with indications on how to improve the accuracy of the responses. Where necessary ITU provided comments and guidance to improve the completed questionnaire.
    - After the necessary rounds of iterations, the pre-final questionnaire was sent back to the concerned Member State for final approval.

[1] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf

- Once formal approval was received, the questionnaire was considered validated and used for the analysis, scoring and ranking.

The GCI 2017 methodology encompassed the use of a panel of experts, identified according to their specific expertise on the subject, who acted in their personal capacity in order to provide an expert view on the weighting to be used for the scoring.

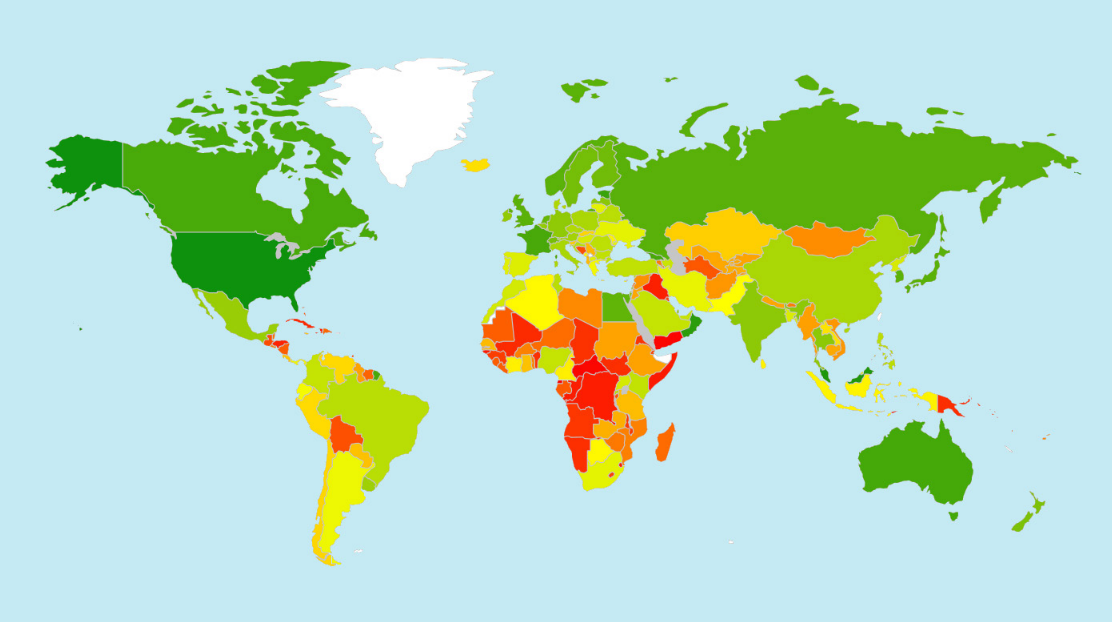
4 Key Findings

4.1 Heat Map of National Cybersecurity Commitments

Out of the 193 Member States, there is a huge range in cybersecurity commitments, as the heat map below illustrates.

Level of commitment: from Green (highest) to Red (lowest)

Figure 4.1.1: GCI Heat Map



4.2 GCI Groups

Member States were classified into three categories by their GCI score (Figure 4.2.1).

- *Initiating stage* refers to the 96 countries (i.e., GCI score less than the 50th percentile) that have started to make commitments in cybersecurity.
- *Maturing stage* refers to the 77 countries (i.e., GCI score between the 50th and 89th percentile) that have developed complex commitments, and engage in cybersecurity programmes and initiatives.
- *Leading stage* refers to the 21 countries (i.e., GCI score in the 90th percentile) that demonstrate high commitment in all five pillars of the index.

Figure 4.2.1: GCI Tiers

INITIATING

- Afghanistan
- Andorra
- Angola
- Antigua and Barbuda
- Armenia
- Bahamas
- Barbados
- Belize
- Benin
- Bhutan
- Bolivia (Plurinational State of)
- Bosnia & Herzegovina
- Burkina Faso
- Burundi
- Cambodia
- Cape Verde
- Central African Republic.
- Chad
- Comoros
- Congo
- Cuba
- Democratic Republic of the Congo
- Djibouti
- Dominica
- Dominican Republic
- El Salvador
- Equatorial Guinea
- Eritrea
- Ethiopia
- Fiji
- Gabon
- Gambia
- Grenada
- Guatemala
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Honduras
- Iraq
- Jordan
- Kiribati
- Kuwait
- Kyrgyzstan
- Lebanon
- Lesotho
- Liberia
- Libya
- Liechtenstein
- Madagascar
- Malawi
- Maldives
- Mali
- Marshall Islands
- Mauritania
- Micronesia
- Monaco
- Mongolia
- Mozambique
- Myanmar
- Namibia
- Nauru
- Nepal (Republic of)
- Nicaragua
- Niger
- Palau
- State of Palestine
- Papua New Guinea
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent & the Grenadines
- Samoa
- San Marino
- Sao Tome and Principe
- Seychelles
- Sierra Leone
- Solomon Islands
- Somalia
- South Sudan
- Sudan
- Suriname
- Swaziland
- Syrian Arab Republic
- Tajikistan
- Timor-Leste
- Togo
- Tonga
- Trinidad and Tobago
- Turkmenistan
- Tuvalu
- Uzbekistan
- Vanuatu
- Vatican
- Viet Nam
- Yemen
- Zambia
- Zimbabwe

MATURING

- Albania
- Algeria
- Argentina
- Austria
- Azerbaijan
- Bahrain
- Bangladesh
- Belarus
- Belgium
- Botswana
- Brazil
- Brunei Darussalam
- Bulgaria
- Cameroon
- Chile
- China
- Colombia
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cyprus
- Czech Republic
- Dem. People's Rep. of Korea
- Denmark
- Ecuador
- Germany
- Ghana
- Greece
- Hungary
- Iceland
- India
- Indonesia
- Iran (Islamic Republic of)
- Ireland
- Israel
- Italy
- Jamaica
- Kazakhstan
- Kenya
- Laos
- Latvia
- Lithuania
- Luxembourg
- Malta
- Mexico
- Moldova
- Montenegro
- Morocco
- Nigeria
- Pakistan
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Qatar
- Romania
- Rwanda
- Saudi Arabia
- Senegal
- Serbia
- Slovakia
- Slovenia
- South Africa
- Spain
- Sri Lanka
- Tanzania
- Thailand
- The Former Yugoslav Rep. of Macedonia
- Tunisia
- Turkey
- Uganda
- Ukraine
- United Arab Emirates
- Uruguay
- Venezuela

LEADING

- Australia
- Canada
- Egypt
- Estonia
- Finland
- France
- Georgia
- Japan
- Korea
- Malaysia
- Mauritius
- Netherlands
- New Zealand
- Norway
- Oman
- Russian Federation
- Singapore
- Sweden
- Switzerland
- United Kingdom
- United States

5 Global Outlook

All of the six ITU regions are represented in the top ten commitment level in the GCI. There are three from Asia and the Pacific, two each from Europe and the Americas, and one from Africa, the Arab States, and the Commonwealth of Independent States.

This suggests that being highly committed is not strictly tied to geographic location.

Table 5.1: Top ten most committed countries, GCI (normalized score)

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

As the GCI shows, there is a wide gulf in cyber preparedness around the globe. This gap exists between and within regions.

Further, cybersecurity related commitments are often unequally distributed with countries performing well in some pillars and less so in others. Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective.

Additionally, cybersecurity is not just a concern of the government but also needs commitment from the private sector and consumers. Thus, it is important to develop a cybersecurity culture where citizens are aware of the trade-off between risks and monitoring when using electronic networks.

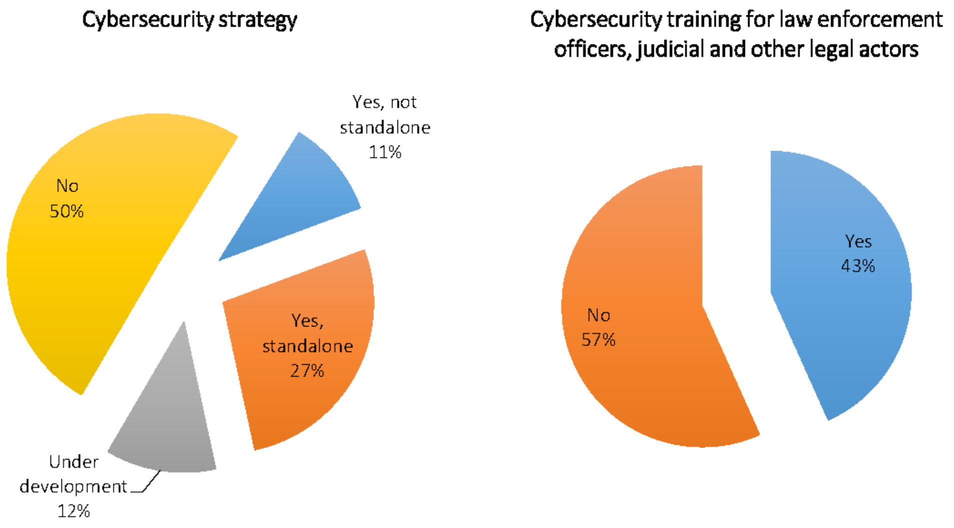
5.1 Noteworthy figures

The GCI consists of 25 different indicators. Some relate to precise commitments that help to concretize the status of specific cybersecurity activities throughout the world.

One of the strongest commitments is to outline a cybersecurity strategy describing how the country will prepare and respond to attacks against its digital networks. Only 38% countries have a published cybersecurity strategy and only 11% have a dedicated standalone strategy (Figure 5.1.1, left); another 12% have a cybersecurity strategy under development.

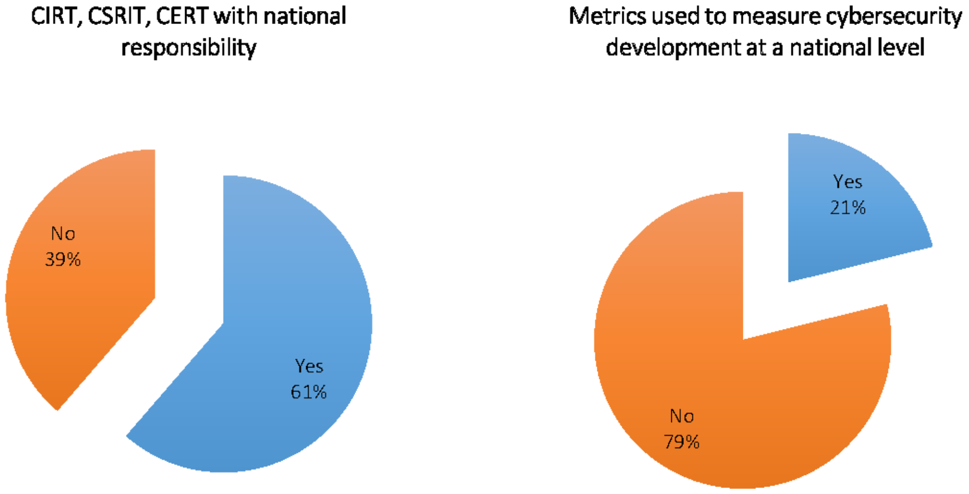
More effort is needed in this critical area, particularly since it conveys that the government considers digital risks high priority. In the area of training, efforts need to be enhanced particularly for those who are most likely going to legally handle cybersecurity crimes given that less than half the Member States (43%) have capacity-building programmes for law enforcement and the judicial system (Figure 5.1.1, right).

