

# Global Cybersecurity Index (GCI)

2018

Draft





# Global Cybersecurity Index 2018

The Global Cybersecurity Index (GCI) is an initiative of the International Telecommunication Union (ITU) involving experts from different backgrounds and organizations. The ICT Applications and Cybersecurity Division would like to acknowledge and thank all partners and contributors for their hard work and commitment in providing support to the GCI, and more importantly, to fulfilling the mission and realizing the 2018 vision of GCI.

The cybersecurity team would therefore like to highlight the contributions of the following experts and individuals from Member States who provided support in assigning a weighting to each indicator and question: Ms. Vanessa Copetti Cravo from Brazil (ANATEL), Ms. Gabriel Gallegos and Mr Boris Castro Armas from Ecuador (Ministry), Mr Danila D'Elia from ECSO, Mr Serge Droz from FIRST, Mr Luc Dandurand from GuardTime, Mr Mohammad Alsalamini from Jordan (Ministry), Dr Jaesuk Yun from Korea (KISA), Ms. Aziza Al-Rashidi from Oman (Ministry), Ms. Natalija Radoja and Mr Milan Vojvodic from Serbia (Ministry), Mr Sebastian Xu and Mr Kai Ling Lee from Singapore (Ministry), Ms. Marie Humeau and Ms. Jenny Crisp from the United Kingdom Mission, Mr Deniz Susar from UNDESA, Ms. Francesca Bosco and Mr Marco Musumeci from UNICRI.

ITU would also like to thank Grace Rachael Acayo, Lisa Jaccoud, Lena Lattion, and Yaroslava Mikhaylova for their support in the initial preparation, online questionnaire, primary data collection, data validation and report elaboration.

Please contact the ITU cybersecurity team at [cybersecurity@itu.int](mailto:cybersecurity@itu.int) should you have any comments or inquiries with respect to this publication.



**Please consider the environment before printing this report.**

© ITU 2018

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

# Executive Summary

---

The Global Cybersecurity Index (GCI) is a composite index produced, analysed and published by the International Telecommunication Union (ITU) to measure the commitment of ITU Member States to cybersecurity in order to raise cybersecurity awareness.

The GCI is rooted in the ITU Global Cybersecurity Agenda (GCA) that was launched in 2007, and reflects its five pillars: legal, technical, organizational, capacity building, and cooperation. The GCI combines 25 indicators into one benchmark measure to monitor the cybersecurity commitment of 194 ITU Member States (including the State of Palestine) to the five pillars endorsed by the Global Cybersecurity Agenda (GCA).

The index uses data collected through an online survey. For each pillar, questions have been developed to assess commitment. Through consultation with a group of experts, the questions are weighted in order to generate an overall GCI score.

The overall result shows improvement and strengthening of all five pillars of the cybersecurity agenda in various countries in all regions. It should be noted, however, that the gap in the level of cybersecurity engagement between different regions is still present and visible. Besides providing the GCI score, this report also provides information on national practices that give insight to the progress achieved.



# Table of Contents

Executive Summary	iii
Important notice on the ranking	vii
1 Introduction	1
2 GCI scope and framework	2
2.1 Background	2
2.2 Reference model	2
2.3 Conceptual framework	2
3 Methodology	5
4 Key findings	8
4.1 Heat map of national cybersecurity commitment	8
4.2 GCI groups	8
5 Global outlook	11
5.1 A selection of noteworthy indicators	12
5.2 Comparing GCI with other indices	14
6 Regional outlook	18
6.1 Africa	19
6.2 Americas	20
6.3 Arab States	21
6.4 Asia Pacific	22
6.5 Commonwealth of Independent States	23
6.6 Europe	24
6.7. The commitment level per pillar in the six regions	25
7 Conclusion	42
List of abbreviations	44
Annex A: Regional ranking GCI 2018	45
Annex B: Global ranking GCI 2018	52
Annex C: Definition of indicators	59
Annex D: Computational details	64
Annex E: Index of cybersecurity indices 2018	66
E.1 Definitions	66
E.2 Indices for assessing countries	67
E.3 Indices for assessing organizations	74
E.4 Indices for assessing other aspects	76





# Important notice on the ranking

The reader may notice variations between ranking in this report and previous rankings. This is due to the following changes:

- The questionnaire has been modified after a number of meetings and discussions based on membership comments and expert views. This has led to a restructured content with fewer questions, from 153 to 50 questions.
- An expert working group re-evaluated and modified weighting values, based on the changes introduced to the questionnaire.
- The GCI scoring relies on responses to the questionnaire. However, the GCI team also researches and collects data to add accuracy to the survey countries are encouraged to share specificities of their country (for example, the option of “other”), and best practices (best practices/ achievements/progress also carry points). The level of participation and quality of answers, in addition to the ITU research and data collection, adds accuracy to the survey.
- IMPACT and HIPPSA projects have been closed and have no further impact on ranking/score variations.
- Draft versions of documents are no longer considered as 100 per cent of the score weighting, in the 2018 index, drafts carry only 50 per cent.
- The question related to national best practices was dropped from consideration due to the low response rate.
- Elements on child online protection were included in the scoring.
- Overall, Europe region countries have improved rankings due to initiatives such as the European Union (UE) certification framework for ICT security products, the implementation of the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive).



## 1 Introduction

More than half of the world's population is currently online. By the end of 2018, 51.2 per cent of individuals, equivalent to 3.9 billion people, were using the Internet. This is a significant step towards a more inclusive global information society but also an important need for increased cyber protection. According to the ITU Connect 2030<sup>1</sup>, there will be 70 per cent Internet penetration by 2023, increasing the need for a more cyber-secure space.

Studies show the global average cost of a data breach was up 6.4 per cent in 2018<sup>2</sup>. At the same time due to the boost in the use of ICTs, the projected cybercrime cost will be an estimated USD 2 trillion by the end of 2019<sup>3</sup>. There has been less ransomware attacks, but more personal data breaches and critical infrastructure breaches, and this included hundreds of universities<sup>4</sup>.

In addition, there is still a visible gap between many countries in terms of knowledge for the implementation of cybercrime legislation, national cybersecurity strategies (NCS), computer emergency response teams (CERTs), awareness and capacity to spread out the strategies, and capabilities and programmes in the field of cybersecurity. Sustainable development in this area should ensure the resilient and adequate use of ICTs as well as economic growth.

This report reviews the cybersecurity commitment and situation in all the ITU regions: Africa, Americas, Arab States, Asia-Pacific, CIS, and Europe, and puts Member States with high commitment and commendable practices in the spotlight.

The methodology used to produce the GCI is explained in more detail in the main content of the report. The scoring process was done in collaboration with a panel of experts.

<sup>1</sup> <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf>

<sup>2</sup> <https://www.ibm.com/security/data-breach>

<sup>3</sup> <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#1fec52ac3a91>

<sup>4</sup> <https://www.wired.com/story/2018-worst-hacks-so-far/>

## 2 GCI scope and framework

### 2.1 Background

The Global Cybersecurity Index (GCI) is included under ITU Plenipotentiary Resolution 130 (Rev. Dubai, 2018) on strengthening the role of ITU in building confidence and security in the use of information and communication technologies. 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”. The ultimate goal is to foster a global culture of cybersecurity and its integration at the core of information and communication technologies.

The first GCI survey was conducted in 2013/2014 in partnership with ABI Research where a total of 105 countries responded out of 193 ITU Member States and the final results were published in 2015: See [www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx).

Following feedback received from various communities and Member States, a second GCI survey was prepared in 2016 with a total number of 134 participants and the final results published in 2017: See [www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx).

The GCI is formulated around the data provided by the ITU membership, including interested individuals, experts and industry stakeholders as contributing partners such as Australia Strategic Policy Institute, FIRST (Forum for Incident Response and Security Team), Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet and Security Agency, NTRA Egypt, Red Team Cyber, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica, UNODC, and the World Bank.

### 2.2 Reference model

The Global Cybersecurity Index (GCI) is a composite index combining 25 indicators into one benchmark to monitor and compare the level of the cybersecurity commitment of Member States with regard to the five pillars of the Global Cybersecurity Agenda (GCA). These pillars form the five sub-indices of GCI. The main objectives of GCI are to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- progress in cybersecurity commitment of all countries from a global perspective;
- 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 initiatives).






The goal of the GCI is to help countries identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide. Through the collected information, GCI aims to illustrate the practices of others so that Member States can implement selected aspects suitable to their national environment, with the added benefit of helping to harmonize practices, and foster a global culture of cybersecurity.

### 2.3 Conceptual framework

The ITU framework for international multi-stakeholder cooperation in cybersecurity aims to build synergies between current and future initiatives, and focuses on the following five pillars:

1. Legal: Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.

Figure 2.3.1: GCI 2018 indicators per pillar

<b>Legal Measures</b> Cybercrime legislation Cybersecurity regulation Containment/curbing of spam legislation	
<b>Technical Measures</b> CERT/CIRT/CSIRT Standards Implementation Framework Standardization Body Technical mechanisms and capabilities deployed to address spam Use of cloud for cybersecurity purpose Child Online Protection Mechanisms	
<b>Organizational Measures</b> National strategy Responsible Agency Cybersecurity Metrics	
<b>Capacity Building Measures</b> Public awareness campaigns Framework for the certification and accreditation of cybersecurity professionals Professional training courses in cybersecurity Educational programs or academic curricular in cybersecurity Investment in cybersecurity R&D programs Incentive mechanisms Home-grown cybersecurity industry	
<b>Cooperation Measures</b> Bilateral agreements Multilateral agreements Participation of international fora/associations Public-private partnerships Inter-agency/intra-agency partnerships Best practices	

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

These five designated areas form the basis of the indicators for GCI because they shape the inherent building blocks of a national cybersecurity culture.

Cybersecurity has a field of application that cuts across all industries, all sectors, both vertically and horizontally. In order to increase the development of national capabilities, efforts have to be made by political, economic and social forces. This can be done by law enforcement, justice departments, educational institutions, ministries, private sector operators, developers of technology, public private partnerships, and intra-state cooperation considering the long-term aim to increase efforts in the adoption and integration of cybersecurity on a global scale.

**Legal:** Legal measures (including legislation, regulation and containment of spam legislation) authorize a nation state to set up basic response mechanisms through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. A legislative framework sets the minimum foundation of behaviour on which further cybersecurity capabilities can be built. Fundamentally, the objective is to have sufficient legislation in place in order to harmonize practices at the regional/international level, and simplify international combat against cybercrime. The legal

context is evaluated based on the number of legal institutions and frameworks dealing with cybersecurity and cybercrime.

**Technical:** Technology is the primary frontier of defense against cyber threats (including the use of computer emergency or incident response teams, standards implementation framework, technical mechanisms and capabilities deployed to address spam, child online protection, etc). Without suitable technical skills to detect and respond to cyber attacks, Member States remain vulnerable. Efficient ICT development and use can only truly prosper in an environment of trust and security. Member States therefore need to build and install accepted minimum-security criteria and accreditation schemes for software applications and systems. These efforts need to be complemented by the creation of a national body with the aim of dealing with cyber incidents, an authoritative government entity and a national framework to watch, warn, and respond to incidents. Technical elements are evaluated based on the number of practical mechanisms to deal with cybersecurity.

**Organizational:** Organizational measures (including national strategies, responsible agencies, cybersecurity metrics) are indispensable for the proper implementation of any national initiative. Broad strategic targets and goals need to be set by the nation state, along with an all-inclusive plan in implementation, delivery, and measurement. National agencies must be present to implement the strategy and evaluate the outcome. Without a national strategy, governance model, and supervisory body, efforts in different sectors become conflicted, preventing efforts to obtain an effective harmonization in cybersecurity development. The organizational structures are evaluated based on the presence of institutions and strategies involving cybersecurity development at the national level.

**Capacity building:** Capacity building (including public awareness campaigns, framework for certification and accreditation of cybersecurity professionals, professional training courses in cybersecurity, educational programmes or academic curricula, etc.) is intrinsic to the first three pillars (legal, technical and organizational). Cybersecurity is most often tackled from a technological perspective even though there are numerous socio-economic and political implications. Human and institutional capacity building is essential to raise awareness, knowledge and the know-how across sectors, for systematic and appropriate solutions, and to promote the development of qualified professionals. Capacity building is evaluated based on the number of research and development, education and training programmes, and certified professionals and public sector agencies.

**Cooperation:** Cybercrime is a global problem and is unrestricted to national borders or sectoral distinctions. As such, tackling cybercrime requires a multi-stakeholder approach with inputs from all sectors and disciplines (including bilateral and multilateral agreements, participation of international fora/associations, public-private partnerships, inter-agency partnerships, best practice, etc.). Greater cooperation can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats and enable better investigation, apprehension and prosecution of malicious agents. National and international cooperation is evaluated based on the number of partnerships, cooperative frameworks and information sharing networks.

### 3 Methodology

The questionnaire used for the 2018 GCI provides a value for the 25 indicators constructed through 50 binary, pre-coded, and open-ended questions. This achieves the required level of granularity and improves the accuracy and quality of the answers. A detailed definition of each indicator is provided in Annex A.

The indicators used to calculate the GCI were selected on the basis of the following criteria:

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

The concept of the GCI is based on a cybersecurity development map with pre-coded and binary answers that define possible paths, and which a country might take into account in order to enhance their cybersecurity commitment. Each of the five pillars have a specific colour. The depth of the path indicates a higher development level of commitment.

Figure 3.1: GCI/GCA mapping of the organizational pillar

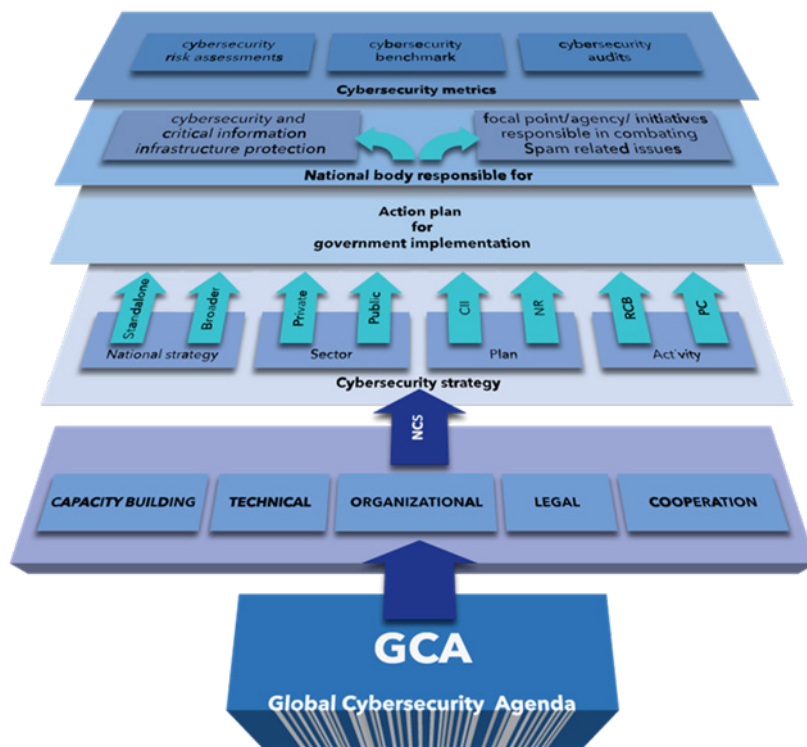


Figure 3.1 illustrates the relationship between the GCA, the pillars, indicators, and questions (expanded only for the organizational pillar illustrating the need for policy coordination institutions and strategies for cybersecurity development at the national level).

The various levels of cybersecurity development among Member States, as well as different cybersecurity needs reflected by national ICT development status, were taken into consideration. The concept is based on an assumption that the more developed cybersecurity is, the more complex the solutions will be. Therefore, the further a country goes along the path for each pillar by confirming

the presence of pre-identified cyber solutions, the more comprehensive and sophisticated the cybersecurity development will be within that country, allowing it to get a higher GCI score.