Figure 5.1.1: Cybersecurity strategy and training commitments



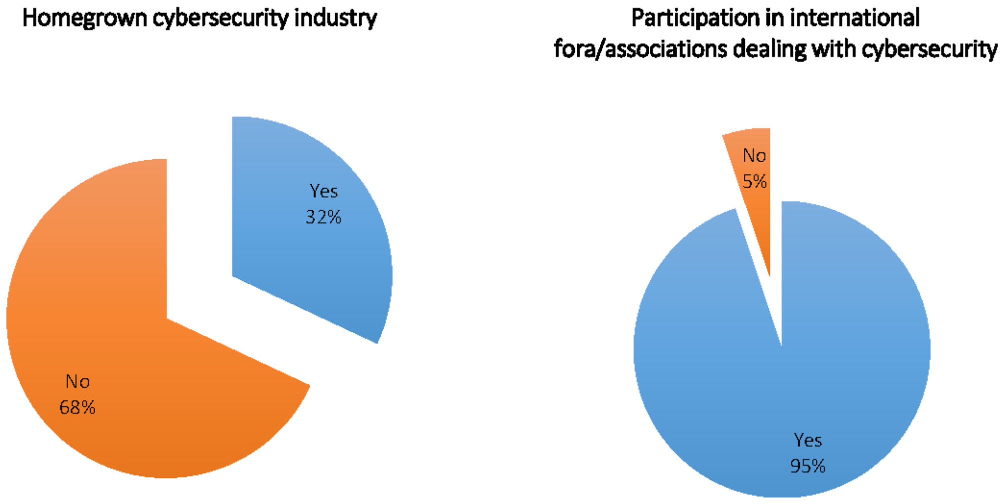
Despite half of the Member States not having a cybersecurity strategy, 61% do have an emergency response team (i.e., CIRT, CSRIT, and CERT) with national responsibility (Figure 5.1.2, left). However, just over a fifth (21%) publish metrics on cybersecurity incidents (Figure 5.1.2, right). This makes it difficult in most countries to objectively assess incidents based on the evidence and determine if protection measures are working.

Figure 5.1.2: Computer emergency response teams and metrics



Just less than a third of countries (32%) replied affirmatively to the existence of a homegrown cybersecurity industry (Figure 5.1.3, left). More efforts need to be devoted to this area as a local industry will have knowledge of national circumstances and make the security ecosystem more sustainable. The potential for global cooperation is heightened by participation in international cybersecurity events. This is almost universal with 95% of countries replying affirmatively (Figure 5.1.3, right).

Figure 5.1.3: Home-grown industry and international participation



5.2 Comparing GCI with other indices

A qualitative comparison has been performed to raise awareness on the importance of investing on cybersecurity, as an integral component of any national ICT for development strategy.

This paragraph is not intended to provide thorough, exhaustive statistical analysis, but rather an indication on how cybersecurity can relate to existing national processes, in order to emphasize the importance of investing and being committed.

Comparing GCI scores to notable ICT for Development Indices does not reveal an especially close relationship as experience shows that countries which score high in term of ICT for Development do not necessarily invest in cybersecurity with the same level of commitment, and vice versa.

For example, comparing the GCI with the ITU ICT for Development Index (IDI), shows that some countries are performing much better in the GCI than their level of ICT development would suggest.

The following figures show the relation between the GCI and IDI with each graph identifying the top three countries for each region.

Figure 5.2.1: Global comparison GCI and IDI

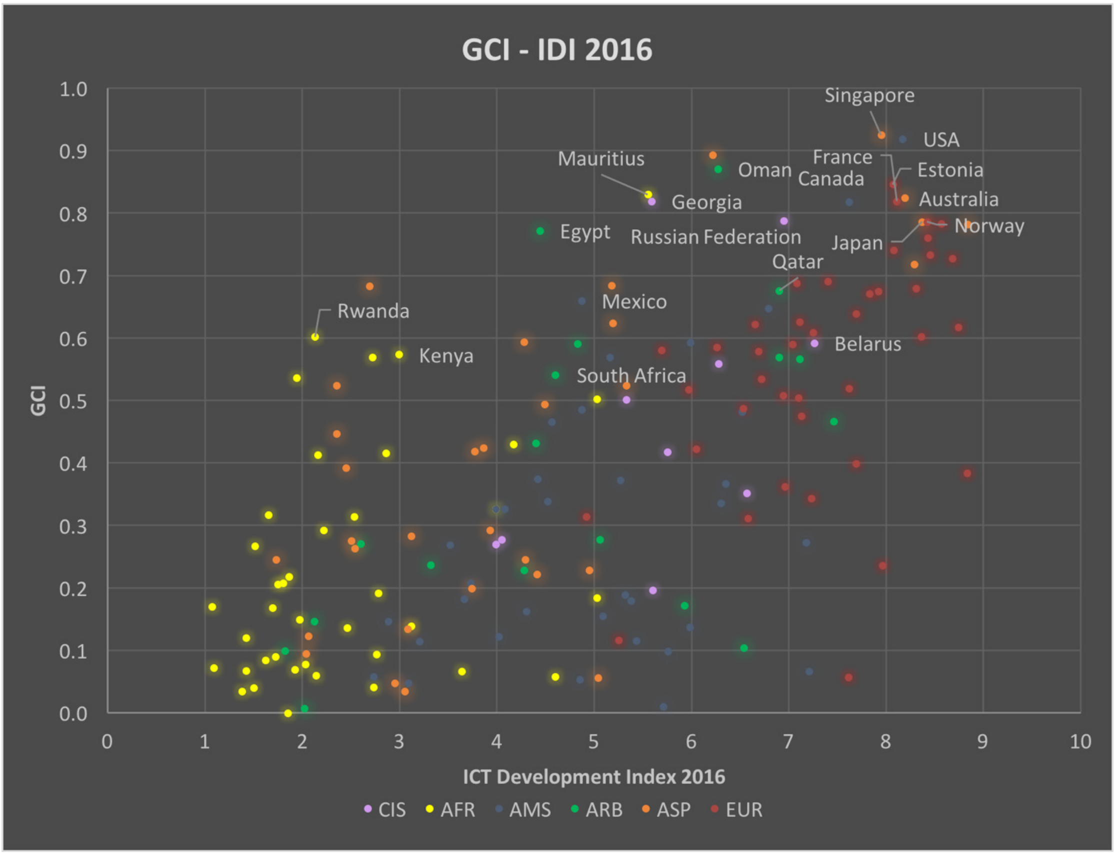


Figure 5.2.2: Comparison GCI and IDI in the Africa region

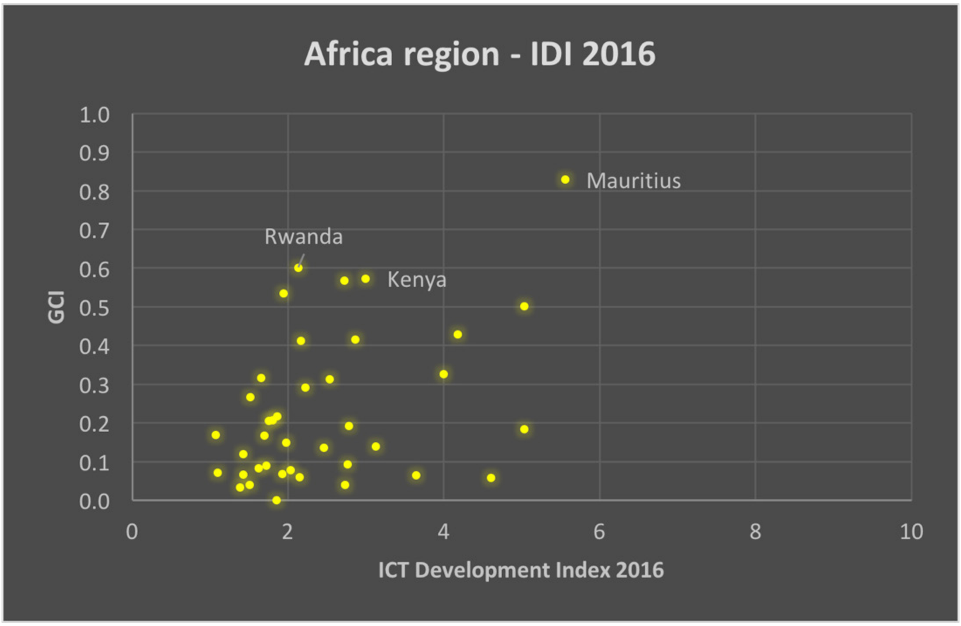


Figure 5.2.3: Comparison GCI and IDI in the Americas region

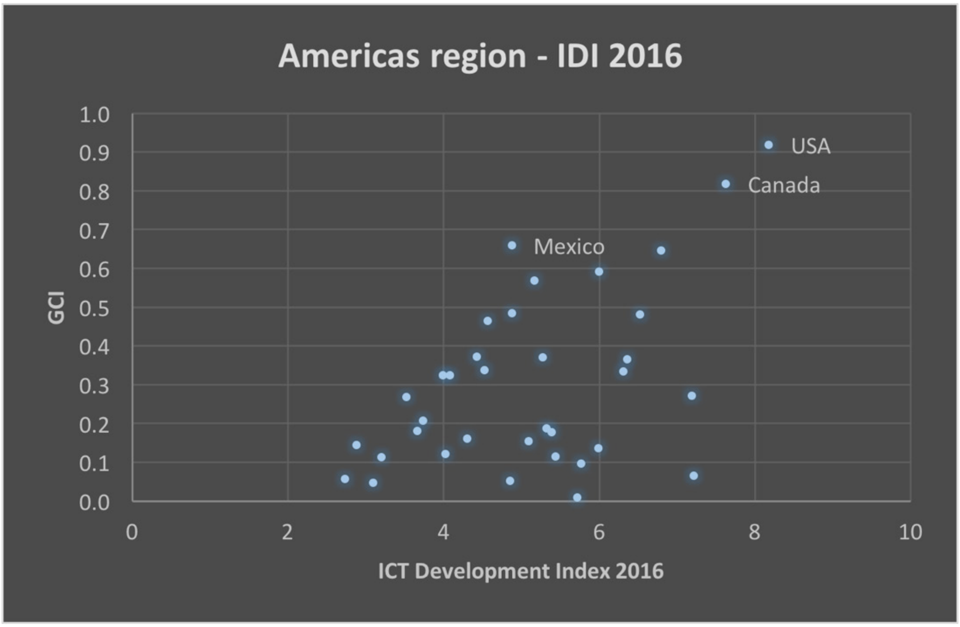


Figure 5.2.4: Comparison GCI and IDI in the Arab States

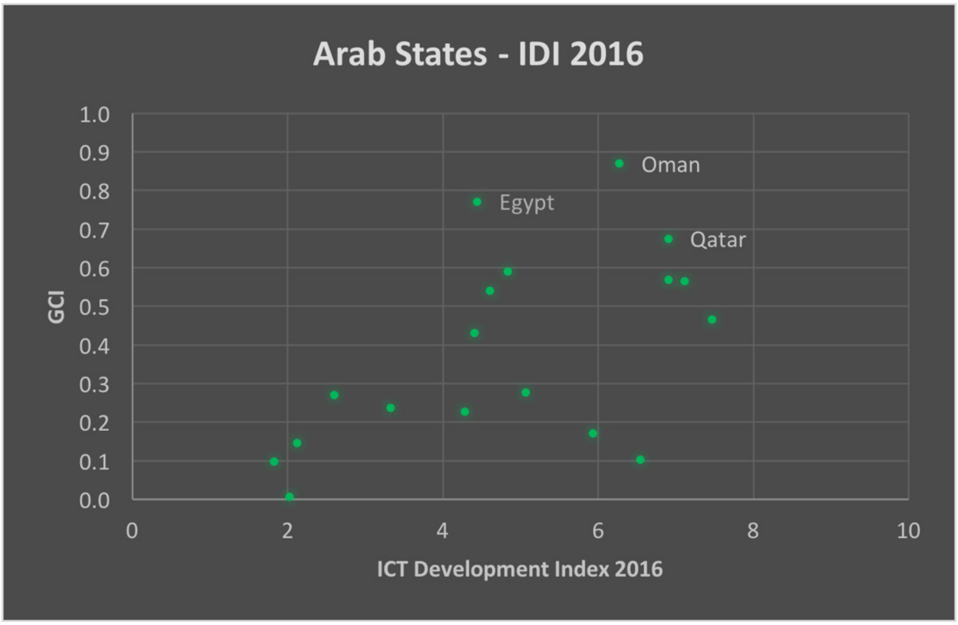


Figure 5.2.5: Comparison GCI and IDI in the Asia and the Pacific region

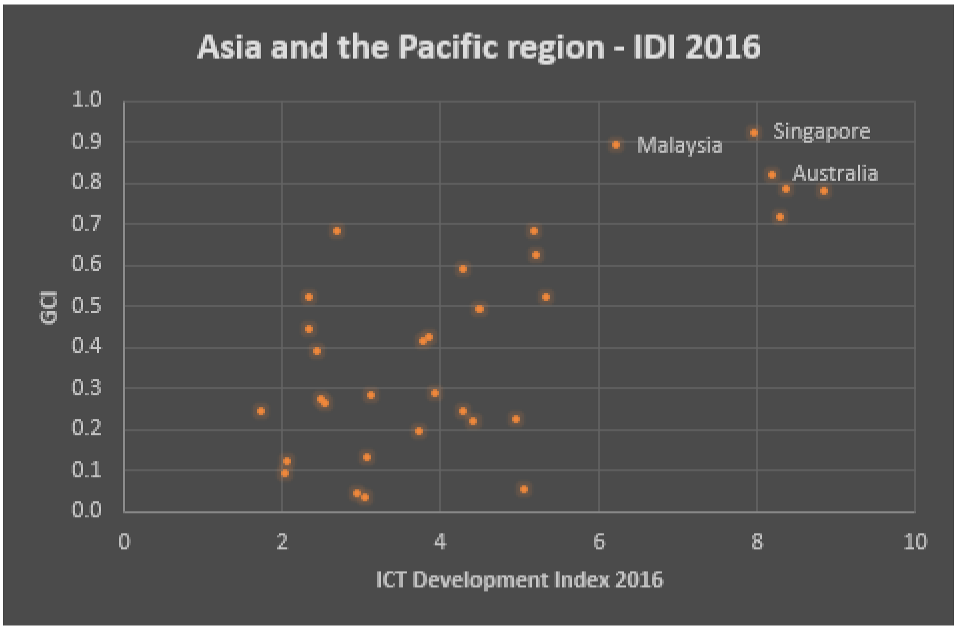


Figure 5.2.6: Comparison GCI and IDI in the Commonwealth of Independent States

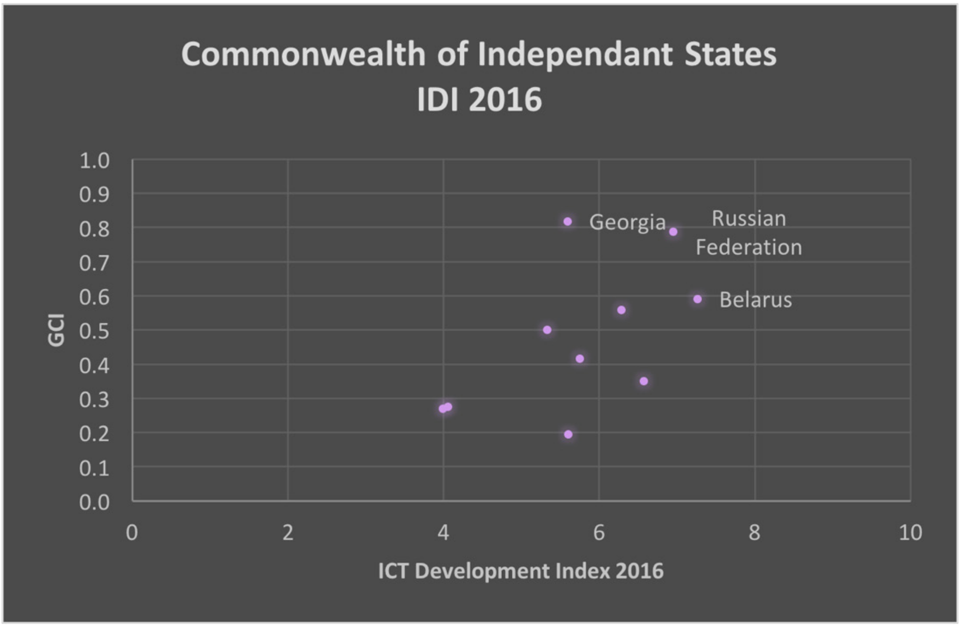
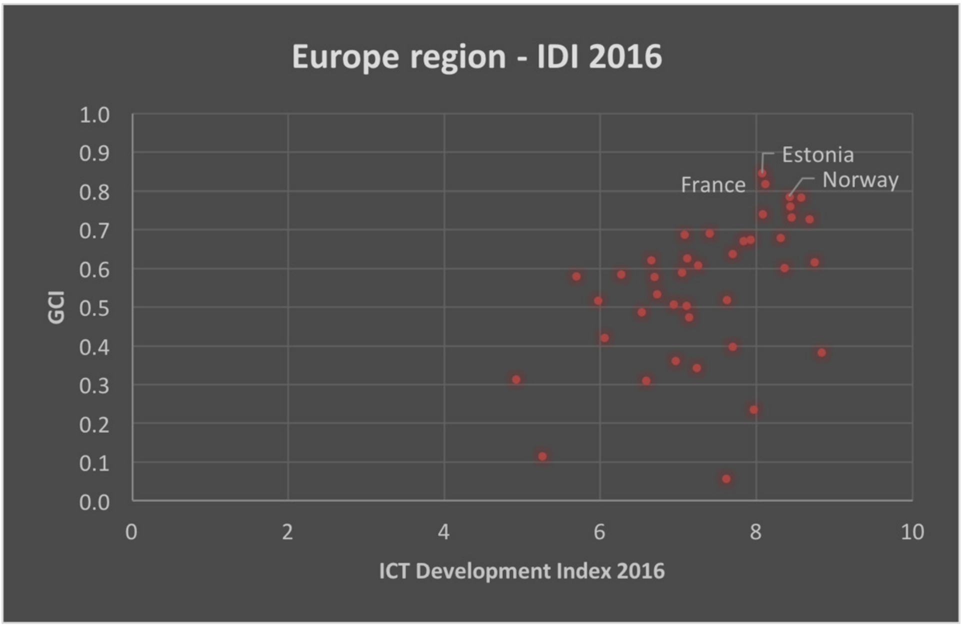


Figure 5.2.7: Comparison GCI and IDI in the Europe region



6 Regional Outlook

During the active data collection phase of the GCI 2017 exercise, there was a varied response from countries in the ITU regions:

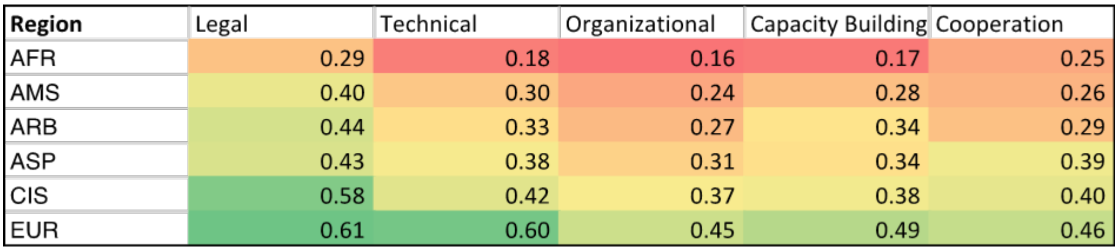
- Out of the 44 Member States in the Africa region, 29 responded to the survey.
- Out of 35 Member States in the Americas region, 23 responded to the survey
- Out of 21 Member States in the Arab States region, 17 including the State of Palestine responded to the survey.
- Out of 38 Member States in the Asia and the Pacific region, 25 responded to the survey
- Out of the 12 Member States in the Commonwealth of Independent States region, 7 responded to the survey
- Out of 43 Member States in the Europe region, 34 responded to the survey.

Figure 6.1 illustrates the average GCI score for all countries in a particular region for the respective pillar. Scores that fall below the 33rd percentile have a red background, scores that are between the 33rd to 65th percentiles have a yellow background and scores that lie above the 65th percentile have a green background. There is scope for improvement since most regions have an average score for the different pillars (i.e., lying between 33rd and 65th percentiles).

The exception is Europe, where average scores are high across all pillars. The Africa region averages low scores for the organizational pillar while the Commonwealth of Independent States region averages a high score for the legal pillar.

The following sub-sections show the findings for each individual ITU region, highlighting the results and findings for the three top-scoring countries in each region. As well, a "regional scorecard" summarizes the countries' level of commitment to every pillar and sub-pillars (green for high, yellow for medium, and red for low).

Figure 6.1: Average pillar scores by region



Region	Legal	Technical	Organizational	Capacity Building	Cooperation
AFR	0.29	0.18	0.16	0.17	0.25
AMS	0.40	0.30	0.24	0.28	0.26
ARB	0.44	0.33	0.27	0.34	0.29
ASP	0.43	0.38	0.31	0.34	0.39
CIS	0.58	0.42	0.37	0.38	0.40
EUR	0.61	0.60	0.45	0.49	0.46

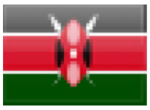
6.1 Africa

Table 6.1.1: Top three ranked countries in Africa

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Mauritius	0.83	0.85	0.96	0.74	0.91	0.7
Rwanda	0.6	0.6	0.71	0.79	0.66	0.28
Kenya	0.57	0.75	0.73	0.36	0.41	0.6

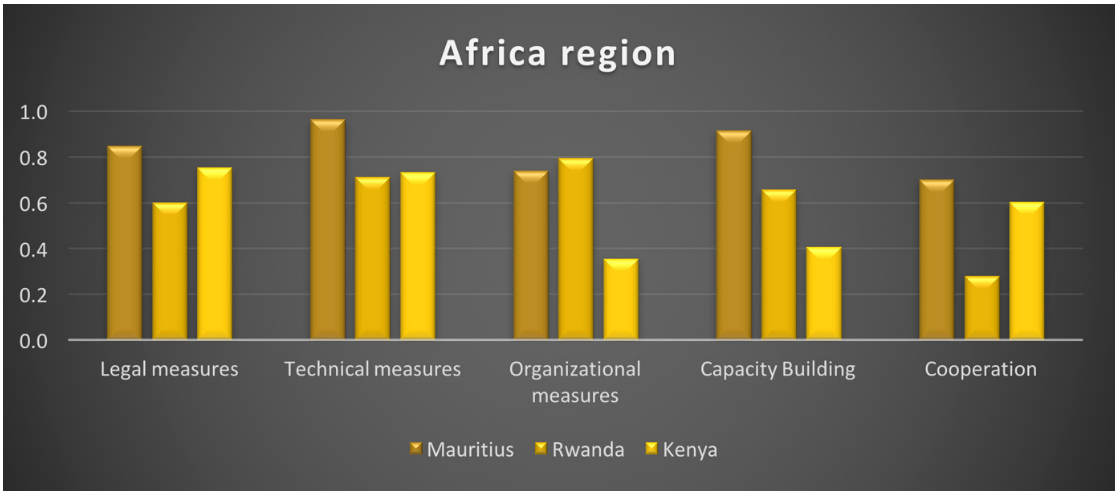
Mauritius is the top ranked country in the Africa region. It scores particularly high in the legal and the technical areas. The Botnet Tracking and Detection project allows Computer Emergency Response Team of Mauritius (CERT-MU) to proactively take measures to curtail threats on different networks within the country. Capacity building is another area where Mauritius does well. The government IT Security Unit has conducted 180 awareness sessions for some 2 000 civil servants in 32 government ministries and departments.