Using binary answers eliminates opinion-based evaluation and any possible bias towards certain types of answers. The pre-coded answers save time and allow a more accurate data analysis. Moreover, a simple binary concept allows quicker and more complex evaluation as it does not require lengthy answers, which accelerates and streamlines the process of providing answers and further evaluation. The respondent should only confirm presence of, or lack of, certain pre-identified cybersecurity solutions. An online survey mechanism, which is used for gathering answers and uploading relevant material, enables the extraction of good practice, and a set of thematic qualitative evaluations by a panel of experts.

The key difference in methodology from the previous GCI surveys is that the structure has been modified to questions with pre-defined answers including free text and open-ended questions in every section of the questionnaire. Multiple choice questions (multiple answers) have been included to allow Member States to simply tick the boxes that apply to them.

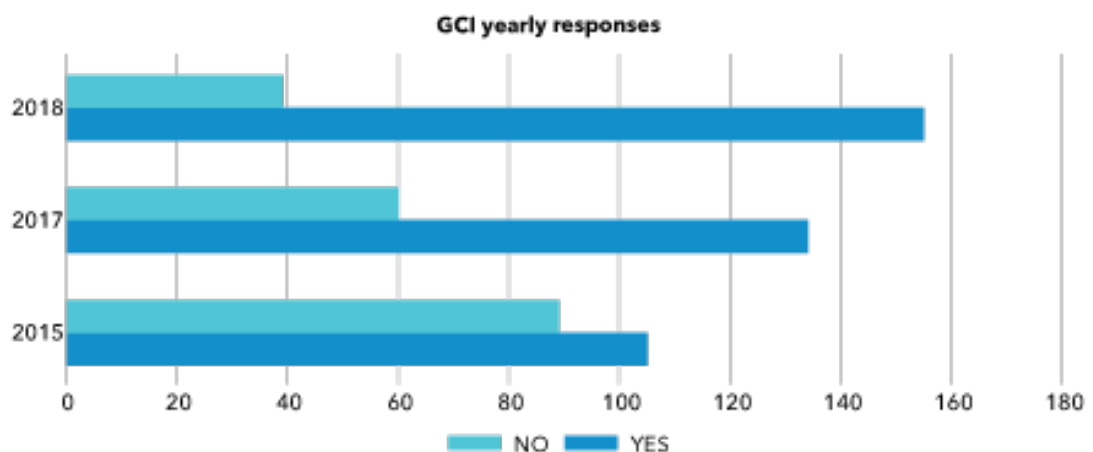
The pre-coded answers require a box to be ticked, saving the respondent time when writing the answers. The option to add further details has also been provided in order for Member States to complement specific information that might not have been captured in the pre-defined answers.

Furthermore, partial answers have been included, to capture *work in progress* material (such as approved drafts of documents, or advanced stage of development of capabilities), in order to ensure that countries are properly ranked. A feature of uploading supporting documents and URLs has also been added as a way to provide proof, accuracy, and more information to substantiate the pre-coded response. A number of questions have been removed or re-defined and new questions have been added in each of the five pillars to refine precision and increase the depth of research.

The scoring process is carried out by a panel of experts who give a weighting for each question. An average of all expert input constitutes the final weighting used to rank the Member States.

This year, the process was improved as a panel of 32 experts (up from 10 previously) met at ITU headquarters, with some experts participating remotely. The experts were given a full explanation of the working process of the GCI, a copy of the questionnaire, an excel sheet to assign their weighting. They were also asked to share their comments and points of view on the questions to further improve the survey. The GCI team came up with the detailed computation of the sub-indices, and the final weighting used for scoring and ranking (see Annex D).

Figure 3.2: Improvement of the GCI responses received since the start of the project in 2015





Apart from building the index, open ended questions have been included in the questionnaire to cater for additional requirements from ITU-D Study Group 2 Question 3 that do not fit within GCI computation. The questionnaire is made available through an online survey for a specific period of time to allow Member States to answer the questionnaire and provide supporting information.

Out of 194 ITU Member States, only 54 per cent participated in GCI in 2015: the survey in 2017 increased to 69 per cent, and in 2018, about 80 per cent provided a focal point to the GCI.

**The overall GCI process is implemented as follows:**

1. A letter of invitation is sent to all ITU Member States, informing them of the initiative and requesting a focal point responsible for collecting all relevant data and for completing the online GCI questionnaire.

During the online survey, the approved focal point is officially invited by ITU to answer the questionnaire.

2. Primary data collection (for countries that do not respond to the questionnaire):
  - ITU elaborates an initial draft response to the questionnaire using publicly available data and online research.
  - The draft questionnaire is sent to focal points for review.
  - Focal points improve the accuracy and returns the draft questionnaire.
  - The corrected draft questionnaire is sent to each focal point for final approval.
  - The validated questionnaire is used for analysis, scoring, and ranking.
3. Secondary data collection (for countries that respond to the questionnaire):
  - ITU identifies any missing responses, supporting documents, links, etc.
  - The focal point improves the accuracy of the responses where necessary.
  - The corrected draft questionnaire is sent to each focal point for final approval.
  - The validated questionnaire is used for analysis, scoring and ranking.

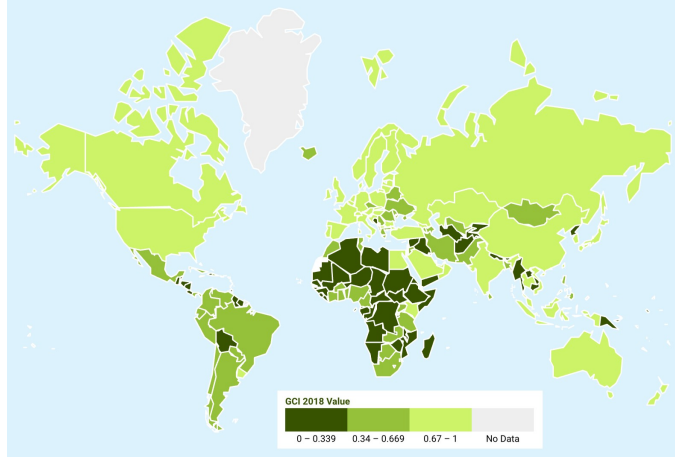
Note: Should a Member State not provide a focal point for the GCI questionnaire, ITU will establish contact with the institutional focal point in the ITU Global Directory.<sup>1</sup>

<sup>1</sup> <https://www.itu.int/online/mm/scripts/gense18>

## 4 Key findings

### 4.1 Heat map of national cybersecurity commitment

Figure 4.1: Heat map showing geographical commitment around the world



### 4.2 GCI groups

Member States are classified according to their level of commitment: high, medium, and low.




1.  Countries that demonstrate high commitment in all five pillars of the index.
2.  Countries that have developed complex commitments and engage in cybersecurity programmes and initiatives.
3.  Countries that have started to initiate commitments in cybersecurity.

Table 4.2: Level of commitment

The level of commitment tables below list the Member States that have maintained high, medium, and low GCI scores. Scores were obtained using the 99 percentile: High countries within this range (1.000-0.670) are ranked (1-51), total 54 countries. Low country scores (0.339-0.000) range in rank from 100-175, with a total of 87 countries.

High		
United Kingdom	Qatar	New Zealand
United States of America	Georgia	Switzerland
France	Finland	Ireland
Lithuania	Turkey	Israel
Estonia	Denmark	Kazakhstan
Singapore	Germany	Indonesia
Spain	Egypt	Portugal
Malaysia	Croatia	Monaco
Norway	Italy	Kenya
Canada	Russian Federation	Latvia
Australia	China	Slovakia
Luxembourg	Austria	Bulgaria
Netherlands	Poland	India
Saudi Arabia	Belgium	Slovenia
Japan	Hungary	Rwanda
Mauritius	Sweden	Viet Nam
Republic of Korea	The former Yugoslav Republic of Macedonia	Uruguay
Oman	Thailand	

Medium		
Uzbekistan	Kuwait	Cote d'Ivoire
Moldova	Bahrain	Iceland
Ukraine	Belarus	Botswana
Azerbaijan	Brazil	Chile
Cyprus	Czech Republic	Ghana
South Africa	Romania	Zambia
Nigeria	Colombia	Cameroon
Philippines	Jordan	Dominican Republic
Serbia	Liechtenstein	Morocco
Tanzania	Tunisia	Argentina
United Arab Emirates	Greece	Pakistan
Iran	Bangladesh	Jamaica
Montenegro	Armenia	Peru
Albania	Benin	Burkina Faso
Mexico	Cuba	Panama
Brunei Darussalam	Malta	Samoa
Uganda	Sri Lanka	Ecuador
Paraguay	Mongolia	Venezuela

Low		
Gabon	Afghanistan	Mali
State of Palestine	Barbados	Timor-Leste
Senegal	Myanmar	San Marino
Sudan	Saint Vincent and the Grenadines	Marshall Islands
Gambia	Congo	Somalia
Ethiopia	Cambodia	South Sudan
Malawi	Mozambique	Saint Kitts and Nevis
Iraq	Bahamas	Sao Tome and Principe
Tajikistan	Grenada	Djibouti
Algeria	Bolivia	Solomon Islands
Nepal	Sierra Leone	Tuvalu
Seychelles	Eswatini	Guinea-Bissau
Kyrgyzstan	Guyana	Cabo Verde
Guatemala	Papua New Guinea	Lesotho
Antigua and Barbuda	Nicaragua	Haiti
Syrian Arab Republic	Belize	Honduras
Costa Rica	Namibia	Micronesia
Tonga	El Salvador	Central African Republic
Liberia	Andorra	Equatorial Guinea
Libya	Turkmenistan	Kiribati
Bosnia and Herzegovina	Suriname	Vatican
Madagascar	Mauritania	Eritrea
Lao	Nauru	Democratic People's Republic of
Fiji	Chad	Korea
Guinea	Vanuatu	Dominica
Trinidad and Tobago	Angola	Yemen
Lebanon	Saint Lucia	Comoros
Zimbabwe	Niger	Democratic Republic of the
Bhutan	Burundi	Congo
	Togo	Maldives

## 5 Global outlook

In 2017, the global commitment level had a distribution in all the six regions of ITU, eliminating geographical theories of commitment. In 2018, only three regions are represented with countries having the most level of commitment: six countries from the Europe region, three from the Asia-Pacific region, and two from the Americas region.

Table 5.1: GCI top ten most committed countries globally in 2018 (normalized score)

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

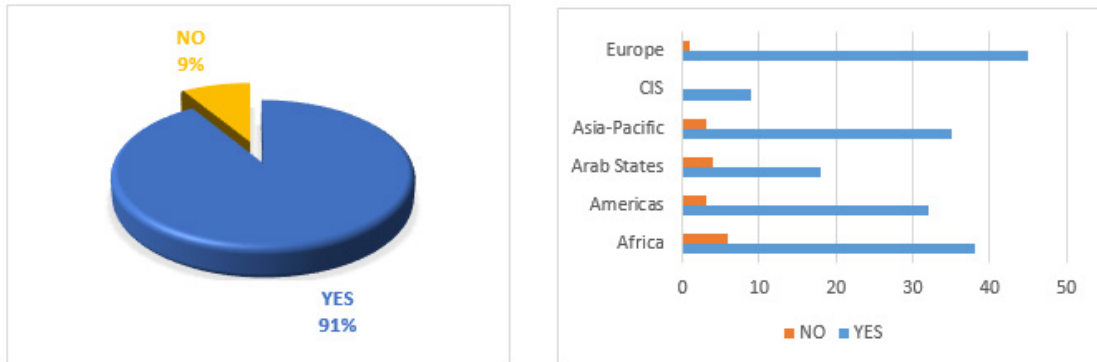
As presented above, there is a wide gap in cyber commitment around the world. This exists within the six regions. Each year, the level of commitment changes according to the information made available to the public, and through the different media and data provided by Member States. The increasing popularity of the GCI among nations has meant that certain countries provided all the relevant documents corresponding to the questionnaire, which resulted in them climbing highly in the ranking. GCI does not measure the level of preparedness of countries to respond to cyber-attacks, being represented in the top ten does not necessarily reflect the actual situation in the country and vice versa. Cybersecurity related commitments are often unequally distributed with countries performing well in some pillars and less so in others.

Information and communications technology (ICT) presents one of the most critical modern challenges to global security. Through the GCI survey, a gap is evident between countries in terms of awareness, understanding, knowledge and capacity to deploy appropriate strategies. With cybersecurity taking centre stage globally, it is imperative that nations all over the world implement solutions to provide a safe space for Internet users in their country and stay engaged to improvement according to the incoming challenges.

The ongoing threats highlights an urgent need for cooperation among Member States to mitigate cybersecurity issues such as cybercrime, cyberattacks on critical infrastructure and offensive operations. Emerging cyber threats could precipitate massive economic and societal damage, and international efforts need to be agreed and acted upon in response to this new trend.

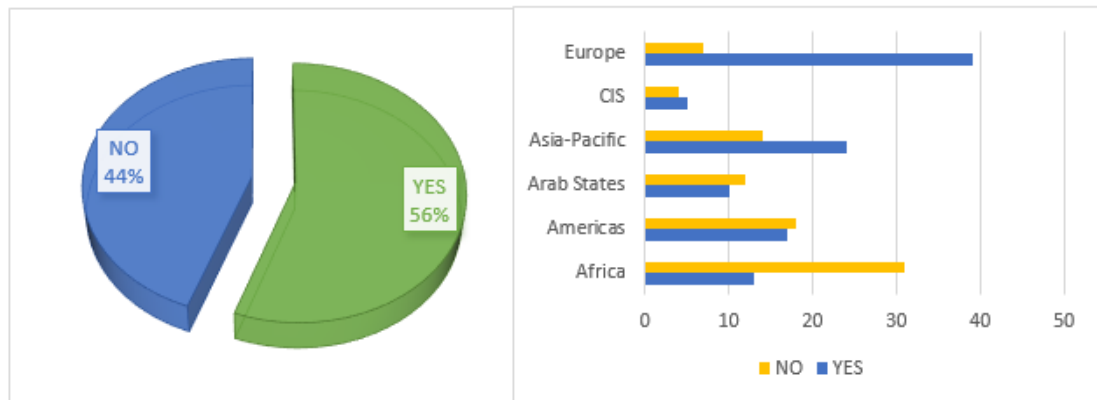
### 5.1 A selection of noteworthy indicators

Figure 5.1.1: Cybercrime legislation per region



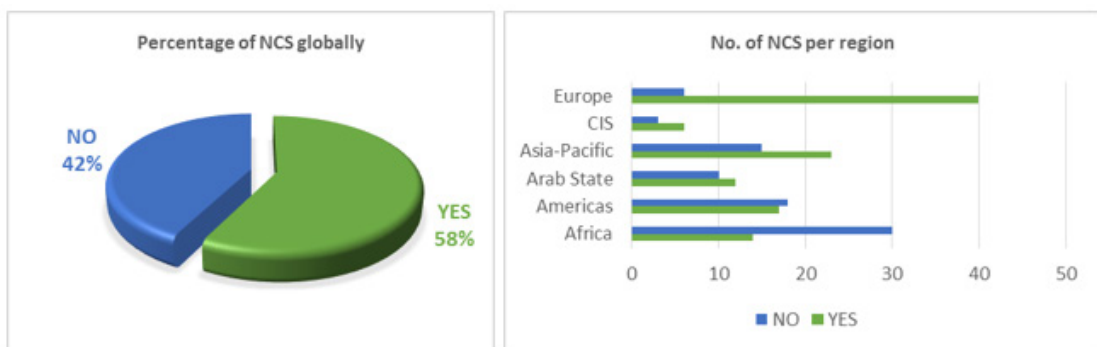
In 2018, cybercrime legislation is globally well implemented. Most countries have cybercrime legislation (91%), which improves on 2017 (79%). But laws should not be adopted and left redundant, governments need to use laws as a framework to implement strategies that ensure government ICT initiatives are sustainable, in compliance with information technology authorities, and enhancing cybersecurity.