Rwanda, ranked second in Africa, scores high in the organizational pillar and has a standalone cybersecurity policy addressing both the public and private sector[1]. It is also committed to develop a stronger cybersecurity industry to ensure a resilient cyber space.



Kenya, ranked third in the region, provides a good example of cooperation through its National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC)[2]. The CIRT coordinates at national, regional and global levels with a range of actors. Nationally this includes ISPs and the financial and educational sectors; regionally it works with other CIRTs through the East African Communications Organization; and internationally it liaises with ITU, FIRST, and bi-laterally with the United States and Japan CIRTs among others.

Figure 6.1.1: Top three ranked countries in Africa and global ranked of all countries in Africa



[1] http://www.myict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf

[2] http://www.ke-cirt.go.ke/index.php/members/

Figure 6.1.2: Africa region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cyberseucrity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	COOPERATION	GCI
Angola	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Benin	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Botswana	🟢	🟢	🟡	🟢	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟡	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🟡
Burkina Faso	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Burundi	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Cameroon	🟡	🟡	🟢	🟢	🟡	🟢	🔴	🟢	🟡	🔴	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Cape Verde	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Central African Republic	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Chad	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Congo	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Cote d'Ivoire	🟡	🟢	🟢	🟢	🔴	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟢	🟡	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🟡	🟡
Democratic Republic of the Congo	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Equatorial Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Eritrea	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Ethiopia	🟡	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🟡	🔴	🟡	🟡	🟢	🟡	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Gabon	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Gambia	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Ghana	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Guinea-Bissau	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Kenya	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟡	🟡	🟡	🟡	🔴	🟡	🟢	🟡	🟡	🟢	🔴	🟡	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Lesotho	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🔴	🟡	🔴
Liberia	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🟡	🔴	🟡	🔴
Madagascar	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🔴
Malawi	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴
Mali	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Mauritius	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Mozambique	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Namibia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Niger	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟢	🔴
Nigeria	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟡	🟢	🟢	🟡	🟡	🔴	🟡	🔴	🔴	🟢	🟡	🟢	🟢	🟢
Rwanda	🟢	🟢	🔴	🟢	🟡	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟡	🟢	🔴	🟢	🔴	🔴	🟢	🟡	🔴	🟡	🟢
Sao Tome and Principe	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Senegal	🟡	🟢	🟡	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🔴	🟢	🟡
Seychelles	🟢	🟡	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Sierra Leone	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
South Africa	🟢	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟡	🟡	🔴	🟢	🟡	🔴	🔴	🟢	🟡	🔴	🟡	🟡
South Sudan	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Swaziland	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Tanzania	🟢	🟡	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🟡	🔴	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Togo	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Uganda	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🟢	🟢	🟡	🟢	🔴	🔴	🟢	🟢	🟡
Zambia	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🟢	🟢	🔴	🔴	🟡	🟡
Zimbabwe	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

6.2 Americas

Table 6.2.1: Top three ranked countries in the Americas

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	0.91	1	0.96	0.92	1	0.73
Canada	0.81	0.94	0.93	0.71	0.82	0.70
Mexico	0.66	0.91	0.89	0.48	0.68	0.34

The top three ranked countries in the Americas region are the members of the North American Free Trade Association (NAFTA).

The United States of America has the highest scores for the legal and capacity building pillars. One notable aspect of both capacity building and cooperation in the country is the initiatives to coordinate cybersecurity among all states. To that end, the National Governor's Association established the Resource Center for State Cybersecurity, which offers best practices, tools and guidelines [3].

Canada ranks second in the region with its highest score in the legal pillar. The country's Personal Information Protection and Electronic Documents Act (PIPEDA) features several sections relating to cybersecurity[4]. It requires organizations to notify privacy authorities in the event of privacy breaches that could cause significant damage with penalties for those who fail to report them.

Mexico is third and some 16 points behind Canada, illustrating the cybersecurity divide in the region. Like the other top ranked countries in the region, it scores best in the legal pillar with a full suite of cyber legislation covering criminality, data protection, data privacy and electronic transactions.

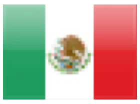
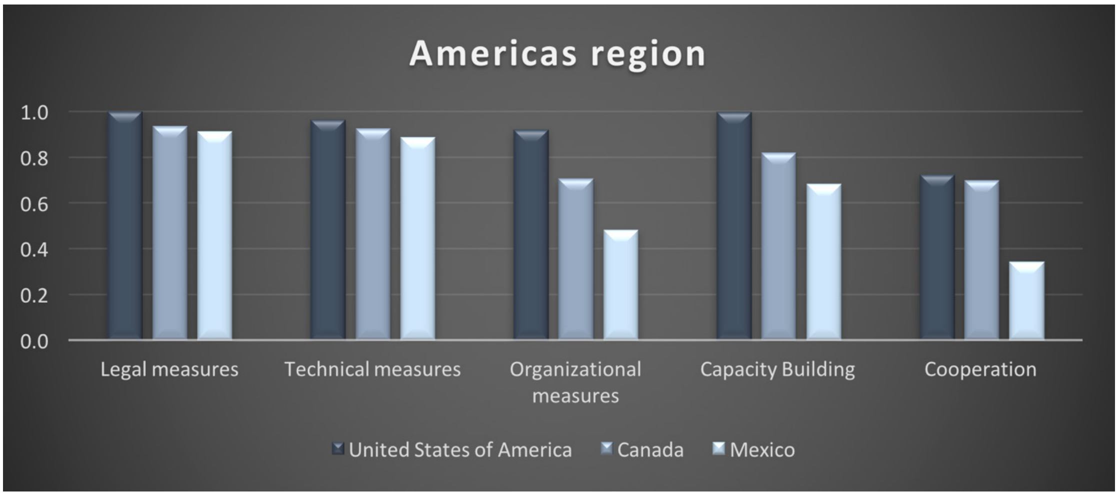


Figure 6.2.1: Top three ranked countries and an average score of all the Americas



[3] https://www.nga.org/cms/statecyber

[4] http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Figure 6.2.2: Americas region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cyberseucrity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Antigua and Barbuda	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Argentina	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🔴	🟡	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🟢	🟡	🟡
Bahamas	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Barbados	🟡	🔴	🟢	🟡	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Belize	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Bolivia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Brazil	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟡	🟡	🔴	🔴	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟡
Canada	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Chile	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🔴	🔴	🔴	🟡	🟢	🔴	🟢	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟡	🔴	🟡	🟡
Colombia	🟢	🟢	🔴	🟡	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🔴	🟡	🔴	🟢	🟢	🟡	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟡
Costa Rica	🟢	🟡	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🟡
Cuba	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Dominica	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Dominican Republic	🟡	🟡	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Ecuador	🔴	🟢	🟢	🟡	🟢	🔴	🟢	🟢	🟡	🔴	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🔴	🔴	🟡
El Salvador	🟡	🟡	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Grenada	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Guatemala	🔴	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Guyana	🟡	🟡	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Haiti	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Honduras	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Jamaica	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🟡	🔴	🟡	🟡	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟡	🔴	🔴	🟢	🟡	🔴	🟡	🟡
Mexico	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟡	🟡	🔴	🟢	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🔴	🔴	🟢	🔴	🟢	🟡	🟢
Nicaragua	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Panama	🟡	🟡	🔴	🟡	🔴	🟢	🔴	🟢	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🟢	🟢	🟢	🟡
Paraguay	🟢	🟡	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🔴	🟡	🟡	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Peru	🟡	🟡	🔴	🟡	🟢	🟢	🔴	🟢	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Saint Kitts and Nevis	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Saint Lucia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Saint Vincent and the Grenadines	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Suriname	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🔴
Trinidad and Tobago	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
United States of America	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🟢
Uruguay	🔴	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟡	🟡	🔴	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Venezuela	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟡	🟡	🔴	🟡	🟡	🟡	🔴	🟢	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡

6.3 Arab States

Table 6.3.1: Top three ranked countries in the Arab States

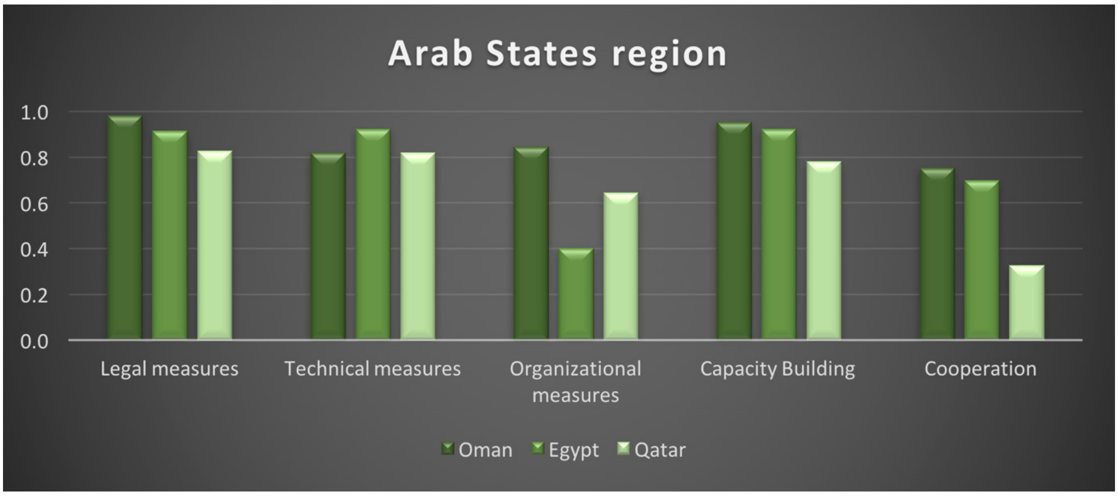
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Egypt	0.77	0.92	0.92	0.4	0.92	0.7
Qatar	0.67	0.83	0.82	0.65	0.78	0.33

Sultanate of Oman is the top ranked in the Arab States with the highest scores in the legal and capacity building pillars. Oman has a robust organizational structure, including a high-level cybersecurity strategy and master plan and comprehensive roadmap.

Egypt ranks second with a full range of cooperation initiatives. It is a member of the UN Government Group of Experts (GGE) on cybersecurity[5], has chaired the ITU Working Group for Child Online Protection[6], was a founding member of AfricaCERT[7], and has a number of bi-lateral and multilateral agreements on cybersecurity cooperation.

Qatar ranks third and has been building a cybersecurity culture through campaigns such as Safer Internet Day and has spread warnings about online threats, such as fraud and Internet scams, via print and social media. The Qatar Cyber Crimes Investigation Center and Information Security Center support efforts to safeguard the public and crack down on those who use technology to carry out criminal activities.