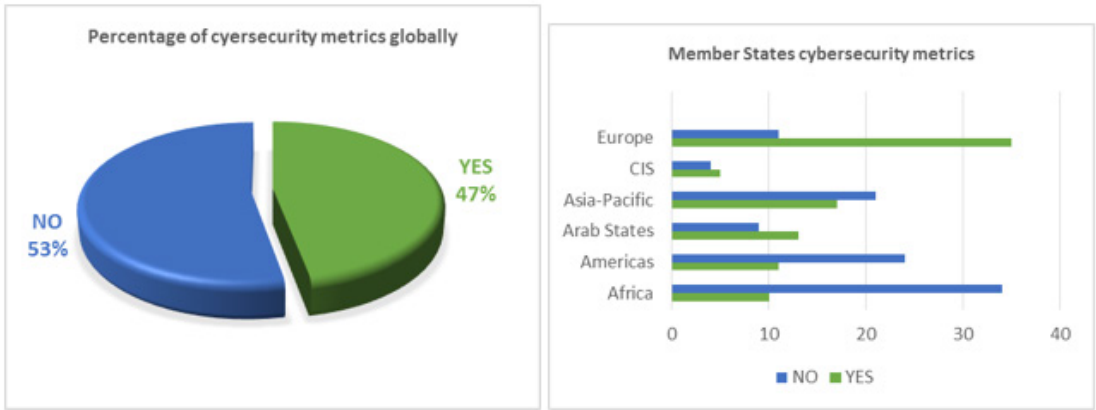
Figure 5.1.2: National CERT/CIRT/CSIRT



The number of countries with a CERT/CIRT/CSIRT has improved since 2017 (50%), with 56 per cent having a CERT/CIRT/CSIRT in 2018. CERTS should be active at all times to help detect attacks on government computer systems and data as well as critical infrastructures.

Figure 5.1.3: National cybersecurity strategy and cybersecurity metrics





In 2018, the majority of countries (58%) reported having a national cybersecurity strategy (NCS), which is an increase from last year (50%), and 47 per cent have metrics to measure cybersecurity development at a national level, which is also an improvement, since in 2017 only 21 per cent had metrics. There is still room for improvement (performance measurement is a key aspect of cybersecurity risk management) through cybersecurity governance and risk management by developing, implementing, monitoring and updating metrics that provide visibility on the performance of key elements of a national cybersecurity programme.

Figure 5.1.4: Awareness campaigns

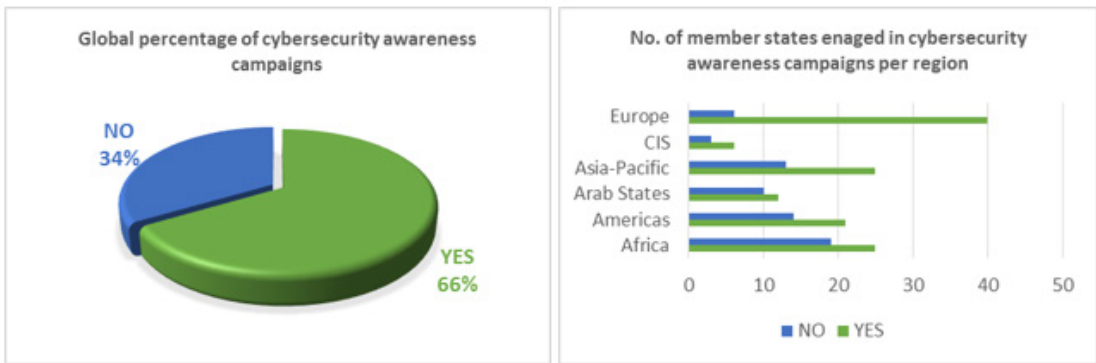
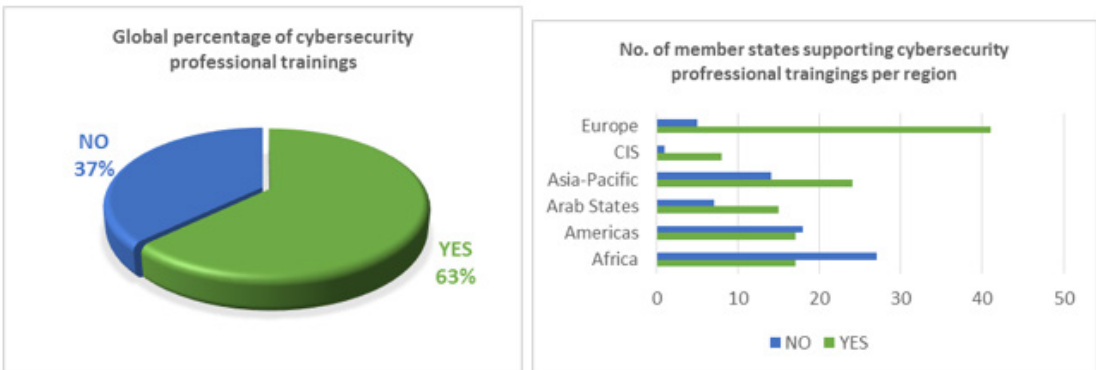


Figure 5.1.5: Professional training



The majority of countries (66%) implement awareness campaigns up from 59 per cent in 2017, in addition to giving professional training courses in cybersecurity (63% vs. 52% in 2017).

Figure 5.1.6: Participation in international forums

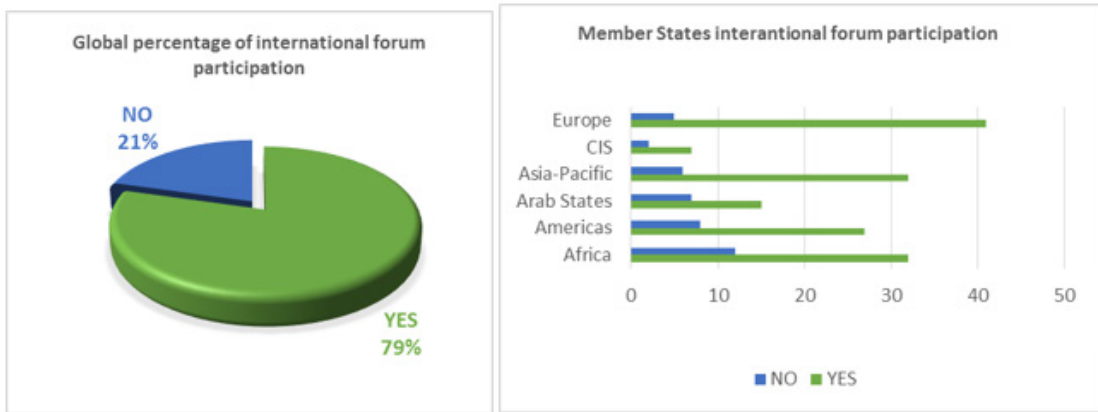
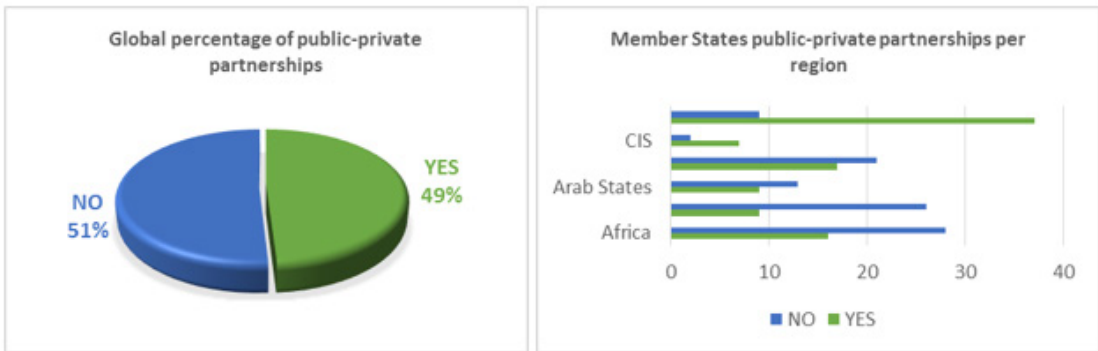


Figure 5.1.7: Public-private partnerships



Participation in international forums and associations dealing with cybersecurity is high (79%). On the other hand, more effort could be made to establish public-private partnerships (only 49 per cent of countries have a public-private partnership cooperative arrangement).

## 5.2 Comparing GCI with other indices

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

This comparison is not intended to provide an exhaustive statistical analysis but it does indicate how cybersecurity can relate to existing national processes, in order to emphasize the importance of considering cybersecurity at every stage of development.

### A The United Nations E-Government Development Index

Comparing GCI to the e-government development index does not reveal any especially close relationships, and as experience shows, countries that score high in terms of e-government do not necessarily invest in cybersecurity with the same level of commitment and vice versa.

Table 5.2.1: showing the top ten 2018 e-government index

Country	Score	Rank
Denmark	0.9150	1
Australia	0.9053	2



Country	Score	Rank
Republic of Korea	0.9010	3
United Kingdom	0.8999	4
Sweden	0.8882	5
Finland	0.8815	6
Singapore	0.8812	7
New Zealand	0.8806	8
France	0.8790	9
Japan	0.8783	10

Some countries that appear in the e-government top ten also appear in the GCI top ten, showing a relative commitment of countries carrying out progressive development in all aspects. However, some countries are performing better in GCI than their level of development in e-government.

*The United Nations E-Government Index is a survey produced by a collective effort of the United Nations Department of Economic and Social Affairs (DESA), Division for Public Institutions and Digital Government (DPIDG) working together with UN Regional Commissions and other UN agencies, as well as several international experts, researchers and related organizations. Since 2001, there have been 11 publications of the e-government reports. The Survey is the only global report that assesses the e-government development status of all Member States of the United Nations. It assesses the rate of performance of countries relative to one another, as opposed to being an absolute measurement. It recognizes that each country should decide upon the level and extent of its e-government initiatives in keeping with its own national development priorities and achieving the Sustainable Development Goals.<sup>1</sup>*

<sup>1</sup> <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018>

Cybersecurity is a central point where organizations and nations traverse for an effective digital governance. There is need for cybersecurity to protect government infrastructure, realizing confidence and trust, hence paving the way for cybersecurity and e-government indices to go hand-in-hand for a transparent and accurate analysis of levels of commitment and development in the use of ICTs. Consequently, the GCI could adopt new cybersecurity indicators to include in the framework as governments are developing more sophisticated e-governance, increasing availability of online services, such as the emergence of online transaction services, and integrated service delivery systems that could lead to more enhanced cyber threats.

## B The ICT Development Index

The information society is challenged by cyber threats such as denial of e-services, data integrity breaches, and data confidentiality breaches, and the effectiveness of the Internet is linked to cybersecurity as more countries are advancing in the use of ICTs.

The ICT Development Index (IDI) has been produced and published annually by ITU since 2009. It is a composite index that combines 11 indicators into one benchmark measure. It is used to monitor and compare developments in information and communication technology (ICT) between countries and over time. The report features key ICT data and a benchmarking tool to measure the information

society, the ICT Development Index (IDI). It also presents a quantitative analysis of the information society and highlights new and emerging trends and measurement issues. The MISR assesses IDI findings at the regional level and highlights countries that rank at the top of the IDI and those that have improved their position in the overall IDI rankings most dynamically. It also uses the findings of the IDI to analyze trends and developments in the digital divide.<sup>1</sup>

Figure 5.2.1: Linking cybersecurity to development and e-governance

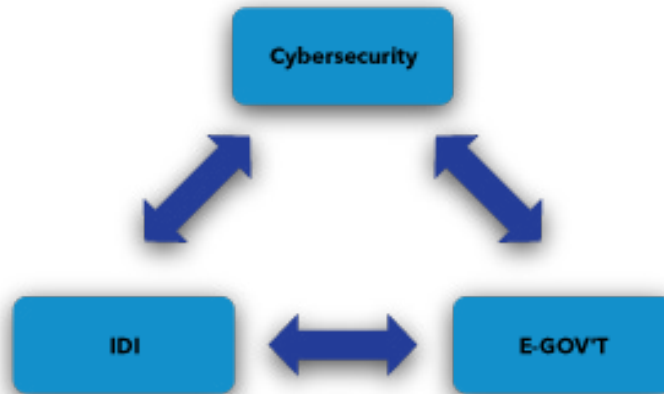


Figure 5.2.1 is a simplified view of the development of the information society leads to government realization that e-governance can only function safely if cybersecurity is implemented effectively, that it also has an impact on the overall developments in information and communication technologies, and development. GCI is not only a benchmark, it should be considered as a tool to guide governments on measures to put in place to overcome cyber threats.

As the Internet becomes more pervasive, from online banking to smart systems, higher standards of cybersecurity are essential. Cybersecurity systems must work for both service providers and service users and in the interest of the public.

<sup>1</sup> <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx>

Figure 5.2.2: Comparison of global IDI and GCI ranking

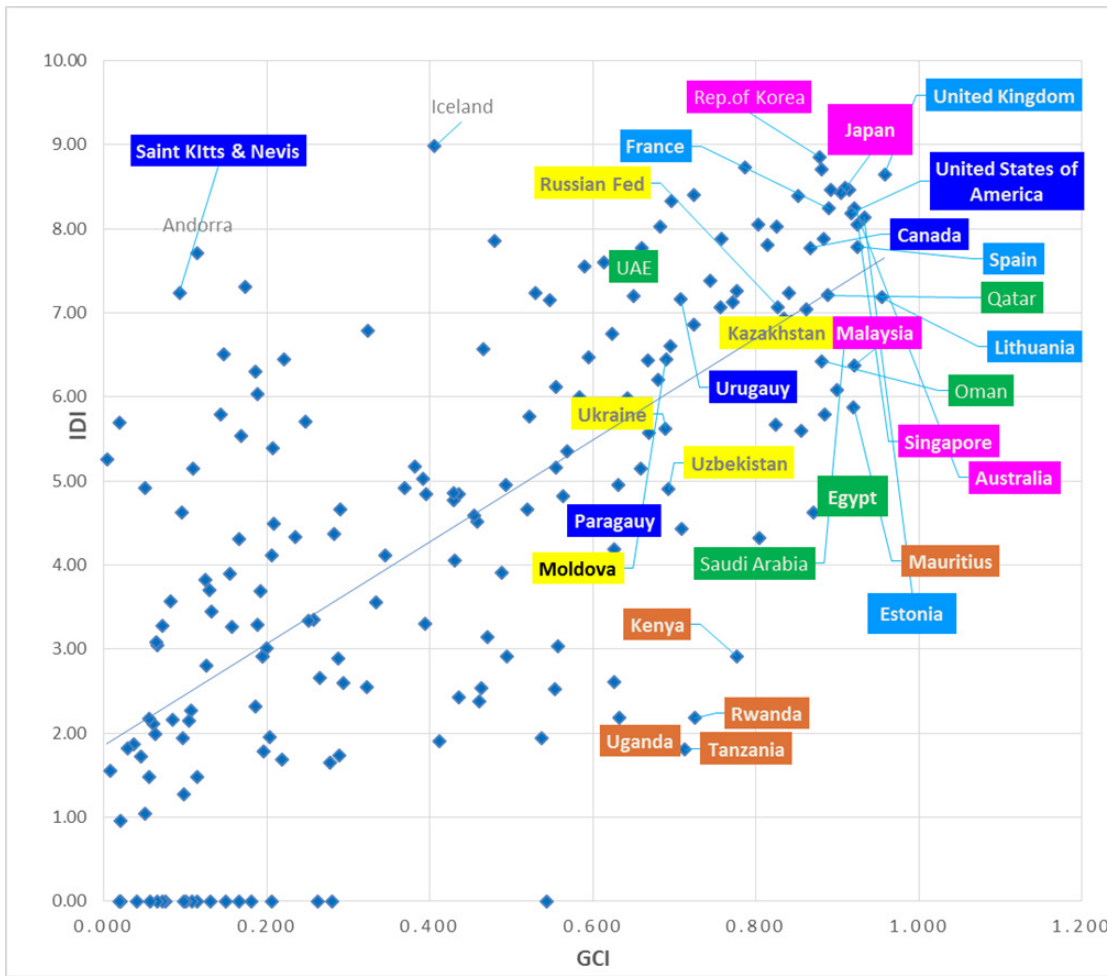
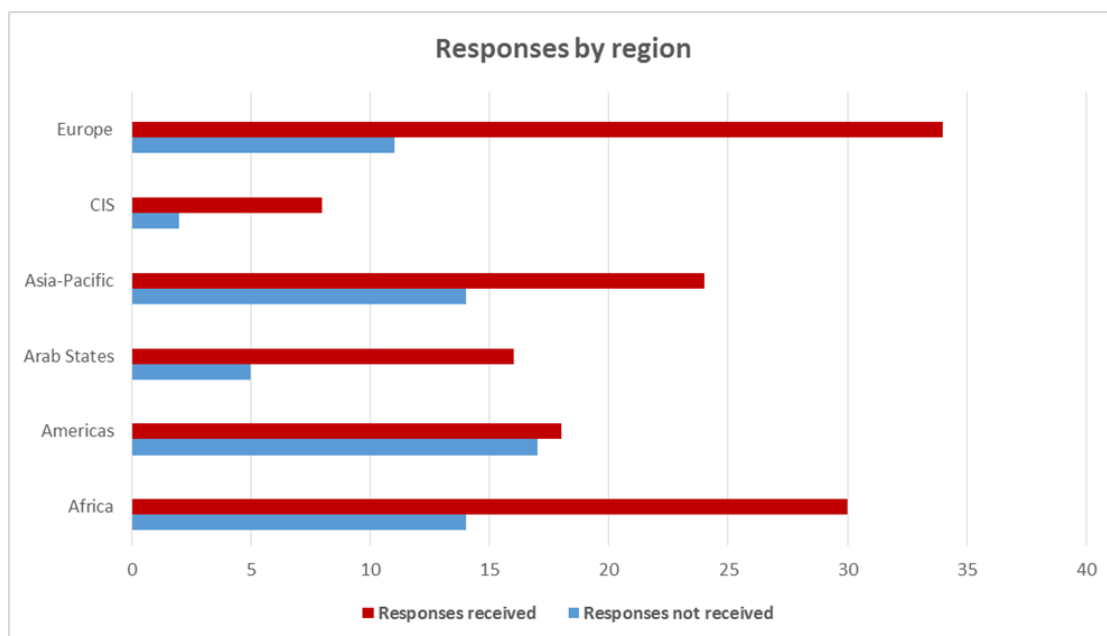


Figure 5.2.2 shows that that not all Member States with high IDI scores have a similarly high score in GCI, for instance Iceland took the top place in IDI scoring 8.98 while only 0.406 in GCI, Andorra, and Saint Kitts and Nevis also score high in IDI and yet very low in GCI, although some Member States are maintaining their leading positions in both indices. For IDI to be effective and resilient, cybersecurity needs to be implemented and regularly updated to reflect changing needs.

## 6 Regional outlook

During the active data collection phase of the GCI 2018 exercise, there was a varied response from countries in the ITU regions.

Figure 6.1: Number of GCI responses per region in 2018



- Of the 44 Member States in the Africa region, 30 responded to the survey.
- Of the 35 Member States in the Americas region, 18 responded to the survey.
- Of the 22 Member States in the Arab States region, 16 including the State of Palestine responded to the survey.
- Of the 38 Member States in the Asia Pacific region, 24 responded to the survey.
- Of the 10 Member States in the Commonwealth of Independent States region, 8 responded to the survey.
- Of the 45 Member States in the Europe region, 34 responded to the survey.

The GCI 2018 saw some changes in the regions: Georgia and Ukraine became part of the Europe region while during the last iteration they were part of the Commonwealth of Independent States region. The following tables and graphs show the top three countries of each region.

## 6.1 Africa

Table 6.1.1: Top three countries in the Africa region

Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
Mauritius	0.880	0.182	0.168	0.200	0.186	0.144
Kenya	0.748	0.195	0.110	0.147	0.147	0.149
Rwanda	0.697	0.157	0.117	0.178	0.137	0.108

**Mauritius** ranks first with the highest score in the organizational pillar. The CERT-MU develops many initiatives, such as the National Cybersecurity Strategy, the National Cybercrime Strategy and the National Cyber Incident Response Plan<sup>1</sup>. Mauritius has set up the National Disaster Cybersecurity and Cybercrime Committee, comprising of the public and private sectors, which facilitates the monitoring, control and transmission of decisions during cyber crisis situations at the national level.

**Kenya** ranks second with a high score in the legal pillar and in the cooperation pillar. Kenya has a multi-stakeholder local collaboration between the government, the different CIRTs and other key stakeholders including financial institutions, telecommunication operators, academia, critical information infrastructure providers, public utility service providers, content service providers, domain name registry service providers, etc.

**Rwanda** ranks third with a high score in the organizational pillar. The National Cybersecurity Agency has been established to oversee the protection of critical information infrastructure (CII)<sup>2</sup>. The Rwanda Information Society Authority has been established to oversee the management of government infrastructure<sup>3</sup>. Moreover, the Rwanda Utilities Regulatory Authority monitors private sector players (such as operators and service providers)<sup>4</sup>.

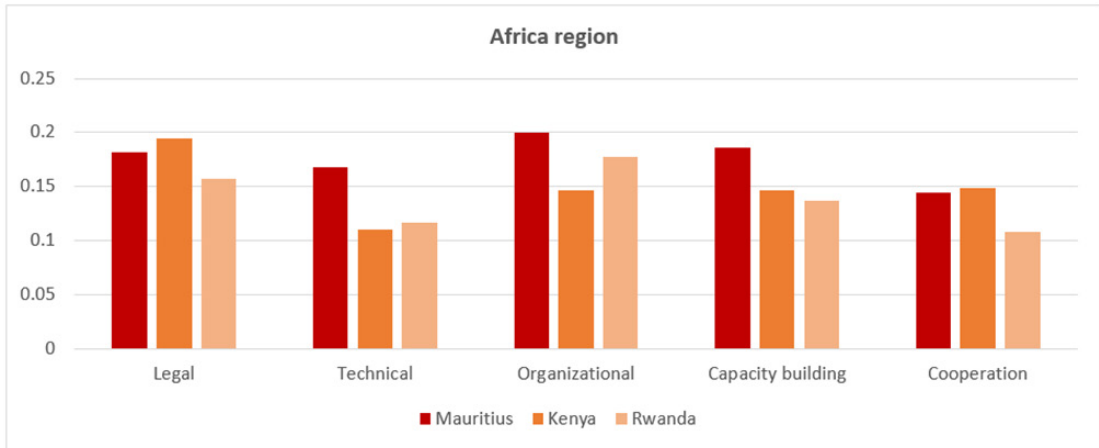
<sup>1</sup> <http://cert-mu.govmu.org/English/Pages/default.aspx>

<sup>2</sup> [http://www.mitec.gov.rw/fileadmin/Documents/Policies\\_and\\_Regulations/ICT\\_laws/Law\\_establishing\\_the\\_NCSA.pdf](http://www.mitec.gov.rw/fileadmin/Documents/Policies_and_Regulations/ICT_laws/Law_establishing_the_NCSA.pdf)

<sup>3</sup> [https://www.risa.rw/fileadmin/templates/documents/RISA\\_Law.pdf](https://www.risa.rw/fileadmin/templates/documents/RISA_Law.pdf)

<sup>4</sup> [http://www.rura.rw/uploads/media/Regulations\\_Governing\\_Telecom\\_Network\\_Security.pdf](http://www.rura.rw/uploads/media/Regulations_Governing_Telecom_Network_Security.pdf)

Figure 6.1.1: Top three scores in the Africa region relative to the five pillars of GCI



## 6.2 Americas

Table 6.2.1: Top three scores in the Americas region

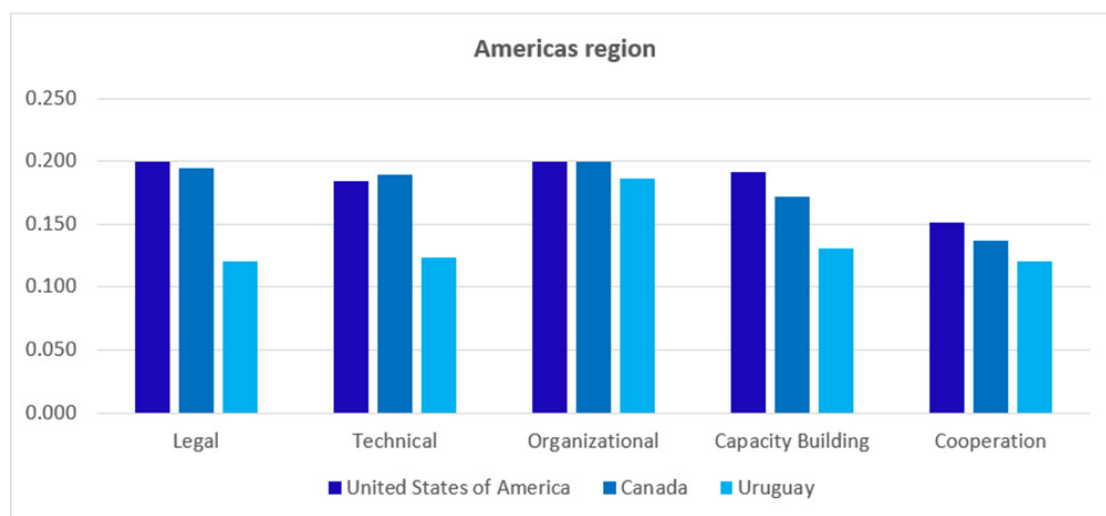
Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
United States of America	0.926	0.200	0.184	0.200	0.191	0.151
Canada	0.892	0.195	0.189	0.200	0.172	0.137
Uruguay	0.681	0.120	0.124	0.186	0.131	0.120

**United States of America** ranks first with the highest score in the legal pillar, and has a wide range of legal provisions, both substantive and procedural, to cover cybercrime.

**Canada** ranks second with the highest score in the organizational pillar with a very complete NCS.

**Uruguay** ranks third with a robust organizational pillar with a complete NCS and a framework on metrics used to measure cybersecurity development.

Figure 6.2.1: Top three scores in Americas region relative to the five pillars of GCI



### 6.3 Arab States

Table 6.3.1: Top three countries in the Arab States region

Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
Saudi Arabia	0.881	0.187	0.179	0.158	0.198	0.160
Oman	0.868	0.133	0.184	0.197	0.195	0.160
Qatar	0.860	0.193	0.154	0.192	0.171	0.151

**Saudi Arabia** is the top ranked country in the Arab States with the highest score in the capacity building pillar. Saudi Arabia shows a strong commitment to capacity building with many initiatives, including the BADIR (programme for technology incubator)<sup>5</sup>, the MAEEN (Saudi Research and Innovation Network)<sup>6</sup> and the SAFCSPP (The Saudi Federation for Cyber Security and Programming)<sup>7</sup>. Saudi Arabia has also developed a strong cooperation pillar.

**Oman** ranks second with the highest score in the organizational pillar and with a strong score for the cooperation pillar. Oman has established cybersecurity offices in government organizations.

**Qatar** ranks third with a strong legal framework and a robust organizational structure with a NCS that has a key focus on securing critical information infrastructure and a National Cybersecurity Committee responsible to implement and drive the NCS<sup>8</sup>. Their eCrime law integrates a large arsenal of procedural measures<sup>9</sup>.

<sup>5</sup> <https://badir.com.sa/en/>

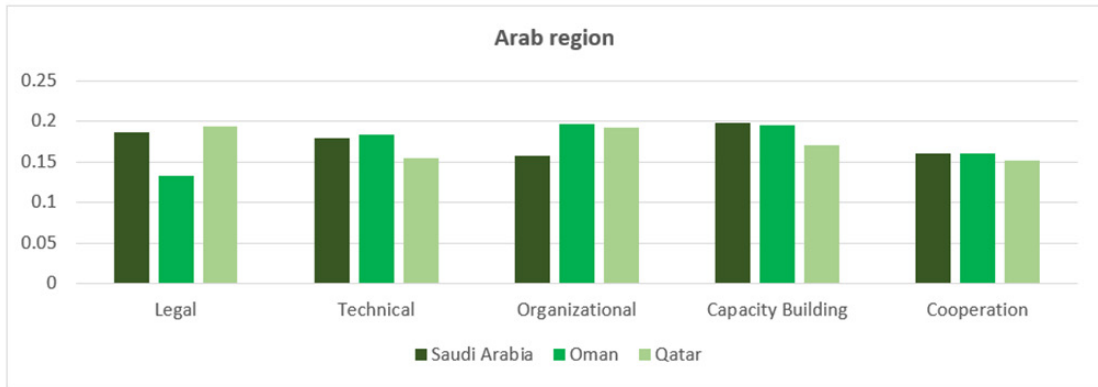
<sup>6</sup> <https://www.maeen.sa/>

<sup>7</sup> <https://safcsp.org.sa/en>

<sup>8</sup> <http://www.motc.gov.qa/en/cyber-security/national-cyber-security-strategy>

<sup>9</sup> <http://almeezan.qa/LawPage.aspx?id=6366&language=ar>

Figure 6.3.1: Top scores in the Arab States region according to the five pillars of GCI



## 6.4 Asia Pacific

Table 6.4.1: Top three scores in the Asia-Pacific region

Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
Singapore	0.898	0.200	0.186	0.192	0.195	0.125
Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
Australia	0.890	0.200	0.174	0.200	0.176	0.139

**Singapore** ranks first with the highest rank in the legal pillar. The Singapore Cybersecurity Act establishes a legal framework for the oversight and maintenance of national cybersecurity<sup>10</sup>. This act has four main objectives which are: the strengthening of the protection of CII against cyber-attacks; the authorization for the Cybersecurity Agency of Singapore to prevent and respond to cybersecurity threats and incidents; the establishment of a framework for sharing cybersecurity information and the establishment of a light-touch licensing framework for cybersecurity service providers.

**Malaysia** ranks second with the highest score in the organizational pillar and the capacity building pillar. Malaysia has established a National Cyber Security Agency (NACSA) that leads and oversees all national cybersecurity matters by coordinating and consolidating the nation’s best experts and resources in the field of cybersecurity<sup>11</sup>. NACSA also conducts periodical training and awareness programmes on cybersecurity matters to professionals from both public and private sectors.

**Australia** still maintains its third place in the Asia-Pacific region scoring 100 per cent in both the legal and organization pillars. Australia is not only home to the Council of Registered Ethical Security Testers (CREST)<sup>12</sup> but also the Australia Cyber Security Centre recently updated its Australian Government Information Security Manual (ISM) to help organisations to use a risk management framework, and

<sup>10</sup> <https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312>

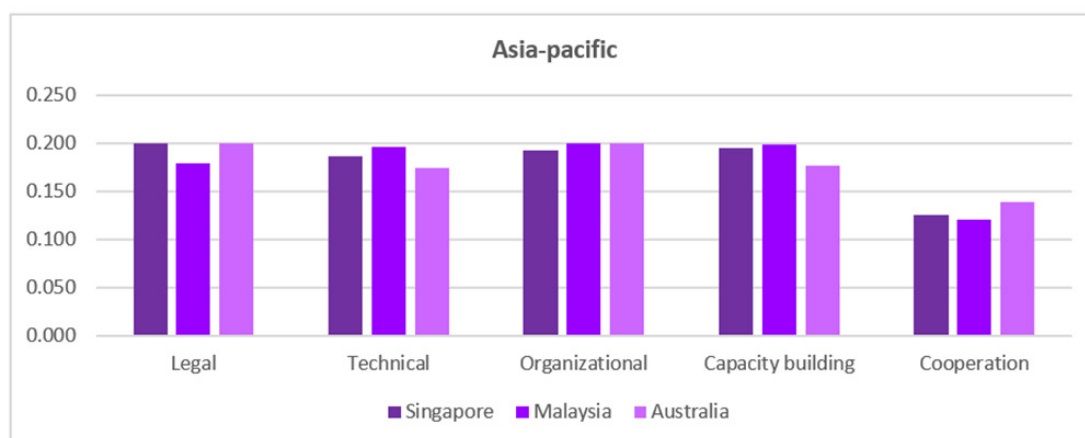
<sup>11</sup> [www.nacsa.gov.my](http://www.nacsa.gov.my)

<sup>12</sup> <https://www.crestaustralia.org/>



the ISM cyber security guidelines are based on ACSC and Australian Signals Directorate (ASD)<sup>13</sup> experience and knowledge.