Figure 6.3.1: Top three ranked countries and an average score of the Arab States

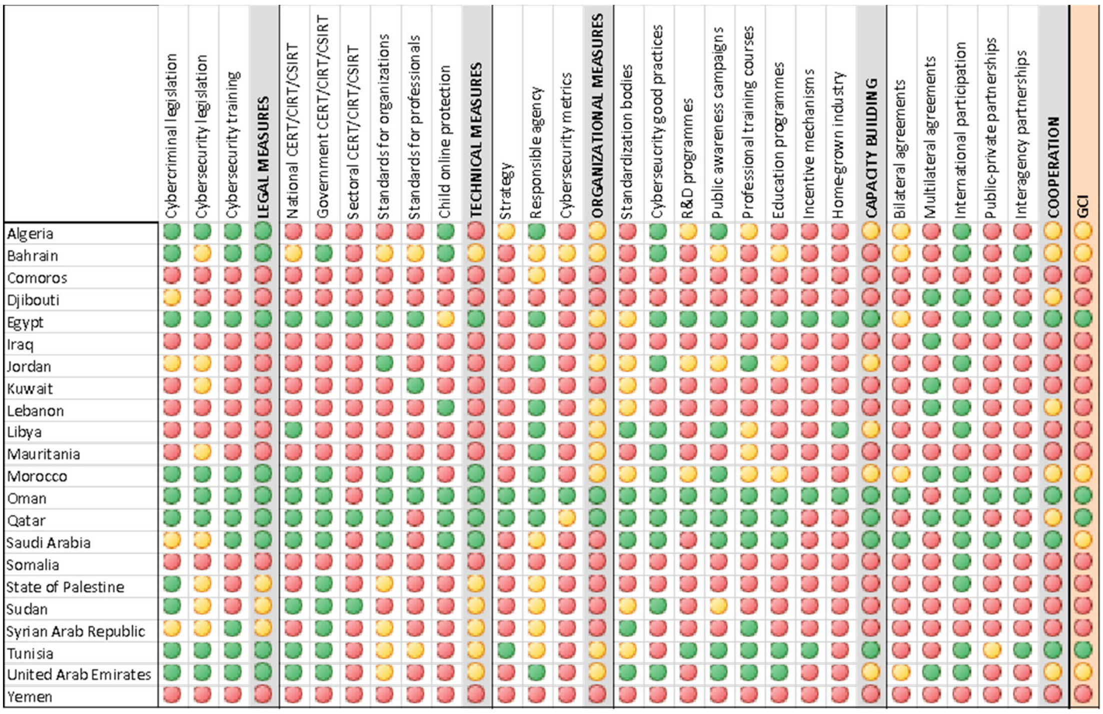


[5] https://www.un.org/disarmament/topics/informationsecurity/

[6] http://www.itu.int/en/council/cwg-cop/Pages/default.aspx

[7] https://www.africacert.org/home/

Figure 6.3.2: Arab States scorecard



	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cyberseucrity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Algeria	🟢	🟢	🟢	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🟡	🔴	🟢	🟡	🟢	🟡	🔴	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🟡	🟡
Bahrain	🟢	🟡	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟡	🔴	🟡	🟡	🟡	🔴	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟢	🟡	🟡
Comoros	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Djibouti	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴
Egypt	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Iraq	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴
Jordan	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🟢	🟡	🟡	🟢	🟡	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Kuwait	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴
Lebanon	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴
Libya	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🟢	🔴	🟢	🟡	🔴	🔴	🟢	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Mauritania	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Morocco	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🟡	🟢	🟡	🟡	🔴	🔴	🟡	🟡	🟢	🟢	🔴	🔴	🟡	🟡
Oman	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢
Qatar	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🟢	🟢	🔴	🔴	🟡	🟢
Saudi Arabia	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟡
Somalia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
State of Palestine	🟢	🟡	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Sudan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🟡	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Syrian Arab Republic	🟡	🟡	🟢	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Tunisia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟡	🔴	🟡	🟢	🟡	🔴	🟡	🟡	🔴	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🔴	🟢	🟡	🟢	🟢	🟢
United Arab Emirates	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🔴	🟡	🟡	🟢	🟢	🔴	🔴	🟡	🟡
Yemen	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴

6.4 Asia and the Pacific

Table 6.4.1: Top three ranked countries in Asia and the Pacific

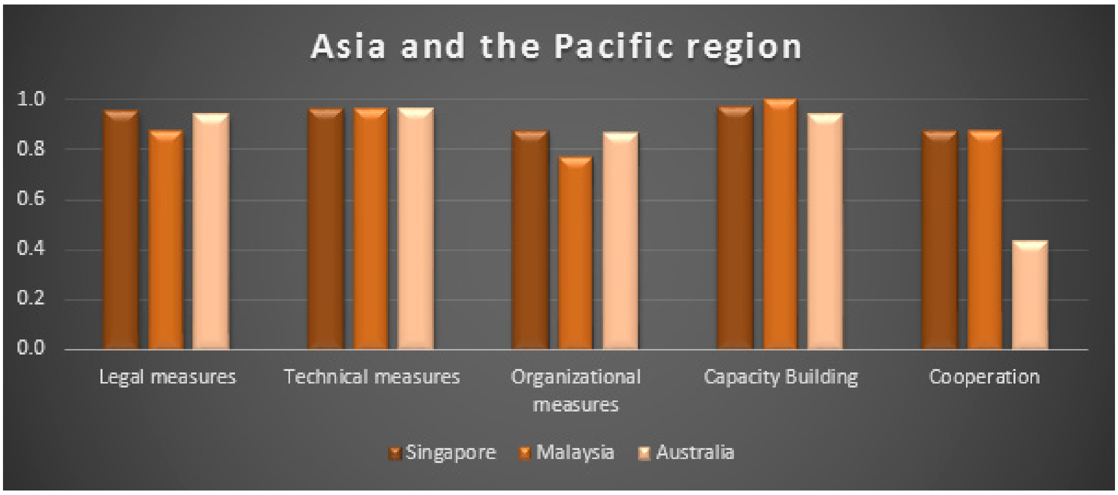
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Australia	0.82	0.94	0.96	0.86	0.94	0.44

Singapore is the top ranked country in the region. The island state has a long history of cybersecurity initiatives. It launched its first cybersecurity master plan back in 2005. The Cyber Security Agency of Singapore was created in 2015 as a dedicated entity to oversee cybersecurity and the country issued a comprehensive strategy in 2016[8].

Malaysia is ranked second in the Asia and the Pacific region and scores a perfect 100 on capacity building due to a range of initiatives in that pillar. Cybersecurity Malaysia, the government entity responsible for information security in the country, offers professional training via higher education institutions in Malaysia. It maintains the *Cyberguru* website, dedicated to professional security training[9].

Australia[10] is third ranked in the region and home to AusCERT, one of oldest CERTs in the region formed in 1993[11]. The highest scoring pillar is technical where there is a certification programme for information security skills provided by the Council of Registered Ethical Security Testers (CREST)[12]. Modelled after CREST, the council offers assessment, accreditation, certification, education and training in cyber and information security for individuals and corporate entities in both Australia and New Zealand.

Figure 6.4.1: Top three ranked countries and an average score of all Asia and the Pacific



[8] https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

[9] http://www.cyberguru.my

[10] http://thecommonwealth.org/member-countries

[11] https://www.auscert.org.au

[12] https://www.crestaustralia.org

Figure 6.4.2: Asia and the Pacific Region Scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cyberseucrity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Afghanistan	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
Australia	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🔴	🟢	🟡	🟢
Bangladesh	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🟢	🔴	🟡	🟢	🔴	🟢	🟢	🟡	🟡	🟢	🔴	🟡	🔴	🔴	🟢	🟡	🔴	🔴	🟡
Bhutan	🔴	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Brunei Darussalam	🟢	🔴	🟢	🟡	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟡
Cambodia	🟡	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🔴	🔴
China	🟡	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🔴	🟢	🟡	🟡
Democratic People'	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🟢	🔴	🟡
Fiji	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🔴
India	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🔴	🟡	🟢
Indonesia	🟢	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🟡	🟢	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🟢	🔴	🟡
Iran	🟢	🟡	🔴	🟡	🟡	🟢	🟢	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟡
Japan	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢
Kiribati	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Lao	🟢	🟡	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟡	🟡
Malaysia	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢
Maldives	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Marshall Islands	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Micronesia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Mongolia	🔴	🟡	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🔴
Myanmar	🟡	🟡	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
Nauru	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
Nepal	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
New Zealand	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟡	🟢	🟢	🟡	🟡	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Pakistan	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🟡
Palau	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Papua New Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Philippines	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟢	🟢	🔴	🟡	🟡	🟢	🟡	🟡	🟢	🟡	🔴	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🟡	🟡
Republic of Korea	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Samoa	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Singapore	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Solomon Islands	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Sri Lanka	🔴	🔴	🟢	🔴	🟢	🟢	🟢	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟢	🟡	🟢	🟢	🟡	🔴	🔴	🟡	🔴	🟢	🟢	🟡	🔴	🟡	🟡
Thailand	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🟡	🔴	🟡	🟢
Timor-Leste	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Tonga	🟢	🔴	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🟡	🟢	🟡	🔴
Tuvalu	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Vanuatu	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🔴
Viet Nam	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

6.5 Commonwealth of Independent States

Table 6.5.1: Top three ranked countries in Commonwealth of Independent States

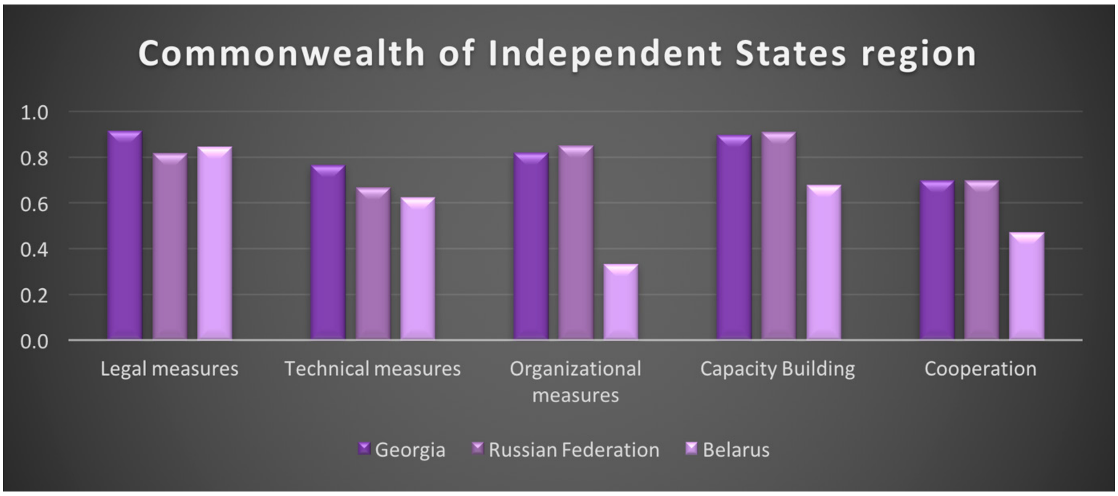
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Georgia	0.81	0.91	0.77	0.82	0.9	0.7
Russian Federation	0.78	0.82	0.67	0.85	0.91	0.7
Belarus	0.59	0.85	0.63	0.33	0.68	0.47

Georgia is top ranked in the CIS. After large-scale cyber-attacks on the country in 2008, the government has strongly supported protection of the country's information systems[13]. The Information Security Law[14] established a Cyber Security Bureau with a particular emphasis on protecting critical information systems in the military sphere.

The Russian Federation, ranked second in the region, scores best in capacity building. Its commitments range from developing cybersecurity standards to R&D and from public awareness to a home-grown cybersecurity industry. An example of the latter is Kaspersky Labs, founded in 1997 and whose software protects over 400 million users and some 270 000 organizations[15].

Belarus is the third ranked country, where child protection initiatives include public and private partnerships. Mobile operator MTS has implemented a project with the Ministry of Education to teach children about safe Internet practices that has so far reached some 6 000 children[16].