Figure 6.4.1: Top three scores in the Asia-Pacific region relative to the five pillars of GCI



## 6.5 Commonwealth of Independent States

Table 6.5.1: Top three scores in the CIS region

Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
Russian Federation	0.836	0.197	0.162	0.177	0.166	0.135
Kazakhstan	0.778	0.179	0.143	0.174	0.160	0.122
Uzbekistan	0.666	0.123	0.142	0.112	0.143	0.144

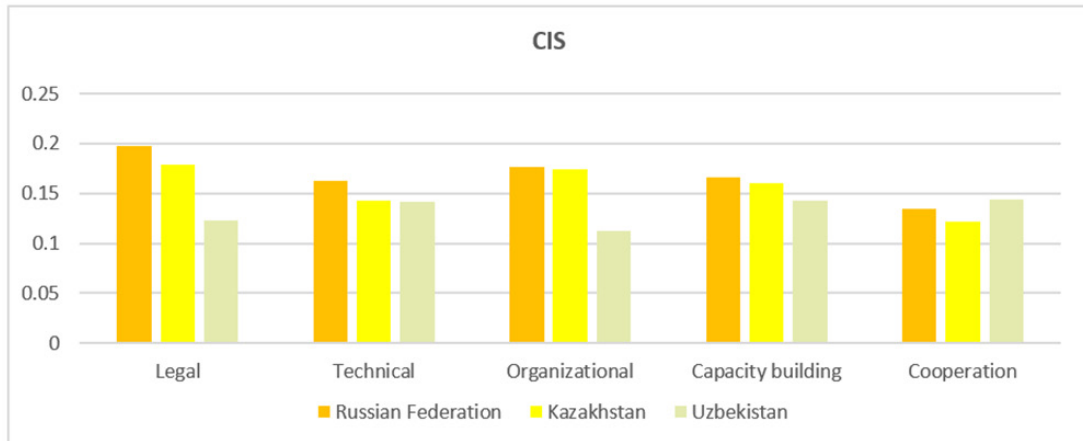
**Russian Federation** ranks first with a good score in the legal pillar, and has reinforced the compliance and regulation for fraud prevention and management with the use of electronic payment systems. The entire financial system of the country has been enhanced to ensure confidence in using online electronic payments.

**Kazakhstan** ranks second with a good score in the legal pillar. Kazakhstan has unified the requirements in the field of information and communication technologies and information security.

**Uzbekistan** ranks third with a good score in the cooperation pillar and has signed a memorandum of understanding (MoU) with different agencies in neighbour countries. Uzbekistan has also developed a strong public-private partnership, including with foreign companies.

<sup>13</sup> <https://www.acsc.gov.au/news.html>

Figure 6.5.1: Top three scores in the CIS region relative to the five pillars of GCI



## 6.6 Europe

Table 6.6.1: Top three scores in the Europe region

Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
France	0.918	0.200	0.193	0.200	0.186	0.139
Lithuania	0.908	0.200	0.168	0.200	0.185	0.155

**United Kingdom** ranks first with the highest score in the legal pillar and the organizational pillar. United Kingdom has a number of legal instruments enabling them to fight cybercrime, including the Computer Misuse Act. The National Crime Agency<sup>14</sup> successfully led an international operation to shut down a website linked to 4 million distributed denial of service (DDOS) attacks globally<sup>15</sup>.

**France for the second time** is ranked in second place in the Europe region, scoring 100 per cent in legal and organizational pillars. France is collaborating with institutional partners (ministries, national authorities, private sector and non-profit organizations) and, under the European cybersecurity month, using various means to raise cybersecurity awareness<sup>16</sup>.

**Lithuania** has the highest score in both the legal pillar and the organizational pillar. The Lithuania Law on Cybersecurity lays down provisions enabling competent authorities to take action against public electronic communication infrastructure participating in malicious online activity (e.g. participating in a botnet)<sup>17</sup>. The State Data Protection Inspectorate can publish cybersecurity incidents involving personal data breaches<sup>18</sup>.

<sup>14</sup> <http://www.nationalcrimeagency.gov.uk/>

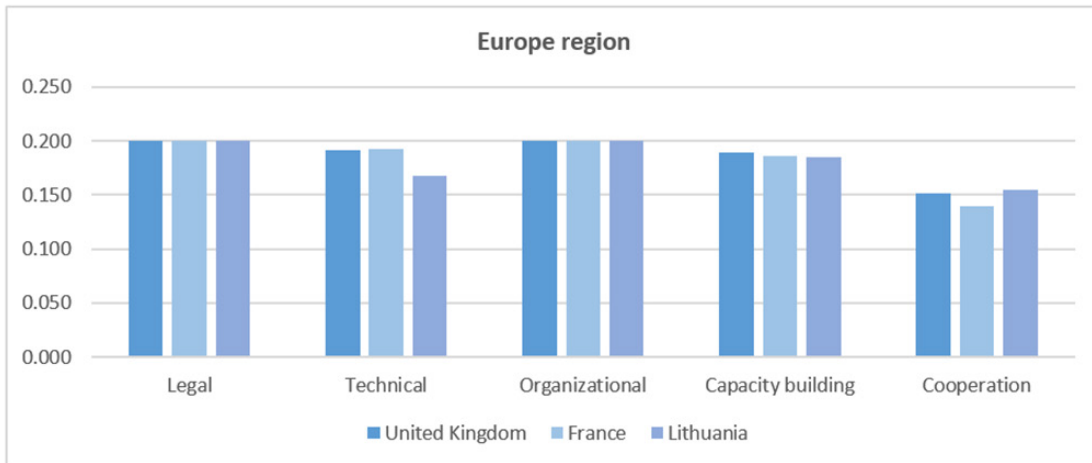
<sup>15</sup> <http://www.nationalcrimeagency.gov.uk/1335-international-action-against-ddos-tool>

<sup>16</sup> <https://www.ssi.gouv.fr/en/actualite/raising-awareness-on-cybersecurity-through-cartoons/>

<sup>17</sup> <https://www.e-tar.lt/portal/lt/legalAct/2a916390c5b211e583a295d9366c7ab3/GSDjgmYIWG>

<sup>18</sup> <https://www.ada.lt/go.php/lit/Informacijos-apie-kibernetinius-incidentus-pateikimas-gali-teikti-tik-duomenu-valdytojai/4/2>

Figure 6.6.1: Top three scores in the Europe region relative to the five pillars of GCI



### 6.7. The commitment level per pillar in the six regions

The information and best practices noted in this section have been provided by Member States.

Figure 6.7.1: Commitment to indicators in the legal pillar per region



#### Legal

This section presents best practices provided by ITU Member States that illustrate what is happening, achievements, and progress taking place related to the legal pillar of the GCI.

Azerbaijan – Chapter 30 of the Criminal Code has been introduced as a result of the Council of Europe expert assistance. One priority area in the work plan of the Cabinet of Ministers for 2018 is discussion of the project of “Cybersecurity Strategy of the Republic of Azerbaijan”.

Belgium – Belgium has launched the ‘Digital Belgium’ action plan, which outlines the long-term digital vision for Belgium and translates this vision into clear ambitions. It states that in order to be able to grow, the digital economy needs confidence and security, which means respecting rights and

strategically and effectively tackling illegal practices. Only when citizens and businesses have full confidence that their data is safe online, can the digital economy achieve its full potential.

Tackling illegal content and practices, Belgium is building a modern legal framework that protects citizens and businesses against illegal content and activities on the net. New measures such as online resolution of consumer disputes or efficient procedures against illegal online content ensure that the same protection applies online and offline.

Brazil – The draft Brazilian Data Protection Law, which includes breach notification provisions, was approved by the Chamber of Deputies on 29 May 2018.

Denmark has a system with personal digital signatures that are adopted as the standard login to all government digital services and is also used by the financial sector, allowing consumers to access their banking information using their digital signature. This solution includes two-factor authentication. Even though both banking and government is highly digitized, this broadly adopted solution is a contributing factor to relatively low rates of significant online fraud. Denmark uses existing legal frameworks when possible, allowing for interpretation of the law by the court when applying them to new technologies. This has allowed the legal system to adapt to, for example, the emergence of spam using regulations originally intended for telephony and mail. Laws can then be adjusted later to specify new technology, but wide frameworks allow for fast response to new trends.

Japan is implementing legal reforms to facilitate information sharing on cyber attackers among telecommunication operators and to take measures against IoT devices that are incomplete in setting proper passwords. The government has sent the bill of amendment of the Basic Act on Cybersecurity to the National Diet of Japan. The amendment aims to encourage public and private sectors to share cybersecurity-related information more strategically.

Lithuania – The parliament adopted the Law on Cyber Security, in force since 1 January 2015, has a number of implementing acts, such as the National Cyber Incidents Management Plan, Organizational and Technical Cyber Security Requirements Applicable to Critical Information Infrastructure and State Information Resources, Methodology of Identification of Critical Information Infrastructure, etc. The law gives authority to the National Cyber Security Centre to take action in the case of malicious activities. The new revision of the Law on Cyber Security has been submitted to the Lithuania Parliament in order to transpose the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Since the adoption of the Law, Lithuanian Criminal Police Bureau (responsible for investigating criminal cyber incidents) in cooperation with CERT-LT, have successfully identified and investigated cyber incidents related to IP addresses involved in botnet activity. CERT-LT can be asked to provide a list of malicious IP addresses, and the Bureau sends compulsory orders to relevant service providers administering respective IP addresses with a request to fix the issue. Failure to fix the issue within 48 hours, can lead to blocked Internet access for the respective IP address. Although the order to block Internet access must be approved by the court, over 100 IP addresses have been “cleaned” since the adoption of the law.

The State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – SDPI) created an online form for reporting cybersecurity incidents involving personal data breaches using the SDPI system of electronic services.

Mauritius – The cabinet has approved the accession of Mauritius to the African Union Convention on Cybersecurity and Personal Data Protection and the instrument for the ratification will be sent to the African Union Office in Addis Ababa, Ethiopia. Further, the Computer Misuse and Cybercrime Act (CMCA) 2003 has been reviewed to align with the Budapest Convention on Cybercrime and African Union Convention on Cybersecurity and Personal Data Protection. The alignment of the CMCA has

been approved by the cabinet and the Ministry of Technology Communication and Innovation and the State Law Office are working on the amendments.

Moldova – In the context of the development of information society aspirations, the Government of the Republic of Moldova approved a strategic and legislative framework for the development of the ICT domain in Moldova, the most important being the National Strategy for Information Society Development “Digital Moldova 2020”.

The Cyber Security Programme 2016-2020 offers a systematic and complex approach of actions necessary to provide cybersecurity in the Republic of Moldova based on the best international practices through its harmonization with European legislation. The programme includes seven areas of intervention: safe processing, data storage and accessing; security and integrity of electronic communication networks and services; prevention capabilities and emergency response; preventing and combating cybercrime; strengthening cyber defence capabilities; education and informing; and international cooperation and interaction. In order to implement the programme, the Government Decision on the Approval of Mandatory Cyber Security Requirements (Government Decision No. 201 of March 28, 2017) was drafted and approved. These minimum cybersecurity requirements apply to the State Chancellery, the Ministries and other central administrative authorities with regard to IT systems, information resources and systems already in place, as well as those under development, testing and implementation to ensure an adequate information protection system.

Saudi Arabia – The Communications and Information Technology Commission (CITC) is the communications authority in Saudi Arabia, and apart from its approval of Resolution No. (81) on the Control of Computer and Information Network Use in Government Agencies law, the CITC has been finalizing the Cyber Security Regulatory Framework for ICT sector, which covers: Cybersecurity governance, cybersecurity risks, cybersecurity compliance, data protection, breach notifications and incident risk, audit requirements and system and network protection.

As a measure to protect children online, Parental Control Service Regulatory Framework (New regulation) was approved in 2018 with guidelines on how to report abuse on social media and a guide on how to protect children from the risks of the Internet.

Serbia – By adopting its Law on Information Security in June 2016, Serbia determined the competent authority for information security through the Regulation on child safety and protection when using information communication technologies (ICT). This Regulation will contribute to a comprehensive approach on child online safety and will develop state mechanisms of assistance and reactions in this area. The goals of the Regulation are to raise awareness and knowledge on the advantages and the risks of Internet use (through seminars, workshops, press releases and in cooperation with competent organizations and civil society organizations), and ways to use the Internet safely; enhance digital literacy of children, parents and teachers and to develop cooperation between public sector bodies in this area.

Singapore – The Cybersecurity Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Prior to the enactment of the Cybersecurity Act, there were several pieces of legislation that touched on different aspects of cybersecurity (e.g. Computer Misuse and Cybersecurity Act (CMCA), as well as sector-specific regulations such as the Telecommunications Act). However, there was not a way to standardize the cybersecurity requirements across all 11 critical sectors. While the CMCA allowed the government to take emergency measures to counter a serious or imminent threat to essential services or national security, there were no levers to require critical information infrastructure (CII) owners to adopt preventive measures to protect CIIs to ensure continuous delivery of services. The newly-introduced Cybersecurity Act addresses these gaps. The Act has four key objectives are to: (i) strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks; (ii) authorize the Cybersecurity Agency of Singapore (CSA) to prevent and respond to cybersecurity threats and incidents – the powers that may be exercised are calibrated according to the severity of the cybersecurity threat or incident and measures required for response; (iii) establish a framework for sharing cybersecurity information and (iv) establish a light-touch licensing

framework for cybersecurity service providers. In particular, Singapore is one of the first countries to introduce legislation for a licensing scheme.

Slovakia – In cybersecurity legislation, Slovakia has achieved several important milestones. In accordance with EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (commonly called the NIS Directive), Slovakia prepared substantive legislation. These legislative efforts have been transposed in the Act on Cyber Security, which entered into force in April 2018. Implementing regulations relating to the Act on Cyber Security have been created, which include specifics in incident categorization, incident reporting, rules of CSIRT unit accreditation, determining identification criteria of the operated service (criteria of the essential service) and security measures.

Spain – Law 36/2015 on National Security in Spain defines the framework for crisis management at the national level. The Law reflects the progress of the implementation of the National Cybersecurity Strategy, emphasizes cyberspace as an area of national security, and establishes the structure of national authorities for security, and cybersecurity in particular. Ministerial Order PRA/33/2018 regulates the functioning of the National Cybersecurity Council, as an expert advisory committee of the National Security Council, chaired by the President of the Government of Spain. Ministerial Order PRA/116/2017 announces an agreement (President and Ministers with responsibilities in the matter) on the implementation of mechanisms to guarantee the functioning of the National Security System, cybersecurity being part of this system.

Sri-Lanka – The Sri-Lanka Cyber Crime Unit (CCU) was established in line with the enactment of Computer Crimes Act. The Sri Lanka Police CCU unit is positioned within the Criminal Investigation Department (CID). The CCU conducts investigations into pure cybercrime (e.g. hacking and malware) and cyber enabled crime, either with the allegation reported to them directly to their unit or referred from elsewhere within the Sri Lanka Police.

Thailand – The government has put great effort in developing and enacting digital laws to modernize Thailand, including cybersecurity and data protection laws. They are already approved in principle by the Cabinet and both laws are expected to become effective in 2018. The ICT Law Center under the supervision of the Electronic Transactions Development Agency, Ministry of Digital Economy and Society keeps track of eight digital laws that are currently being considered. The government also actively seeks public input when reviewing new draft laws.

UAE – The Ministry of Interior (MoI) established the Higher Committee for Child Protection in 2009 and the MoI Child Protection Centre in 2011 to undertake the role of developing, implementing and customizing the initiatives and processes aiming at providing safety, security and protection for all children living in the UAE or even those coming as visitors. The committee plays a key role in maintaining the safety of children, because achieving justice and protection for children is a shared responsibility. The COP Committee aims to achieve several strategic goals to promote the issue of child online protection.

United Kingdom – The National Crime Agency (NCA) continues to lead and coordinate the United Kingdom fight against cybercrime, working closely with a range of domestic and international cybersecurity partners. Recent successful activity, as a result of close collaboration between NCA, Police and judiciary partners both domestically and abroad, includes: Criminals offering Webstresser tools often look to exploit grey areas arising from the ability of such tools to be used for both legitimate networking stress testing activity and illegal activity such as DDOS attacks. However, on 24 April 2018, the NCA and Dutch National Police, in collaboration with international law enforcement partners, successfully led an international operation that shut down a website linked to 4 million DDoS attacks globally, including against the biggest banks in the United Kingdom linked to the 'Webstresser' service. A significant criminal website was shut down and the sophisticated crime group behind it stopped. In June 2017, NCA and United Kingdom Police partners, as part of a coordinated international law enforcement operation targeting people suspected of using cyber tools to get around anti-virus computer protection. At the heart of the investigation was a platform used by malware

developers before they launch cyber-attacks to test samples for their ability to evade popular off the shelf anti-virus software. Data sharing between the United Kingdom and its partners in the Europol European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) triggered and enabled these arrests to take place.

Figure 6.7.2: Commitment to the indicators in the technical pillar per region



### Technical

This section reports on best practice provided by Member States that illustrate what is happening, achievements and progress taking place in each Member State relative to the technical pillar of the GCI.

Belarus - Authorized Internet service providers are providing hosting services to implement mechanisms to ensure control over the integrity of Internet resources. Such mechanisms include using software tools for detecting anomalies of operating systems caused by the presence in the system of malicious programmes, such as "ARKIT" – a software protecting against malicious software, unauthorized access and firewalling (CANOE ).

Belgium – CERT.be is the technical and operational service located within the Centre for Cybersecurity Belgium (CCB) and ensures the management and treatment of cyber incidents, information sharing, and recommendations concerning attacks and threats. CERT.be provides proactive and reactive services to different target groups, and primarily to critical service providers and critical infrastructure providers. To carry out the missions of CERT.be, the CCB increase the number of staff in 2017. At the end of 2017, CERT.be had around twenty staff members including a director, a programme manager, a technology advisor, a communication manager, cyber analysts, cyber experts and an office manager. At the end of 2018, CERT.be will be available 24 hours a day, in order to meet a real need and to be constantly ready to react in the event of national cybersecurity incidents and crises. The government decided recently to continue to expand CERT.be in 2019 to 36 experts.

Denmark –The Centre for Cybersecurity has deployed a network of intrusion detection systems on a number of networks related to critical infrastructure and sensitive government information, including defence. These provide valuable data about attempted advanced cyber-attacks against Denmark. An

expanded supplementary network is under development, intended to provide a broader real-time picture of broader cyber threats against industry, businesses, and government. An updated version of the national login and digital signature infrastructure is currently under development, and a newly developed alternative to printed one-time codes for the two-factor login was launched. A mobile app allows the user to verify login-attempts. This is intended to improve usability and counter certain attack vectors, where criminals had been able to intercept or otherwise attain the printed codes from the users. In spite of a very high degree of digitization in Denmark there have been very few incidents of compromise of user information or government systems due to technical vulnerabilities or shortcomings in the solutions.

Moreover, reporting security incidents must be a simple and easy matter for businesses and authorities alike. For this reason a shared digital solution for reporting security incidents, ensuring that businesses only have to report an incident once and in one location and enabling the communication of action-oriented information concerning prevention and handling of incidents back to the reporter, has been initiated. The digital portal for reporting of security incidents will be accessible via Virk.dk, which already serves as the digital portal for businesses and authorities reporting to the public authorities. A first basic version covering 10 authorities including the Network and Information Security (NIS) Directive and the EU General Data Protection Regulation (GDPR) was launched on 9 May 2018. A more advanced version will be ready in 2019.

Estonia – In September 2017, the CERT-EE Certification Certificate was issued, and a quality certificate was issued by Trusted Introducer. There are over 300 CERTs in the world, of which 22 are recognized by the Certification Certificate. Six of the recognized entities are national, including Estonia since September.

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

Jordan – The government has conducted several technical activities related to protecting citizens including providing the National Broadband Network (optical fibre connection between all government entities) with an additional secure layer, the Secure Government Network (SGN). In addition, to manage and harmonize approaches to cyber risks and threats among all government entities, the government has established JO-CERT (Jordan Computer Emergency Response Team).

Jordan has also conducted national electronic authentication projects by adopting a PKI (public key infrastructure) solution. One of the projects is Smart ID, where traditional citizen identity cards have been replaced with a smart identification card. The National Smart Card has two certificates for authentication and a digital signature in order to move toward full digital identity of citizens as well as enhancing the Digital Jordan project.

Lithuania- To consolidate functions and resources, which were previously scattered among various institutions into single entity, the National Cyber Security Centre (NCSC) has been created. Consolidation has helped to concentrate best expertise and avoid not always efficient inter-institutional interaction issues, thus enabling faster decision making and response time. The National Cyber Security Center serves as a single stop shop for all entities in the Republic of Lithuania to notify cyber incidents and to ask for support in case of incident when reporting entity is unable to cope alone.

In order to ensure higher level of collective cybersecurity of state information resources, Lithuania further develops solutions for provision of secure governmental cloud services for public institutions, as well for integration of public IT infrastructure into governmental data network. In both these cases there is a possibility to employ more efficient and advanced collective cybersecurity measures.

NCSC operates Cyber Security Information Network, which serves as information sharing and incident management information platform for state information resources and critical information



infrastructure. Access to the network is granted for registered users, complying with specific security requirements and is not publicly accessible.

Local practices of CSIRT community competences are being very successfully exported to assist governments in other countries (including support for national CIRTs in Bhutan, Bangladesh, Cyprus, additionally assisting governments including Burundi, Lesotho, Rwanda, Tanzania, and Uganda).

Luxembourg- Technical software is being used to implement cybersecurity including:

- MISP – the malware information sharing platform used by CSIRTs around the world
- AIL – the analysis information leak framework, principally developed by CIRCL.

AIL is a modular framework used to analyze potential information leaks from unstructured data sources like pastes from Pastebin or similar services, or unstructured data streams. The AIL framework is flexible and can be extended to support other functionalities to mine sensitive information.

Malaysia- Best practice guidelines have been developed for security services and cloud security practice in collaboration with the industry. A cloud security practice document is being prepared to establish a cloud security certification scheme. An Internet Banking Task Force, consisting of local financial institutions, the Malaysian Communications and Multimedia Commission (MCMC), Cybersecurity Malaysia, and the Royal Malaysian Police, is being established to combat online banking fraud. The Digital Forensics Working Group, comprising all law enforcement agencies that operate digital forensic laboratories, is being created. Critical national information infrastructure (CNII) agencies meet to discuss best practices and information sharing in technical areas in cybersecurity. The National Cyber Coordination and Command Centre (NC4), which is connected to other cyber operating centres including MCMC Network Security Centre, and the Defence Security Centre, provides technical advisories to all CNII agencies. The National Cyber Drill (X-Maya) is testing and improving the technical skills of CNII IT personnel to handle cyber incidents. The Coordinated Malware Eradication and Remediation Project (CMERP) has implemented a pilot project to tackle malware threats at the national level. Malaysia is a member of the Common Criteria Recognition Arrangement (CCRA) and a certificate-authorizing member of the Common Criteria Information Technology Security Evaluation (CC). A supervisory control and data acquisition (SCADA) Security Testing Simulation lab is being established in addition to an Information Security Management System (ISMS) business process automated tools for organizational/agencies self-assessment to the MS ISO/IEC 27001: 2013 standard compliance. In addition, NC4 is being fed data from honeypots set up by CyberSecurity Malaysia and MCMC.

Mauritius – A cyber incident response protocol has been finalized and will be implemented at the country level to handle incidents in the cyber crisis situation. A centralized incident reporting portal has been put in place to report cyber incidents and a Security Operations Centre (Anti Cyber Threat Monitoring System) is being implemented. This system will detect and monitor malicious traffic in real time and will help the country to enhance its cyber threat preparedness.

Mongolia- The General Intelligence Agency, the National Data Center, and MN-CERT NGO are responsible for the prevention of and response to cyber-attacks, but there is no overarching system in place to implement this function at a national level. In 2017, the Mongolia Government started a feasibility study to establish a CERT and an IT security audit system for Mongolia. The feasibility study project aims to identify the status of the cybersecurity environment such as the organization/manpower, ICT infrastructure, legal environment and standards, IT security/auditing process, and to investigate a development plan. In addition, this project aims to make a proposal for the To-Be Model of a Mongolia CERT.

Nepal – The Digital Forensics Lab has been established by Nepal Police within its headquarters. Security audits of different governmental applications/websites have been carried out effectively by the Department of Information Technology (DoIT). All financial institutions in Nepal are required to carry out security audits as regulated by the Central Bank of Nepal. The Nepal Telecommunications

Authority has signed a memorandum of understanding (MoU) with Nepal Police to enhance Digital Forensic Capabilities and strengthen the Digital Forensics Laboratory.

Serbia – In 2017, the Ministry established the helpline “National Contact Centre for Child Online Protection (19833)” and an Internet portal. Children, parents and teachers are advised on the advantages and risks of Internet use, and on safe ways for using the Internet, including advice on the risks of video games and Internet use addiction. It is possible to report harmful, illicit and illegal content and behaviour on the Internet either through the helpline or the portal. The Ministry dispatches such reports to the appropriate recipient – website administrators for harmful content and to the competent prosecutor office, and the Ministry of Interior (Service for combating cybercrime) in cases of criminal offences.

Singapore – Development of Standards: The public and private sectors in Singapore have worked together to develop or adopt new cybersecurity standards to address gaps in cybersecurity standards. For example, in 2013, the InfoComm Media Development Authority (IMDA) worked with Enterprise Singapore (ESG) and industry players to develop the world’s first multi-tiered cloud computing standard to address the security of cloud services provided by government agencies and private sector. This new standard caters for different levels of security, depending on the level that service providers can offer to their users. The Singapore Standards Council has also embarked on the development of new standards that are currently not available at the international level. These include cybersecurity standards for autonomous vehicles and general requirements for IoT security for smart nation projects in Singapore.

- Internet Surfing Separation: The government has adopted the separation of Internet surfing infrastructure from the government network to counter Advanced Persistent Threats.
- Bug Bounty programme: This is a cybersecurity exercise initiated by the Ministry of Defence (MINDEF) in January 2018, and which has demonstrated that a managed vulnerability hunting exercise can be deployed to complement traditional vulnerability management approaches. It also provided a platform for skilled cybersecurity practitioners to better channel their talents and energies to coordinated programmes to help the government test and validate its cybersecurity posture.
- Industrial Control Systems Guidelines: Singapore launched the Industrial Control Systems (ICS) Cybersecurity Guidelines in January 2018 to provide ICS operators with recommended practices to improve their cybersecurity processes and controls in their ICS environment. The ICS Cybersecurity Guidelines were co-developed by a community of organizations and regulators in different sectors that rely more heavily on industrial control systems (Water, Energy, Land Transport and Maritime).

Sri Lanka – The Sri Lanka Police Cyber Security Division has been established and investment is continuing on capacity building on the latest developments of technical tools and best practices required for effective cybersecurity.

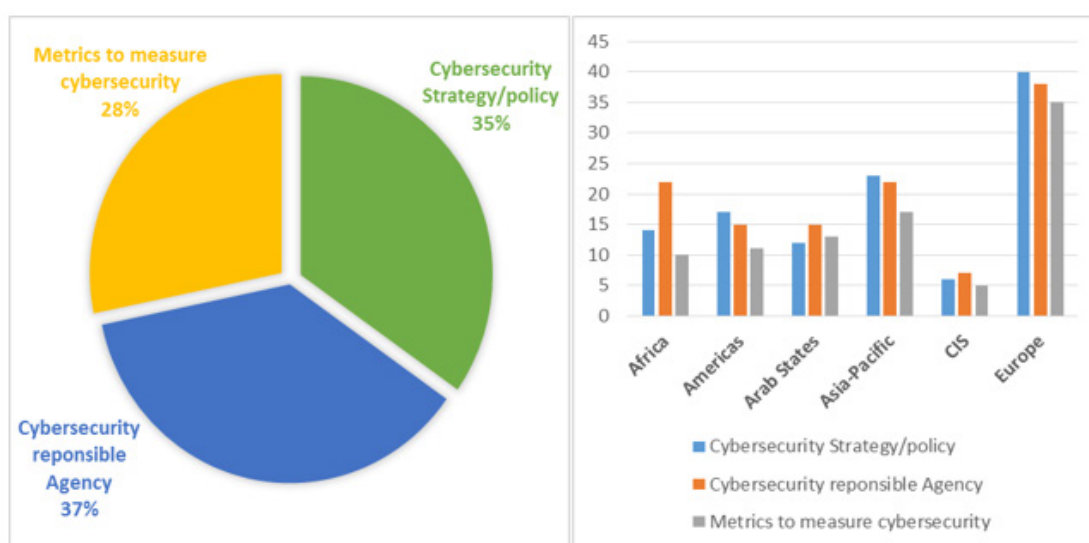
Ukraine – The CERT-UA team is constantly taking steps to engage with other Member State CERT teams, as well as with the Cisco Talos Intelligence Group on issues related to overcoming the effects of cyber-attacks on critical information infrastructure and identifying the causes and circumstances of cyber incidents. In addition, given its membership in international institutions, taking into account the commitments undertaken and the importance of public-private partnership in cybersecurity, CERT-UA is helping to eliminate threats to the Ukrain private sector, as well as to foreign public and private sectors.

It should be noted that the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine", among other things, determines the tasks of the CERT-UA at the legislative level. In accordance with this Law, the CERT-UA and the Cybercrime Response Centre will play a coordinating role in measures aimed at operational (crisis) response to cyberattacks and cyber incidents, and the introduction of counter-measures aimed at minimizing the vulnerability of communication systems. The State Service of Communications is involved in the work of the EU Cybersecurity Agency and the European Centre

for Cybersecurity Research and Competence, as well as the EU-planned exercises on the implementation of the Operational Joint Response Scheme of the EU and Member States on large-scale cyber-attacks. The Crisis Response Framework in the field of cybersecurity will facilitate the expansion of the capabilities of the Centre for Cybersecurity Response and the CERT-UA teams.

United Kingdom – The NCSC Active Cyber Defence Programme aspires to protect the majority of people in the United Kingdom. Four initial measures have already had a significant impact: blocking fake emails; stopping systems veering into malicious websites; helping organizations easily fix website problems; phishing and malware mitigation. The programme is expected to continue to drive change over the next two to five years. The NCSC launched Active Cyber Defence, which has prevented thousands of attacks and reduced the average time a phishing site is online from 27 hours to 1 hour. There has been a 43 per cent increase in visits (4 000 visitors per month) to the Cyber Security Information Sharing Partnership (CISP), which allows the community to share information about cyber threats.

Figure 3: Member States commitment to the indicators in the organizational pillar per region



### Organizational

This section sets out the best practices provided by Member States that illustrate what is happening, achievements and progress taking place in each Member States as regards to the organizational pillar of the GCI.

Albania – In January 2017, Albania approved law No.2/2017 On Cyber Security. The purpose of this law is to achieve a high level of cybersecurity by defining security measures, rights, obligations, and mutual co-operation between entities of critical and important infrastructures and the national authority for electronic certification and cyber security (NAECCS) in the role of a national CIRT. The "Policy Paper on Cyber Security 2015-2017" of December 2015 reviewed and coordinated the obligations arising out of commitments made for a secure cyber space in order to ensure compliance responsibilities of all stakeholders in a coordinated manner. This helps to guarantee further development of the information society as a safe, reliable and open environment as well as promoting the values and opportunities offered by the use of cyber space.

Currently, cybersecurity is included in the National Security Strategy. However, the government of Albania considers cyber space to be an environment that needs to be given an important role and has authorized NAIS (National Agency of Information Society) and NAECC, which is the responsible

authority for cybersecurity in Albania, to coordinate efforts with all the other stakeholders to draft a national strategic document.

Japan – The government of Japan revised and published "The Cybersecurity Policy for Critical Infrastructure Protection" (4th Edition in April, 2017). Under the policy, critical infrastructure operators are responsible for safe and continuous provision of critical infrastructure-related services, and the government supports critical infrastructure operators as necessary. The National center of Incident readiness and Strategy for Cybersecurity (NISC) conducts cybersecurity audit and gives appropriate advice, not only to government but also to incorporated administrative agencies and special corporations and authorized corporations. The Information and communication technology-information Sharing and Analysis Center (ICT-ISAC) composed of telecommunication operators, broadcasters, security vendors, etc. shares cyber threat intelligence and takes measures.