Figure 6.5.1: Top three ranked countries and an average score of all CIS



[13] http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx?lang=en-US
[14] https://matsne.gov.ge/en/document/view/1679424
[15] https://usa.kaspersky.com/about
[16] http://www.mts.by/news/97338/

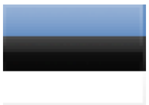
Figure 6.5.2: CIS region scorecard

	Cybercriminal le	Cybersecurity le:	Cybersecurity t	**LEGAL MEA**	National CERT/CI	Government CERT/C	Sectoral CERT/CII	Standards for orga	Standards for prof	Child online pro	**TECHNICAL ME**	Strate	Responsible a	Cybersecurity	**ORGANIZATIONAL I**	Standardization	Cyberseucrity good	R&D progra	Public awareness c	Professional trainin	Education progr	Incentive mech	Home-grown i	**CAPACITY BU**	Bilateral agree	Multilateral agre	International part	Public-private par	Interagency part	**COOPERA**	**GC**
Armenia	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Azerbaijan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🔴	🔴	🟡	🟢	🟡	🟢	🟢	🟡	🔴	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡
Belarus	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟢	🟡	🟡
Georgia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Kazakhstan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟡	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Moldova	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🟡	🟢	🟡	🟡
Russian Federation	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Tajikistan	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Turkmenistan	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Ukraine	🟡	🟢	🟢	🟢	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🔴	🟡	🟡	🟡	🔴	🔴	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟡
Uzbekistan	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

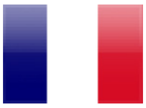
6.6 Europe

Table 6.6.1: Top three ranked countries in Europe

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
France	0.81	0.94	0.96	0.6	1	0.61
Norway	0.78	0.96	0.89	0.64	80.8	0.57



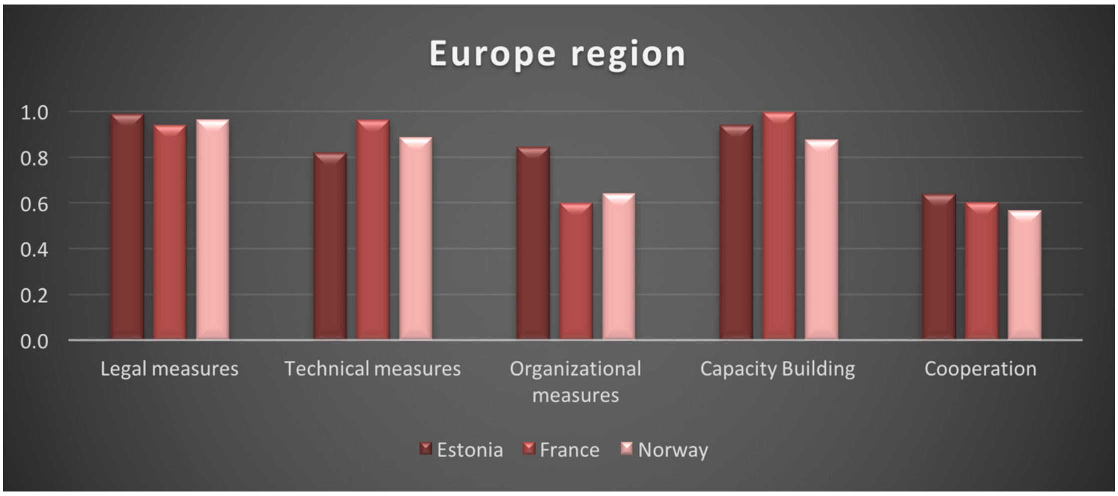
Estonia is the highest-ranking nation in the Europe region. Like Georgia, Estonia enhanced its cybersecurity commitment after a 2007 attack. This included the introduction of an organizational structure that can respond quickly to attacks as well as a legal act that requires all vital services to maintain a minimal level of operation if they are cut off from the Internet[17]. The country also hosts the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence[18].



France is the second highest ranked in the Europe region, scoring a perfect 100 in capacity building. There is widespread cybersecurity training available in the country, and the National Agency for Information System Security (ANSSI in French) publishes a list of dozens of universities that provide accredited cybersecurity degrees recognized[19].

Norway is ranked third in Europe with its highest score in the legal pillar. Apart from laws dealing with cybersecurity, Norway has also conducted research on its cybersecurity culture including surveying citizens about the degree to which they will accept monitoring of their online activities.[20]

Figure 6.6.1: Top three ranked countries and an average score of all Europe



[17] http://www.nextgov.com/cybersecurity/2015/01/heres-what-us-could-learn-estonia-about-cybersecurity/103959/

[18] https://ccdcoe.org

[19] https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/

[20] https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

Figure 6.6.2: Europe region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cyberseucrity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	COOPERATION	GCI
Albania	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟢	🟡	🔴
Andorra	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Austria	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🟡	🔴	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🟡	🔴	🟢	🔴	🟢	🟡	🟢
Belgium	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🔴	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟢
Bosnia and Herzegovina	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴
Bulgaria	🔴	🟢	🟢	🟡	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🔴	🟡	🟢	🟡	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟡
Croatia	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟡	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🟢	🔴	🟢	🟢	🟢	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟢
Cyprus	🔴	🟡	🟢	🟡	🔴	🟢	🟢	🔴	🔴	🟢	🟡	🟢	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🟢	🔴	🟡	🟡	🔴	🟢	🟢	🟡	🔴	🟡	🟡
Czech Republic	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🔴	🔴	🟢	🟡	🔴	🔴	🟢
Denmark	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🔴	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Estonia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🟢
Finland	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢
France	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢	🟡	🟢	🟢	🟢
Germany	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢	🟡	🟡	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟢
Greece	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🟡
Hungary	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🟡
Iceland	🟡	🟡	🟡	🟡	🟡	🔴	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🟡	🔴	🟡	🟡
Ireland	🟡	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Israel	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Italy	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟢	🟡	🟢	🟡	🟢	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Latvia	🟢	🟡	🟡	🟡	🟢	🔴	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🟡	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢
Liechtenstein	🟢	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Lithuania	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🟡	🔴	🟢	🟡	🔴	🟡	🟡
Luxembourg	🟡	🟢	🟡	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟢
Malta	🔴	🟢	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🟢	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Monaco	🟡	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Montenegro	🔴	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🟢	🟡	🟡	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🟡
Netherlands	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟡	🟢	🟡	🟢	🟡	🔴	🟢	🟢	🟢	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢
Norway	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Poland	🟢	🟢	🔴	🟡	🟡	🟢	🟢	🟡	🔴	🟢	🟡	🟡	🟢	🟡	🟢	🟡	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Portugal	🟡	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟢	🟢	🟢	🟡	🟡	🟡	🔴	🔴	🟢	🔴	🟢	🟡	🟡
Romania	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🟢	🟢	🟢	🟢	🟡
San Marino	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Serbia	🟢	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🟢	🟡	🔴	🔴	🔴
Slovakia	🟡	🔴	🔴	🔴	🟢	🟢	🟢	🟡	🔴	🔴	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Slovenia	🔴	🟢	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🟢	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Spain	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🟡	🟢	🔴	🟢	🟢	🟡	🟡	🟢	🔴	🟢	🔴	🔴	🟡	🟡
Sweden	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🟢	🟡	🔴	🟡	🟡	🟢	🟡	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢	🟢
Switzerland	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢
The former Yugoslav Republic of Macedonia	🔴	🟢	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟡
Turkey	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🟡	🟢	🟢	🟡	🟢	🟡	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
United Kingdom	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟡	🟢

7 Illustrative practices by pillar

This chapter identifies noteworthy and thought-provoking practices in cybersecurity across the various GCI pillars. Examples are drawn from a number of countries and provide an insight on the cybersecurity commitment taken in their focus areas.

7.1 Legal

Examples for this pillar illustrate practices in national cybercrime legislation regarding unauthorized access, data and system interference or interception, and misuse of computer systems.

7.1.1 Cybercrime legislation

Colombia became one of the first countries in the world when, in 2009, it enacted a law specifically targeting cyberspace. Law 1273 (entitled "By means of which the Penal Code is amended, a new legal right is created- called ’protection of information and data‘- and systems that use information and communication technologies are fully preserved, among other provisions"[1]) calls for a prison sentence or large fines for anyone convicted of information systems or telecommunication network crimes. The law covers areas such as illegally accessing personal information, intercepting data, destroying data or using malicious software.

Georgia established cybercrime legislation in line with the principles and rules of the Budapest Convention both in terms of substantive and procedural aspects. Illegal access to information systems, data and system interference, and misuse of devices are criminalized by the Georgia criminal code. The Personal Data Protection Act was enacted by Parliament in 2011 and is intended to ensure protection of human rights and freedoms, including the right to privacy, in the course of personal data processing.[2]

7.1.2 Cybersecurity regulation

Sultanate of Oman established the eGovernance Framework, a set of standards / best practices and process management systems to enhance the delivery of government services in alignment with the mission of e.oman (Sultanate of Oman Digital Oman Strategy and eGovernment). The framework spells out the rules and procedures that ensure that government IT projects and systems are sustainable and in compliance with the Information Technology Authority (ITA) strategies and objectives. It provides assurance about the value of IT projects and framework for the management of IT-related risks. It helps in putting controls to minimize risks and better delivery of IT initiatives[3].

7.1.3 Cybersecurity training

Mauritius makes available training for law enforcement and judiciary which has been conducted under the GLACY Project since 2013 and is still ongoing. CERT-MU also carried out cybersecurity trainings on digital forensic investigator professional and network forensic (packet analysis) for law enforcement officers. Training on

[1] Government of Colombia. Law 1273 of 2009. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. http://www.mintic.gov.co/portal/604/w3-article-3705.html

[2] https://personaldata.ge/en/legislation/national-legislation ; https://matsne.gov.ge/ka/document/view/16426?impose=translateEn

[3] http://www.ita.gov.om/ITAPortal/Government/Government_Projects.aspx?NID=76

information security standards and best practices is given to the technical officers of the IT Security Unit (ITSU) of the Ministry of Technology, Communication and Innovation[4].

The **New Zealand** (NZ) Police is introducing a 3-tiered training program for specialist cyber staff, investigators and then frontline staff. This is outlined in NZ Police's Prevention First National Cybercrime Strategy 2014-2017[5]. NZ Police also provides training to the judiciary and prosecutors.

7.2 Technical

Examples for this pillar illustrate practices in areas such as existence of technical institutions, child online protection and industry standards and certification.

7.2.1 National CERT/CIRT/CSIRT

Egypt provides computer emergency response team (EG-CERT) support to several entities in the ICT sector, the financial sector as well as the government sector, in order to help them tackle cybersecurity related threats. EG-CERT is expanding and is currently upgrading its laboratories in the four key operational departments. Additional laboratories are being planned for mobile cybersecurity and industrial control systems cybersecurity[6].

Brazil has three computer emergency response teams with different functions, namely: the national CERT, a government CSIRT and a sector specific SCIRT. The Brazil Federal Police participates in the I-24/7 global police communications system developed by Interpol to connect law enforcement officers, including cybercrimes. There is also a complementary Standard No. 17/IN01/DSIC/GSIPR that establishes guidelines for the certification and accreditation for information and communication security professionals of the direct and indirect Federal Public Administration.

7.2.2 Government CERT/CIRT/CSIRT

Luxembourg created a computer emergency response team (GOVCERT.LU) in 2011 to help protect government computer systems and data as well as specific infrastructures and is engaged at both national and international level under the name of NCERT.LU[7]. GOVCERT.LU is also a critical player in the event of a large cyber-attack affecting country's ICT assets.

7.2.3 Sectoral CERT/CIRT/CSIRT

Sri Lanka created the Financial Sector Computer Security Incident Response Team (FINCSIRT) in 2014 with responsibility for receiving, reviewing, processing and responding to computer security alerts and incidents affecting banks and other licensed financial institutions in the country[8]. FINCSIRT is a joint initiative of the Central Bank of Sri Lanka and the Sri Lanka computer emergency response team and is steered and funded by the banking sector. Related to FINCSIRT is LankaClear, the country's certification authority owned by the Central Bank and commercial banks[9].

[4] http://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/glacy-support-to-mauritius-judicial-training-courses-on-cybercrime-delivered

[5] http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf (page 10)

[6] http://www.egcert.org

[7] https://www.govcert.lu/en/ncert.html

[8] http://www.fincsirt.lk

[9] http://www.lankaclear.com/about/index.php

7.2.4 Cybersecurity standards implementation framework for organizations

Malaysia created the Information Security Certification Body (ISCB), a department of Cybersecurity Malaysia, which manages information security certification[10]. The certification services are consistent with international standards and guidelines and include among others the Malaysian Common Criteria Evaluation and Certification (MyCC), which certifies security functions of ICT products based on the ISO/IEC 15408 international standard[11].

Hungary national regulation lays out the framework for information security training for state and local government officials[12]. The National University for Public Service (NKE) is charged with training and establishing a certification system[13]. Certificates issued include information security risk assessment and testing of electronic information systems.