Jordan – Risk assessment report has been completed in cooperation with consultation company (BAE Systems) – British Aerospace Systems. The National Cybersecurity Programme (NCP) was established to focus on delivering the strategic objectives and national priorities set out in the National Information Assurance and Cyber Security Strategy (NIACSS) in 2012 and the programme of the KPMG auditing for the financial sector. The new cybersecurity policy for Central Bank of Jordan was distributed internally for review as a preliminary phase before final approval.

Kuwait – The creation of the National Cyber Security Centre (NCSC) was mandated in the National Cyber Security Strategy for the State of Kuwait (2017-2020). In order to increase the cybersecurity of the nation, a consultancy project has been implemented to address "Development of the Framework, Operating Model and Programme for National Cyber Security for the State of Kuwait" and the NCSC will implement the strategy, allow early delivery of key functionality and support controlled growth over the three-year period. The major achievement of the consultancy project was the provision of initial assessment of the risk and maturity position among a number of critical national infrastructure (CNI) stakeholders, and the level of national cybersecurity maturity to strengthen Kuwait's ability to protect national interests from possible cyber-attacks. CNI entities (45) were given risk and maturity questionnaires to identify appropriate standards and processes for national risk management and were advised on how they should be adopted at a national level. After conducting the risk and maturity assessment, CITRA, as the responsible agency for delivering the National Cyber Security Programme in Kuwait, provided roadmaps with specific best-practice recommendations for each entity pertaining to cybersecurity and on how each entity can mature. A new National Cyber Security Framework was defined for Kuwait and building on this, an National Cyber Security Operating Model was developed in conjunction with CITRA to define the key roles and responsibilities of the main actors in the framework.

Mongolia – In line with Government Resolution No. 312, an information system risk assessment and audit is conducted every two years in the public information system targeting governmental agencies and departments. Mongolia has an exclusive team comprising members of CITA, Cabinet, General Information Agency, National Data Centre, and Communications Regulatory Commission for this purpose.

Netherlands – The new Digital Trust Centre will enhance information sharing and will be a platform for strengthening cybersecurity for non-vital sectors and companies. The aim is to create a cyber ecosystem that provides information and tailor-made perspectives for action. Moreover, a nationwide network of cybersecurity partnerships will be created to share cybersecurity information between public and private parties more widely, efficiently and effectively. The aim of this nationwide network is to strengthen the capabilities of public and private parties.

Other best practices include pilot projects with two major ports - Rotterdam (FERN) and Schiphol (CYSSIC); coordinated vulnerability disclosure; and continuously improving information sharing agencies.

Oman – OCERT, while managing and operating the ITU-Arab Regional Cyber Security Centre, organized the CyberGreen High-level meeting (Jan 2017, Oman) for focal points from different critical sectors

in Oman, which highlighted and demonstrated the ecosystem health metrics called CyberGreen for critical national information infrastructure sectors. It aimed to enhance the communication and incident response capabilities of the participating teams as well as to ensure a continued collective effort in mitigating cyber threats among the Arab States region national computer incident response teams (CIRTs).

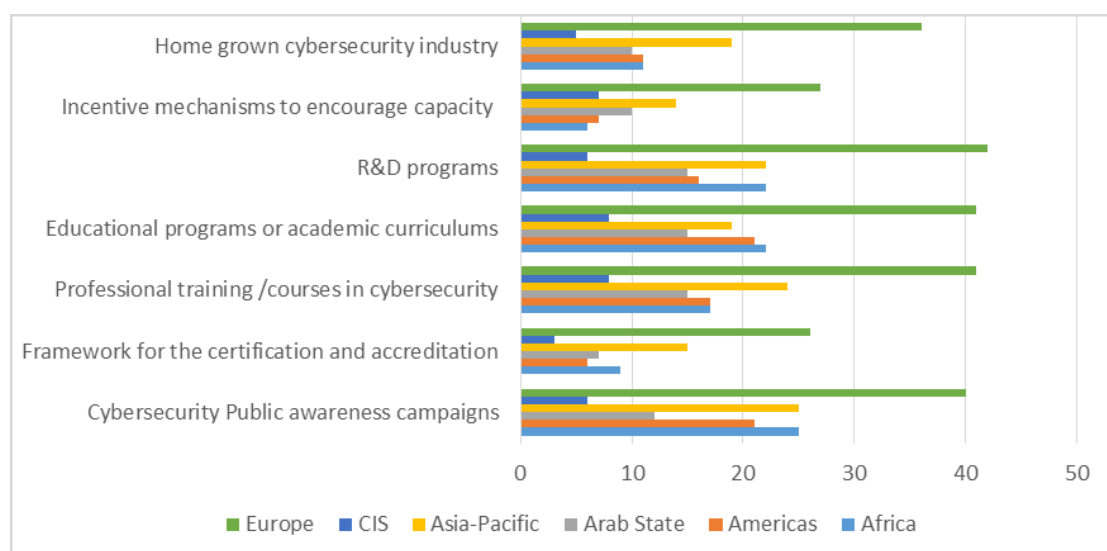
Singapore – The Cyber Security Agency of Singapore (CSA) was set up as a single national agency to oversee all cybersecurity matters, including cybersecurity strategy, operation, and education, outreach, and ecosystem development. As described in the Singapore National Cybersecurity Strategy, as the central agency, CSA oversees the protection of critical information infrastructure sectors, public education and outreach, industry development and international cooperation efforts. CSA has established a national structure that is able to maintain centralized oversight and maintenance of national cybersecurity, yet remain flexible in responding to sectoral needs, through its three-tier model (pages 16-17 of the National Cybersecurity Strategy of Singapore).

Rwanda – The National Cyber Security Policy (NCSP) addresses national risks, priorities and objectives and describes measures that address issues relating to public awareness raising, mitigation of cybercrime, incident response capability and critical national infrastructure protection. The establishment of the National Cyber Security Agency (NCSA) is tasked with implementing the National Cybersecurity Strategic Plan (NCSSP) 2015-2020, which provides an implementation guidance of the defined National Cyber Security Policy (NCSP).

The NCSP and NCSSP also facilitate capacity building and investments in cybersecurity; and cybersecurity related metrics and measurement processes have been established, being implemented and used to inform decision making.

Spain – The PILAR tool supporting risk analysis and management of information systems, and approved for use by NATO, has been adapted to comply with the new regulation for the protection of personal data of the EU (2016/679 of April 27, 2016) and has a large flexibility to adapt to new security domains. It is also being used by several agencies in the EU.

Figure 4: Commitment to the indicators in the capacity building pillar per region



### Capacity building

The following section reports on best practice provided by Member States that illustrate what is happening, achievements and progress taking place in each country relative to the capacity building pillar of the GCI.

Belgium – The Centre for Cybersecurity (CCB) has been reinforced to accelerate the efforts undertaken in the field of cybersecurity, with a comprehensive package of concrete measures. Belgium has held multiple campaigns, for example:

- campaign for young people and how to use the Internet;
- main guidelines for cybersecurity protection, GDPR compliance, and cybersecurity kits;
- special training programmes for cybersecurity readiness;
- Clicksafe for ChildFocus, an ICT security education programme.

Denmark – Research funds have been earmarked to research in new technologies, including cybersecurity. An initiative has been created with the goal of focusing on cybersecurity and information security throughout the educational system. With the national strategy, it has become a requirement that a dedicated cybersecurity and information security unit is created for each of the critical sectors in society (telecommunications, health, energy, finance, maritime, transportation) – central funding is provided for this. Each sector must develop a specific strategy, taking into consideration the specific threats and vulnerabilities that apply in the sector. The sector strategies are to be approved by a central government committee.

The government is establishing an information portal that will enable citizens, businesses and public authorities to protect themselves by making available relevant, specific and useful information and tools.

The Danish Business Authority and the Council for Digital Security launched a security check based on the ISO 27001 standard that generates an overview and benchmark of the company digital security, and guidelines on how to enhance it

Egypt – A national committee for Internet Safety and Child Online Protection (COP) was formed in June 2013, with the aim of activating a national strategy for protecting and empowering children online with the belief that empowerment is the key to online protection. The national COP Committee works on preventive, protective and corrective mechanisms addressing children, parents and educators. Committee membership reflects a unique public-private partnership including members from government (MCIT, NTRA, Ministry of Education, Ministry of Justice, Ministry of Interior, National Council for Childhood and Motherhood), private sector (Telecommunication operators: Telecom Egypt Data, Orange and Vodafone, ISPs, Microsoft, IBM, Oracle, Intel) and NGOs (Chamber of CIT, EITESAL), in addition to observers from international organizations (ITU and UNICEF). The national COP committee has produced awareness materials and publications on Internet Safety for children, and parents. The National Council for Childhood and Motherhood (NCCM) has been central to child protection in Egypt, including child online protection. The NCCM has a special child help line, and is a key member of the national COP committee.

Georgia – Georgia has built up cyber capacity in-house through on-the-job training and training of teacher measures. Technical teams participate in international competitions with other CERT representatives, often successfully. In addition, the Georgia technical community provides trainings to other country stakeholders and counterparts. Representatives participate as invited experts and trainers of some international training in information and cybersecurity.

Hungary – A radio programme is broadcast in Hungarian every second week on the online radio station ‘Radio Orient’ that deals exclusively with the newest issues of personal data protection in order to facilitate public awareness.

Japan – NISC discusses policies and programmes of cybersecurity human resource development with experts from industry, academia and government in the Research Committee on Promotion and Human Resource Development at the Cybersecurity Strategy Headquarters and the associated working group. A Cyber Security Human Resources Development Program has also been developed. Japan is drafting and consulting for opinion on a Working Group Report on Corporate Management with Security Mind (Draft) and a Working Group Report on Policy Collaboration on Cyber Security Human Resource Development (Draft). As of May, 2018, the National Cyber Training Center was established at NICT and is engaged in capacity building projects such as CYDER, CYBER COLOSSEO and SecHack 365.

Luxembourg – A Cyber Security Board and a Cybersecurity Competence Center have been implemented. Luxembourg has four public CERTs and seven private CERTs. Luxembourg has a research centre with 250 researchers in cybersecurity (SNT). Every year awareness campaigns for the general public are launched. Luxembourg promotes the development and use of the exchange platform MISPL. Every tool developed by CIRCL and CASES is put in open source and is at everyone’s disposal. Amongst these tools are: an exchange platform for threats, a risk analysis platform, a tool meant for the assessment of the maturity of businesses and to advise on security measures. As part of project Secure MJ, government approved youth centres have been secured: BEE SECURE and CASES have elaborated a security approach allowing the centre managers to comply with legal obligations (data protection), to physically secure their network (setting up of firewalls and anti-virus) and to train the educators to the risks that they and the young people could be exposed to. This project is presently being extended to reception centres for children (4-12 years old):

Netherlands – The Global Forum on Cyber Expertise (GFCE) is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. It was launched by the Netherlands and is a driver to the GFCE secretariat. Moreover, the Netherlands has initiated several cybersecurity initiatives via the GFCE. All projects are indicated on the website.

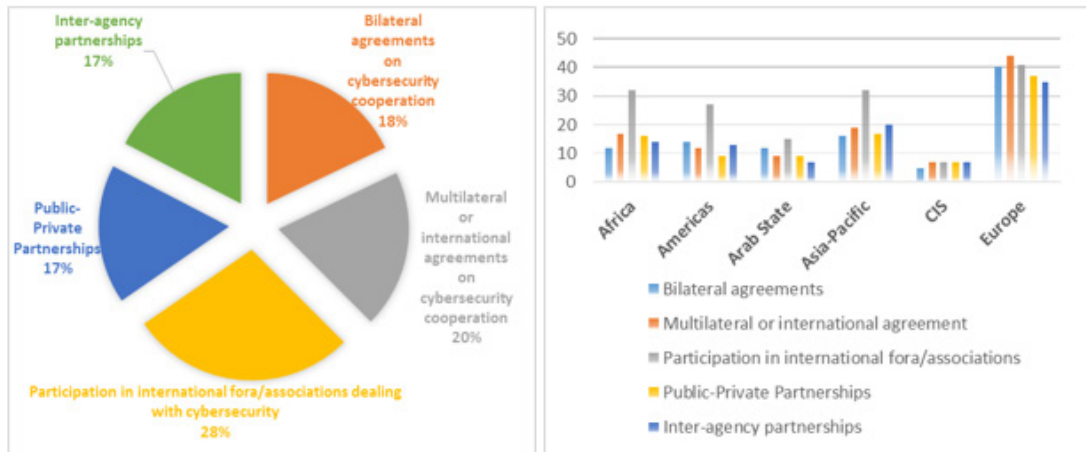
Singapore – The Ministry of Defence (MINDEF) will be training full-time national servicemen (NSF) as cyber defenders under a new scheme as part of its cyber-security strategy. The pilot scheme accepts applications from national service pre-enlistees, with 50 to 60 cyber specialists for the pilot batch, and 80 to 90 for subsequent batches. These cyber specialists will take classes under the Singapore Institute of Technology (SIT) cybersecurity degree once a week, while deployed in advance cyber defence roles such as penetration testing, cyber forensics, and malware analysis. The classes earn academic credits for a subsequent SIT degree. In addition to the cyber specialists, the Cyber NSF scheme also includes NSF cyber operators performing more basic roles such as round-the-clock monitoring and analysis. The Cyber NSF scheme represents the first work-learn programme where NSFs can attend academic courses while employed in an operational role.

The SkillsFuture Series is a curated list of short, industry-relevant training programmes that focus on emerging skills. Cybersecurity is one of the eight identified categories under this series. To ensure course fees remain affordable, SkillsFuture Singapore (SSG) will provide up to a 70 per cent subsidy for Singapore citizens and permanent residents. Individuals can offset the remaining course fees using their SkillsFuture credit. Eligible individuals can further benefit from other SSG subsidies up to 95 per cent.

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

The Cybersecurity Challenge Singapore is a series of challenges and competitions designed to inspire and spur cyber enthusiasts to join the cybersecurity profession. One component of the challenge is

Figure 5: Commitment to the indicators in the cooperation pillar per region.



a Singapore floor on CyPhinx (a virtual skyscraper), an initiative arising from the memorandum of understanding (MoU) signed between CSA and the Cabinet office of the United Kingdom.

The Cybersecurity Career Mentoring Programme, jointly organized by CSA and the Singapore Computer Society, aims to connect students and young professionals with industry mentors. During each quarterly session, industry practitioners and leaders provide mentorship and guidance to students and young aspiring professionals keen to pursue cybersecurity as a profession. Participants can use these programmes to address their queries as they make their decision to enter the cybersecurity profession. Through these sessions, participants gain insights into opportunities offered by cybersecurity as a career and the various ways they can develop professionally in each of the cybersecurity specializations.

Turkey – An online cybersecurity competition, Cyber Star, was organized in January 2017. Over 27 000 applications were received, with about 15 000 competitors. The competition identified cybersecurity experts in the country and some of the successful competitors were hired by TRCERT (Turkey National CERT). TRCERT participated in the NATO CMX-2017 Crisis Management Exercise in October 2017 and in the National Cyber Defense Exercise in November 2017.

The Safe Internet Center (SIC) was established to increase awareness regarding the proper and safe use of the Internet. SIC operates an Internet Helpline, and Safe Web, a website where families can find advice on how to make the best use of the Internet. The Safer Internet Trailer provides children and young people who have limited access to ICTs with a platform where they can experience technology closely, and learn the opportunities it provides. The Trailer raises awareness about safe use of Internet for children, and consists of five facilities: Technological Experience Area, Robotic Coding Area, Virtual Reality Area, Conscious and Safe Usage of Internet Area, Training Area, and Competition Area. SIC also operates a specialized website for children, which involves games, activities, competitions and trainings. SIC has organized the Safer Internet Day event with the main theme of "Create, connect and share respect: A better Internet starts with you". ICTA and Bahçeşehir University launched a board game contest to encourage young people aged 12-18 to design a game, and during this event, Facebook and Google conducted workshops for students on digital games and safer Internet.