7.2.5 Child online protection

Singapore's Internet Content Providers (ICPs) and Internet Access Service Providers (IASPs) are licensable under the Broadcasting Act and they are required to comply with the Internet Code of Practice to protect children online. Since 2012, all service providers have been legally obligated to offer filtering services with Internet subscriptions and to make this known to consumers when they subscribe or renew. The Info-communications Media Development Authority also symbolically blocks 100 pornographic, extremist or hate websites.

7.3 Organizational

Examples for this pillar illustrate practices where governments are organized by having a cybersecurity strategy, a coordinating agency and compilation of indicators for tracking cybercrime.

7.3.1 Strategy

United Kingdom issued in 2016 its second five years *National Cyber Security Strategy*[14]. The strategy, issued by the Cabinet Office, aims to make the country one of the safest places in the world to carry out online business and doubles investment in cybersecurity compared to the first plan.

Russian Federation officially adopted its National Security Strategy in 2000 and National Security Concept of the Russian Federation as well as Concept of the Foreign Policy of the Russian Federation in 2013. It established an Information Security Doctrine of the Russian Federation in 2000 and each government entity in the Russian Federation performs an annual audit of its own networks and systems in line with the doctrine and the areas identified in the various strategies adopted.

[10] http://www.cybersecurity.my/en/our_services/iscb/main/detail/2327/index.html

[11] http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

[12] http://njt.hu/cgi_bin/njt_doc.cgi?docid=164331.250717

[13] http://en.uni-nke.hu

[14] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

7.3.2 Public consultation

Canada conducted a three-month public consultation on updating its cybersecurity strategy, asking security professionals and citizens for inputs and views. The consultation was done to help identify gaps and opportunities, bring forward new ideas to shape Canada's renewed approach to cybersecurity and capitalize on the advantages of new technology and the digital economy[15].

7.3.3 Responsible agency

Iceland created the Cyber Security Council, appointed by the Minister of the Interior that is responsible for overseeing the implementation of the National Cyber Security Strategy. In addition, a cyber security forum has been created as a collaborative venue for representatives of public bodies who sit on the Cyber Security Council and of private entities.

7.3.4 Cybersecurity metrics

Netherlands uses metrics annually in order to measure cybersecurity development at a national level, summarized in the Cyber Security Assessment Netherlands report[16]. The National Cyber Security Centre (NCSC) compiles disclosure reports, security advisories and incidents using a registration system. The metrics allow trends to be observed and acted on.

7.4 Capacity building

Examples of practices for capacity building include the aspects of developing the technical and human resources for fighting cybercrime. This includes raising awareness about cybersecurity among the public, the existence of cybersecurity standards and standards bodies, best practices guides, education initiatives and research and development.

7.4.1 Standardization bodies

Romania created the National Standardization Organization[17] to produce relevant national standards on processes, tools and technologies for software products and systems in the area of security in information technology. It also tests the standardization integrity of encryption algorithms, authentication services and algorithms for confidential services in compliance with accepted international standards[18].

7.4.2 Good practice

Canada created the Investment Industry Regulatory Organization (IIROC) that is the national self-regulatory organization overseeing investment dealers and their trading activity in the country's debt and equity markets. IIROC published a cybersecurity best practices guide for its members[19].

[15] http://www.itworldcanada.com/article/breaking-news-ottawa-announces-public-consultation-on-cyber-security-strategy/385740#ixzz4dm1QjsTu

[16] https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html

[17] http://www.asro.ro/

[18] http://www.asro.ro/CTmementoSite.html#BM208

[19] http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

7.4.3 Cybersecurity research and development programmes

Germany signed an agreement in 2009 on cooperation in IT security research between the Federal Ministry of Education and Research (BMBF) and the Federal Ministry of the Interior (BMI). The IT Security Research programme covers research and development in new information security technologies. The BMBF has been supporting three research centres since 2011 that bring together leading university and non-university establishments in cybersecurity[20].

Kenya Education Network, (KENET), is the National Research and Education Network (NREN) of Kenya. KENET is the computer emergency response team (CERT) for the academic community and is licensed by the Communications Authority of Kenya (CA) as a not-for-profit operator serving the education and research institutions. They most notably provide affordable, cost-effective and low-congestion Internet bandwidth services to member institution campuses in Kenya.

7.4.4 Public awareness campaigns

Latvia has published a series of articles on its national CERT portal about free-of-charge security solutions including anti-viruses, firewalls, NoScript, etc.[21] Twice a year, the national CERT organizes a campaign where people can bring their computers for a check-up to see if they are infected, and it also distributes commercial anti-virus installations during the campaigns that are made available free-of-charge for one year.

7.4.5 Cybersecurity professional training courses

Bulgaria established the International Cyber Investigation Training Academy in 2009, which is a non-governmental organization[22]. The academy aims to improve the qualification of specialists working in the field of cybersecurity. It has trained over 1 300 people from both the public and private sectors.

7.4.6 National education programmes and academic curricula

Germany has several universities and institutes providing degrees and certificates in information security[23]. The Federal Ministry of Education and Research funds the KASTEL competence centre that offers training leading to a certificate equivalent to a specialized master degree in IT security[24]. The Technical University of Darmstadt has been offering a Master of Science Degree in IT security since 2010[25].

7.4.7 Incentive mechanisms

Korea Internet Security Agency (KISA) is committed to establishing a network foundation for Internet users and Internet companies by improving competitiveness of Internet services and reliability of Internet information and knowledge. KISA supports start-ups to commercialize their business models and enhance competitive edge in the field of security technology through programmes that aim to nurture start-ups in the Internet-of-things, security, and Fintech industry. They also established the one-stop

[20] https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html
[21] https://www.esidross.lv/category/bezmaksas-risinajumi/page/2/
[22] http://e-crimeacademy.com/
[23] https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html
[24] http://www.kastel.kit.edu
[25] https://www.tu-darmstadt.de/studieren/abschluesse/master/it-sicherheit-msc.en.jsp

service to support start-ups to gain ground not only in the domestic market but also the global market to expand their business models.

7.4.8 Home-grown cybersecurity industry

Ireland has the largest proportion of the Information and Communication sector of its economy compared to all other countries in Europe and is leveraging that advantage to grow its cybersecurity industry. The country is drawing on existing incentives and attractions with the aim of being a cybersecurity capital[26]. These incentives include a favourable business environment and low taxes, a talented pool of highly skilled and multilingual workers and a good base for access to European markets[27].

7.5 Cooperation

This pillar considers collaborative efforts across national and international domains and between the public and private sector.

7.5.1 Bilateral agreements

Finland is an active member of many organizations, such as the Council of Europe (CoE), the Organization for Security and Co-operation in Europe (OSCE) and the United Nations (UN). Finland has also joined the NATO Partnership for Peace and is engaged in cooperation with the organization in, for example, crisis management. There is also local partnership with Finnish company Codenomicon, which later was acquired by Synopsys, to develop the national IDS system and automatic incident reporting service with FICORA[28].

7.5.2 Multilateral agreements

Denmark, Finland, Iceland, Norway and **Sweden** collaborate through the Nordic National CERT Collaboration. This includes technical cooperation and cybersecurity exercises to assess and strengthen cyber preparedness, examine incident response processes and enhance information sharing in the region[29].

7.5.3 Participation in international fora

Participation in international cybersecurity events, workshops and training is the one indicator where virtually all countries score high on the GCI. Therefore, it is more revealing to describe one of the most significant initiatives in this regard. The Forum of Incident Response and Security Teams (FIRST)[30] was founded in 1990. Its members are security and incident response teams from the public, private and academic sectors. It organizes an annual conference, technical colloquia and training workshops.

[26] https://www.siliconrepublic.com/companies/cybersecurity-hub-ireland

[27] http://www.idaireland.com/how-we-help/resources/infographics/ida-cyber-security/IDA_CYBER_SECURITY.pdf

[28] http://formin.finland.fi/public/default.aspx?nodeid=49303&contentlan=2&culture=fi-FI https://www.synopsys.com/services.html

[29] https://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/

[30] www.FIRST.org

7.5.4 Public -private partnerships

The **United Kingdom** is working with local company Netcraft on cyber security initiatives.[31] This includes combatting phishing and malware hosted in the United Kingdom as well as phishing targeting the government[32]. The partnership helped stop 34,550 potential attacks on government departments in the last six months of 2016, or 200 incidents a day.

7.5.5 Interagency partnerships

The **United States of America** started its first cross-government security information sharing agreement in 2015. The Multilateral Information Sharing Agreement (MISA) binds government agencies from defence, health, justice, intelligence community and energy to work collaboratively to enhance cybersecurity information sharing, with an emphasis on information exchanges at machine speed[33].

South Africa established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. The hub enhances interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society[34].

[31] https://news.netcraft.com/archives/2016/11/01/the-chancellor-of-the-exchequer-sets-out-plans-for-the-uk-government-to-work-with-netcraft.html

[32] https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

[33] https://www.ise.gov/blog/kshemendra-paul/coordinating-cybersecurity-programs

[34] https://www.cybersecurityhub.gov.za/

8 Conclusion

Cybersecurity is an increasingly important part of our life today, and the degree of interconnectivity of networks implies that anything and everything can be exposed, and everything from national critical infrastructure to our basic human rights can be compromised. Governments are therefore urged to consider policies that support continued growth in technology sophistication, access and security, and as a crucial first step, to adopt a national cybersecurity strategy.

The GCI 2017 edition measured the commitment of the ITU Member States to cybersecurity and highlighted a number of illustrative practices from around the world. As a logical continuation of the first iteration of the GCI issued in 2014, this version has motivated countries to improve their work related to cybersecurity, raised awareness in countries for the need to start bilateral, multilateral and international cooperation, and increased the visibility of what countries are doing to improve cybersecurity.

However, the research also revealed that while increased Internet access and more mature technological development is correlated with improvement in cybersecurity at the global level, this is not necessarily true for countries with developing economies and lower levels of technological development. The data collection shows that developing countries lack well-trained cybersecurity experts as well as a thorough appreciation and the necessary education on cybersecurity issues for law enforcement, and continued challenges in the judiciary and legislative branches. There is a need for the developed world to help train local experts in cybersecurity, and more cooperation should be initiated between developed and developing countries to assist them in cybersecurity development.

For the Global Cybersecurity Index to have an impact on raising awareness on this crucial emerging concern over time, continuity of the GCI effort is essential. ITU therefore welcomes all Member States and industry stakeholders to actively participate in future efforts to enhance the current reference model. As well, the success of future iterations of the GCI largely depends on the engagement of Member States and the quality of their responses to the questionnaire, and ITU calls on all Member States to take part in the next GCI survey.

ITU would like to thank all Member States for their valuable support for the conduct of the GCI survey and the publication of this report as well as future ones.

Abbreviations

CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CIIP	Critical Information Infrastructure Protection
CIS	Commonwealth of Independent States
CREST	Council of Registered Ethical Security Testers
CSIRT	Computer Security Incident Response Team
COP	Child Online Protection
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GOVCERT	Governmental Computer Emergency Response Team
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
ITU	International Telecommunication Union
ISP	Internet Service Provider
NCS	National Cybersecurity Strategy
UN	United Nations
R&D	Research and Development
NATO	North Atlantic Treaty Organization
NAFTA	North American Free Trade Association
PIPEDA	Personal Information Protection and Electronic Documents Act
ANSSI	National Agency for Information System Security
ISCB	Information Security Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification
MTPS	Malaysia Trustmark for Private Sector
NCSC	The National Cyber Security Centre
BMBF	Federal Ministry of Education and Research
ISACA	Information Systems Audit and Control Association
ICP	Internet Content Provider
IASPs	Internet Access Service Provider
NCSC	Nation Cyber Security Centre
MSIP	Ministry of Science, ICT and Future Planning

IDI	ICT Development Index
GDP	Gross Domestic Product
FINCSIRT	Financial Sector Computer Security Incident Response Team
KISA	Korea Internet and Security Agency
IIROC	The Investment Industry Regulatory Organization of Canada
CERT-MU	Computer Emergency Response Team of Mauritius
National KE-CIRT/CC	National Kenya Computer Incident Response Team Coordination Centre
AfricaCERT	Computer Emergency Response Team of Africa
AusCERT	Computer Emergency Response Team of Australia
GOVCERT.LU	Government Computer Emergency Response Team of Luxembourg
NCERT.LU	National Computer Emergency Response Team of Luxembourg
OCERT	Oman Computer Emergency Response Team
APCERT	Asia and the Pacific Computer Emergency Response Team

Annex 1 – ITU Member States Global Cybersecurity Commitment Score By Region

AFRICA Region	Score	Global Rank
Mauritius	0.830	6
Rwanda	0.602	36
Kenya	0.574	45
Nigeria	0.569	46
Uganda	0.536	50
South Africa	0.502	58
Botswana	0.430	69
Côte d'Ivoire	0.416	74
Cameroon	0.413	75
Ghana	0.326	87
Tanzania	0.317	88
Senegal	0.314	89
Zambia	0.292	91
Ethiopia	0.267	99
Togo	0.218	107
Burkina Faso	0.208	108
Mozambique	0.206	109
Zimbabwe	0.192	113
Seychelles	0.184	115
Niger	0.170	120
Madagascar	0.168	121
Liberia	0.149	124
Sierra Leone	0.145	126
Gabon	0.139	128
Gambia	0.136	130
Burundi	0.120	135
Lesotho	0.094	143
Guinea	0.090	144

AFRICA Region	Score	Global Rank
Malawi	0.084	145
Angola	0.078	146
Eritrea	0.076	147
Chad	0.072	148
Benin	0.069	149
South Sudan	0.067	150
Namibia	0.066	151
Mali	0.060	152
Cape Verde	0.058	153
Swaziland	0.041	160
Congo	0.040	161
Democratic Republic of the Congo	0.040	161
Sao Tome and Principe	0.040	161
Guinea-Bissau	0.034	162
Central African Republic	0.007	164
Equatorial Guinea	0.000	165

AMERICAS Region	Score	Global Rank
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	62
Argentina	0.482	63
Ecuador	0.466	66
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81

AMERICAS Region	Score	Global Rank
Jamaica	0.339	85
Costa Rica	0.336	86
Paraguay	0.326	87
Barbados	0.273	95
Guyana	0.269	98
El Salvador	0.208	108
Saint Vincent and the Grenadines	0.189	114
Belize	0.182	116
Antigua and Barbuda	0.179	117
Dominican Republic	0.162	122
Suriname	0.155	132
Nicaragua	0.146	125
Bahamas	0.137	129
Bolivia	0.122	134
Grenada	0.115	137
Guatemala	0.114	138
Trinidad and Tobago	0.098	141
Saint Kitts and Nevis	0.066	151
Cuba	0.058	153
Saint Lucia	0.053	156
Honduras	0.048	157
Haiti	0.040	161
Dominica	0.010	163

ARAB STATES Region	Score	Global Rank
Oman	0.871	4
Egypt	0.772	14
Qatar	0.676	25
Tunisia	0.591	40
Saudi Arabia	0.569	46

ARAB STATES Region	Score	Global Rank
United Arab Emirates	0.566	47
Morocco	0.541	49
Bahrain	0.467	65
Algeria	0.432	68
Jordan	0.277	93
Sudan	0.271	96
Syrian Arab Republic	0.237	102
State of Palestine	0.228	104
Libya	0.224	105
Lebanon	0.172	119
Mauritania	0.146	125
Kuwait	0.104	139
Djibouti	0.099	140
Iraq	0.043	159
Comoros	0.040	161
Somalia	0.034	162
Yemen	0.007	164

COMMONWEALTH OF INDEPENDANT STATESCIS Region	Score	Global Rank
Georgia	0.819	8
Russian Federation	0.788	10
Belarus	0.592	39
Azerbaijan	0.559	48
Ukraine	0.501	59
Moldova	0.418	73
Kazakhstan	0.352	83
Tajikistan	0.292	91
Uzbekistan	0.277	93
Kyrgyzstan	0.270	97
Armenia	0.196	111
Turkmenistan	0.133	132

ASIA AND THE PACIFIC Region	Score	Global Rank
Singapore	0.925	1
Malaysia	0.893	3
Australia	0.824	7
Japan	0.786	11
Republic of Korea	0.782	13
New Zealand	0.718	19
Thailand	0.684	20
India	0.683	23
China	0.624	32
Philippines	0.594	37
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Iran	0.494	60
Pakistan	0.447	67
Indonesia	0.424	70
Sri Lanka	0.419	72
Lao	0.392	77
Tonga	0.292	91
Cambodia	0.283	92
Nepal	0.275	94
Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Mongolia	0.228	104
Fiji	0.222	106
Bhutan	0.199	110
Nauru	0.140	127
Vanuatu	0.134	131
Kiribati	0.123	133
Solomon Islands	0.095	142

ASIA AND THE PACIFIC Region	Score	Global Rank
Papua New Guinea	0.067	150
Maldives	0.056	155
Palau	0.053	156
Samoa	0.048	157
Marshall Islands	0.048	157
Micronesia	0.044	158
Timor-Leste	0.034	162
Tuvalu	0.034	162

EUROPE Region	Score	Global Rank
Estonia	0.846	5
France	0.819	8
Norway	0.786	11
United Kingdom of Great Britain and Northern Ireland	0.783	12
Netherlands	0.760	15
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
Israel	0.691	20
Latvia	0.688	21
Germany	0.679	24
Ireland	0.675	26
Belgium	0.671	27
Austria	0.639	30
Italy	0.626	31
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35
Luxembourg	0.602	36
Croatia	0.590	41

EUROPE Region	Score	Global Rank
Romania	0.585	42
Turkey	0.581	43
Bulgaria	0.579	44
Hungary	0.534	51
Spain	0.519	54
The Former Yugoslav Republic of Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
Cyprus	0.487	61
Greece	0.475	64
Montenegro	0.422	71
Malta	0.399	76
Iceland	0.384	78
Slovakia	0.362	82
Slovenia	0.343	84
Albania	0.314	89
Serbia	0.311	90
Monaco	0.236	103
Liechtenstein	0.194	112
San Marino	0.174	118
Bosnia and Herzegovina	0.116	136
Andorra	0.057	154
Vatican	0.040	161

Annex 2 – GCI 2017 Score

Member State	Score	Global Rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.830	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10
Japan	0.786	11
Norway	0.786	11
United Kingdom	0.783	12
Republic of Korea	0.782	13
Egypt	0.772	14
Netherlands	0.760	15
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
New Zealand	0.718	19
Israel	0.691	20
Latvia	0.688	21
Thailand	0.684	20
India	0.683	23
Germany	0.679	24
Qatar	0.676	25
Ireland	0.675	26
Belgium	0.671	27

Member State	Score	Global Rank
Mexico	0.660	28
Uruguay	0.647	29
Austria	0.639	30
Italy	0.626	31
China	0.624	32
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35
Rwanda	0.602	36
Luxembourg	0.602	36
Philippines	0.594	37
Brazil	0.593	38
Belarus	0.592	39
Tunisia	0.591	40
Croatia	0.590	41
Romania	0.585	42
Turkey	0.581	43
Bulgaria	0.579	44
Kenya	0.574	45
Colombia	0.569	46
Saudi Arabia	0.569	46
Nigeria	0.569	46
United Arab Emirates	0.566	47
Azerbaijan	0.559	48
Morocco	0.541	49
Uganda	0.536	50
Hungary	0.534	51
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Spain	0.519	54

Member State	Score	Global Rank
The Former Yugoslav Republic of Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
South Africa	0.502	58
Ukraine	0.501	59
Iran	0.494	60
Cyprus	0.487	61
Panama	0.485	62
Argentina	0.482	63
Greece	0.475	64
Bahrain	0.467	65
Ecuador	0.466	66
Pakistan	0.447	67
Algeria	0.432	68
Botswana	0.430	69
Indonesia	0.424	70
Montenegro	0.422	71
Sri Lanka	0.419	72
Moldova	0.418	73
Côte d'Ivoire	0.416	74
Cameroon	0.413	75
Malta	0.399	76
Lao	0.392	77
Iceland	0.384	78
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81
Slovakia	0.362	82
Kazakhstan	0.352	83
Slovenia	0.343	84
Jamaica	0.339	85

Member State	Score	Global Rank
Costa Rica	0.336	86
Ghana	0.326	87
Paraguay	0.326	87
Tanzania	0.317	88
Senegal	0.314	89
Albania	0.314	89
Serbia	0.311	90
Zambia	0.292	91
Tajikistan	0.292	91
Tonga	0.292	91
Cambodia	0.283	92
Uzbekistan	0.277	93
Jordan	0.277	93
Nepal	0.275	94
Barbados	0.273	95
Sudan	0.271	96
Kyrgyzstan	0.270	97
Guyana	0.269	98
Ethiopia	0.267	99
Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Syrian Arab Republic	0.237	102
Monaco	0.236	103
Mongolia	0.228	104
State of Palestine	0.228	104
Libya	0.224	105
Fiji	0.222	106
Togo	0.218	107
Burkina Faso	0.208	108
El Salvador	0.208	108

Member State	Score	Global Rank
Mozambique	0.206	109
Bhutan	0.199	110
Armenia	0.196	111
Liechtenstein	0.194	112
Zimbabwe	0.192	113
Saint Vincent and the Grenadines	0.189	114
Seychelles	0.184	115
Belize	0.182	116
Antigua and Barbuda	0.179	117
San Marino	0.174	118
Lebanon	0.172	119
Niger	0.170	120
Madagascar	0.168	121
Dominican Republic	0.162	122
Suriname	0.155	132
Liberia	0.149	124
Mauritania	0.146	125
Nicaragua	0.146	125
Sierra Leone	0.145	126
Nauru	0.140	127
Gabon	0.139	128
Bahamas	0.137	129
Gambia	0.136	130
Vanuatu	0.134	131
Turkmenistan	0.133	132
Kiribati	0.123	133
Bolivia	0.122	134
Burundi	0.120	135
Bosnia and Herzegovina	0.116	136
Grenada	0.115	137
Guatemala	0.114	138

Member State	Score	Global Rank
Kuwait	0.104	139
Djibouti	0.099	140
Trinidad and Tobago	0.098	141
Solomon Islands	0.095	142
Lesotho	0.094	143
Guinea	0.090	144
Malawi	0.084	145
Angola	0.078	146
Eritrea	0.076	147
Chad	0.072	148
Benin	0.069	149
South Sudan	0.067	150
Papua New Guinea	0.067	150
Saint Kitts and Nevis	0.066	151
Namibia	0.066	151
Mali	0.060	152
Cape Verde	0.058	153
Cuba	0.058	153
Andorra	0.057	154
Maldives	0.056	155
Saint Lucia	0.053	156
Palau	0.053	156
Honduras	0.048	157
Samoa	0.048	157
Marshall Islands	0.048	157
Micronesia	0.044	158
Iraq	0.043	159
Swaziland	0.041	160
Congo	0.040	161
Democratic Republic of the Congo	0.040	161
Haiti	0.040	161

Member State	Score	Global Rank
Sao Tome and Principe	0.040	161
Vatican	0.040	161
Comoros	0.040	161
Guinea-Bissau	0.034	162
Somalia	0.034	162
Timor-Leste	0.034	162
Tuvalu	0.034	162
Dominica	0.010	163
Central African Republic	0.007	164
Yemen	0.007	164
Equatorial Guinea	0.000	165

**International
Telecommunication
Union**

Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN: 978-92-61-25071-3

9 789261 250713

Printed in Switzerland
Geneva, 2017

Photo credits: Shutterstock