### Cooperation

The following section reports on best practice provided by Member States that illustrate what is happening, achievements and progress taking place in each Member State relative to the cooperation pillar of the GCI.



Estonia – As one of the first countries in the world to create a cybersecurity strategy in 2008, the current strategy is in force until end of 2018, consultations and writing is ongoing for the next generation (fourth) strategy that will begin on 1 January 2019 for four years. The Estonian Information Security Association (EISA) was officially founded in January 2018. The role of the EISA is to boost cross-sectorial cooperation in Estonia between academia and private sector as well as with the government, including supporting the EU contractual Public Private Partnership (cPPP) model on cybersecurity. The joint effort intends to formalize existing ties and enhance R&D activities in the information security and cybersecurity field in Estonia. The EISA will also be part of the next generation strategy “Estonian Cybersecurity Strategy for 2019-2022”.

Hungary – As a founding member of the Global Forum on Cyber Expertise (GFCE) and co-initiator of the initiative on Coordinated Vulnerability Disclosure, Hungary actively engages with partners within the GFCE and share information and best practices on a number of issues (cyber incidents, critical information infrastructure protection, etc.).

Based on the recently adopted Delhi Communiqué, Hungary participates in a number of working groups aiming to implement the Global Agenda for Cyber Capacity Building.

GovCERT-Hungary works in close cooperation with the European Union Agency for Network and Information Security (ENISA) on several cybersecurity related questions – not only in working groups and different researches, but at a technical level. GovCERT Hungary takes part in an EU level project called Project Smart 2014/1079, which aims to define and create a core service platform for the cooperation of CSIRTs within the EU. The new platform (still under development and testing) is named MeliCERTes.

Lithuania – The Cyber Security Council, a permanent consultative body, comprising state institutions responsible for formulation and implementation of national cybersecurity policy, other stakeholders from state institutions, representatives from public and private sector, representing managers of critical information infrastructure and state information infrastructure, business, industry and academia working in the area of cybersecurity, meets on regular basis and provides advice on further development and improvement of cybersecurity in Lithuania.

The Cyber Security Information Network provides an electronic secure platform to share cyber incidents information, facilitate incident notification and management and to provide some malicious software containment tools. Access to the Cyber Security Information Network is restricted to users from public and private sectors meeting specific criteria.

Accounting for countries that might need external support in case of large scale or specific cyber incidents, Lithuania has initiated the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security cooperation project. The overall project objective is to develop new cyber capabilities that would be able to support EU Member States, partners, EU institutions and common security and defence policy missions by working as a team, using a unified set of cyber tools, and participating in common exercises.

In 2017, a joint initiative, by the Lithuanian Criminal Police Bureau and the biggest telecommunication service provider Telia, was launched to reduce availability and dissemination of certain material online. The necessary technical measures to stop Telia clients from accessing such material/resources meant that access is blocked to any Telia client attempting to access such resources from the Telia network, and the resource is replaced by a “stop page”, informing the client that he/she is attempting to reach unlawful content.

Malawi – Malawi has been fully involved in the process of preparing the African Union Convention on the establishment of a credible legal framework for cybersecurity in Africa. Article II of the Convention provides that each Member State shall adopt the measures required to establish and maintain cross-border collaboration with other CERT/CSIRT at regional and global levels. Member States may join existing early warning and surveillance networks (WSN) such as FIRST (Forum for

Incident Response and Security Team), the European Government CERTs (EGC) group, and others. Malawi will implement this Article, the MW-CERT has already been initiated and is in progress.

In March 2018, MACRA signed a cooperation agreement with ITU for assisting Malawi to establish the national CERT (MW-CERT) to serve as a trusted, central coordination point of contact for cybersecurity. Further, MACRA organized a workshop in March 2018, facilitated by ITU to assist Malawi in the assessment of its readiness to implement a national CERT.

Oman – Oman fully participates in international fora, such as the providing a Co-Chair of ITU Study Group 17 on standardization on cybersecurity, and delivering a workshop on cybersecurity at ITU World Summit on the Information Society (WSIS) in cooperation with the United Nations International Computing Centre.

Oman hosts events promoting cybersecurity, such as Oman activities on Safer Internet Day, which were published in the European BIK portal due to their success. Oman also conducts an annual Regional Cyber Security Summit for the Arab States region, in addition to the ITU-FIRST Regional Symposium for Africa and Arab Regions, and cyber drill in Tanzania. Oman also develops scenarios and conducts annual regional cyber drills and cybersecurity workshops in cooperation with third party institutions such as Chatham House.

OmanCERT has obtained international accreditation for the national digital forensics lab, is ranked in the top 100 chief information security officers (CISO) in the women leadership category of the region, and reached third place in the regional CTF (capture the flag) hacking competition. Through the ITU Arab Regional Cybersecurity Centre (ITU-ARCC), Oman supports other countries both in the Arab States region and internationally by sharing their expertise, and has assisted Member States to gain FIRST (Forum for Incident Response and Security Team) membership by sponsoring other CIRTs.

Singapore –Through memorandum of understanding (MoU) with other countries, Singapore has established channels for information exchange on cyber threats and incidents. This provides us with early warning information on real cyber threats and incidents around the world. One example is the outbreak of the WannaCry ransomware in May 2017, during which CSA received the initial alert from the GCHQ-NCSC in the UK.

In reference to, CSA and the Infocomm Media Development Authority of Singapore (IMDA) have established a public-private partnership, the Cyber Security Associates and Technologists Programme (CSAT), to train and up-skill ICT professionals to acquire practical skills for specialized job roles for cybersecurity operations. The programme is aimed at helping fresh and mid-career ICT individuals attain the necessary practical skills to better equip them for cybersecurity roles and positions. CSA and IMDA will collaborate with industry partners for the training and up-skilling of ICT professionals.

The annual Singapore International Cyber Week (SICW) is a premier platform that brings together global leaders across government, industry, NGOs and academia to discuss a broad range of important cybersecurity issues. SICW 2017 attracted over 7 000 international and regional policy makers, thought leaders, industry experts and visitors from close to 50 countries to connect, forge partnerships and engage in multi-faceted exchanges and critical knowledge-sharing. Singapore will host SICW 2018 from 18 to 20 September 2018.

The Association of Southeast Asian Nations (ASEAN) Cyber Capacity Programme (ACCP) is an example of the Singapore approach to cybersecurity cooperation with SGD 10 million support over five years. The ACCP takes a modular, multi-disciplinary and multi-stakeholder approach to building cybersecurity capacity for all ASEAN Member States across technical and policy aspects.

Through partnerships with relevant stakeholders from other governments, industry, academia and NGOs, the ACCP has managed to provide training for more than 120 Director/Deputy Director-level officials from all ASEAN Member States in a broad range of cybersecurity-related issues, including cyber norms, international law in cyberspace, cybersecurity strategy building and legislation development, incident response and critical information infrastructure protection. The contribution of the

ACCP has been acknowledged in official documents, most recently in the ASEAN Leaders' Statement on Cybersecurity Cooperation.

Singapore provides cornerstone sponsorship for the CyberGreen initiative, alongside Japan and the United Kingdom. CyberGreen is a global non-profit organization that develops and publishes risk-based common metrics for assessing cyber risks and vulnerable servers across the world's networks. It also works with partners to make cyberspace clean and more resilient to cyber-attacks. Singapore provides all ASEAN Member States with access to the CyberGreen portal to gauge their own cyber health status, so that risk levels are better understood and the efficacy of mitigation strategies can be more accurately monitored.

Spain – The National Cybersecurity Council strengthens the relations of coordination, collaboration and cooperation between the different public administrations with responsibilities in the field of cybersecurity and between the public and private sectors. The composition of the National Cybersecurity Council reflects the spectrum of areas covered by the departments, agencies and agencies of the public authorities with responsibilities in the field of cybersecurity, in order to coordinate actions that must be addressed together with the objective of increasing security levels. Other relevant actors of the private sector and specialists whose contribution is considered necessary can take part in the Committee.

Sudan – The government of Sudan together with the International Telecommunication Union organized a three-day workshop on cybersecurity strategy in the Africa region at the National Telecommunication Corporation (NTC) headquarters in Khartoum. The main objectives of the workshop was to build capacity, to share experiences and best practices in countries, to provide information regarding the status of implementations of existing cybersecurity strategies; to identify any gaps; and to devise a way forward. The workshop brought together leading specialists in the field, from developing countries, ITU Member States, regulatory agencies, policy makers, private sector (service providers, telecommunication operators, manufacturers and solution providers), academia, standardization organizations, forums and consortia.

Uzbekistan – Cooperation agreements with the member states of the Commonwealth of Independent States (CIS) to combat crimes in the field of information technology have been signed, as well as the regional anti-terrorist structure of the Shanghai Cooperation Organization (SCO) agreement to counter cybersecurity.

## 7 Conclusion

The GCI 2018 edition builds on the previous editions. Measuring progress towards the cybersecurity commitment of Member States globally is a complex task which entails striking a balance between different dimensions of cybersecurity experiences in different countries. The GCI brings together 25 indicators concerned with legislative measures, technical mechanisms, organizational structures, capacity building activities and cooperative arrangements into a composite index that reflects high levels of diversity and complexity.

The GCI originally succeeded in measuring commitment to cybersecurity and generated interest on cybersecurity assessment among Member States. As recognized at the ITU Plenipotentiary Conference in Dubai Resolution 130 (Rev. Dubai, 2018) on strengthening the role of ITU in building confidence and security in the use of information and communication technologies, GCI has motivated countries to intensify their efforts in cybersecurity, raised awareness in countries for the need to start bilateral cooperation, and increased visibility of what countries are doing in cybersecurity.

The survey shows that countries are becoming more responsive to the aims of the GCI project, with 155 out of 194 Member States providing data that captures the cybersecurity commitment, as well as providing information on their own best practice. The level of awareness and commitment worldwide has visibly improved.

The survey shows more progress and more commitment in the legal pillar with Benin, Estonia and Poland bringing in new laws on cybercrime, Zimbabwe, Zambia, Egypt, South Africa, and Eswatini (formerly known as Swaziland) have new draft cybercrime laws, and Uganda is drafting its data/privacy protection legislation. In the organizational pillar, some Member States including Australia, Botswana, Canada, Czech Republic, Denmark, Japan, Jordan, Netherlands, Spain, Samoa, Singapore, and Luxembourg have updated national cybersecurity strategies, while Cameroon, Malawi, Tanzania and Zimbabwe are in the process of drafting theirs.

A risk assessment-based approach to cybersecurity allows an adjustment to the changing threats each country faces, and despite this, the survey shows only 53 per cent (about 92) of Member States carry out cybersecurity risk assessments. The framework and standards discussed in the GCI survey provides recommendations to countries thinking at a programmatic and also an individual control level. As it is noted during the GCI data collection, there is no one-size-fits-all tailored solution to address cybersecurity.

It is also notable that, as in previous years, most countries have improved their GCI values. Overall GCI rankings can undergo dramatic ranking changes, in 2018 this is most notably in the Europe region, whilst in all pillars, the Africa region and the Americas region scores have changed little.

Looking forward, cooperation will play a major role in cybersecurity development. With the increasing interest in cybersecurity knowledge sharing and transfer in organizations, cooperation among relevant stakeholders such as central government, local public authorities, the private sector, academia, civil society, and international organizations, being a key factor. This can only be accomplished through collaboration and communication. As such, the Global Forum on Cyber Expertise (GFCE)<sup>1</sup>, the Global Commission on the Stability of Cyberspace (GCSC)<sup>2</sup>, the Internet Governance Forum (IGF)<sup>3</sup>, the Commonwealth Telecommunication Organization (CTO)<sup>4</sup> and the Global Cyber Security Capacity Centre (GCSCC)<sup>5</sup> offer international forums where cybersecurity solutions can find ways forward, from areas of technology, to sharing of best practices. Government officials need to take these opportunities to learn more from other outstanding organizations to find ways on how to protect their nations from cyber-attacks.

<sup>1</sup> <https://www.thegfce.com>

<sup>2</sup> <https://cyberstability.org/>

<sup>3</sup> <https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1>

<sup>4</sup> <https://cto.int/strategic-goals/cybersecurity/>

<sup>5</sup> <https://www.oxfordmartin.ox.ac.uk/cybersecurity/>

ITU calls upon Member States to join the initiatives carried out in their regions to provide support in cybersecurity awareness and capacity building. In the Africa region, Member States can participate in the ECOWAS<sup>6</sup> Convention on Cybersecurity, the SADC<sup>7</sup> cyber drills and capacity building activities and the East African Initiatives<sup>8</sup>. In the Americas, the Organization of the American States (OAS)<sup>9</sup> is helping its Member States in the fight against cybercrime. In the Asia-Pacific region, the ASEAN Cooperation on Cybersecurity is building cooperation and coordination among ASEAN<sup>10</sup> Member States on cybersecurity policy development and capacity building initiatives. In the Europe region, there are many organizations and initiatives working on enhancing the effectiveness of cybersecurity in the region such as, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)<sup>11</sup>, the Council of Europe (COE)<sup>12</sup>, and the Organization for Security and Cooperation in Europe (OSCE)<sup>13</sup>.

The GCI continues to contribute to the cybersecurity awareness in the least developed countries providing capacity building activities through the production of guidelines on cybersecurity legislation, regulation and technology, asserting the need and importance for countries to establish national computer incident response teams (CIRTs) and providing fundamental tools to develop a national cybersecurity strategies. Countries can also consider the use of the ITU Guide to Developing a National Cybersecurity Strategy<sup>14</sup> as a toolkit to support the creation or enhancement of their national strategy. These are critical elements and frameworks for any country's socio-economic security.

To have more effectiveness in promoting awareness of ICT development and trends, the success of this extensive data-gathering effort depends heavily on the response rate to the questionnaire. Accordingly, ITU calls upon all Member States, industry stakeholders, academia, NGOs and all interested individuals to actively take part in the GCI exercises. The future GCI survey will offer more opportunities for open consultation with ITU Member States and relevant stakeholders and will be an exercise with results reported at various forums such as ITU-D Study Group Meeting and the WSIS Forum. The goal of this initiative is to help foster a global culture of cybersecurity and to ensure its integration at the core of ICT developments.

<sup>6</sup> <http://www.ecowas.int/?s=CYBERSECURITY>

<sup>7</sup> <https://www.sadc.int/news-events/news/sadc-convenes-cyber-security-workshop-and-sadc-regional-cyber-drill/>

<sup>8</sup> <https://africabusinesscommunities.com/tech/tech-news/east-africa-cybersecurity-clinic-launched/>

<sup>9</sup> [http://www.oas.org/en/topics/cyber\\_security.asp](http://www.oas.org/en/topics/cyber_security.asp)

<sup>10</sup> <http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf>

<sup>11</sup> <https://ccdcoe.org/index.html>

<sup>12</sup> <https://70.coe.int/achievements>

<sup>13</sup> <https://www.osce.org/cyber-ict-security>

<sup>14</sup> [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-CYB\\_GUIDE.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf)

## List of abbreviations

<b>AfricaCERT</b>	Computer Emergency Response Team of Africa
<b>APCERT</b>	Asia-Pacific Computer Emergency Response Team
<b>CERT</b>	Computer Emergency Response Team
<b>CIIP</b>	Critical Information Infrastructure Protection
<b>CIRT</b>	Computer Incident Response Team
<b>CIS</b>	Commonwealth of Independent States
<b>COP</b>	Child Online Protection
<b>CSIRT</b>	Computer Security Incident Response Team
<b>FIRST</b>	Forum of Incident Response and Security Teams
<b>GCA</b>	Global Cybersecurity Agenda
<b>GCI</b>	Global Cybersecurity Index
<b>GOVCERT</b>	Governmental Computer Emergency Response Team
<b>IASPs</b>	Internet Access Service Providers
<b>ICT</b>	Information and Communication Technology
<b>IDI</b>	ICT Development Index
<b>ISACA</b>	Information Systems Audit and Control Association
<b>ISCB</b>	Information Security Certification Body
<b>ISP</b>	Internet Service Provider
<b>ITU</b>	International Telecommunication Union
<b>NATO</b>	North Atlantic Treaty Organization
<b>NCS</b>	National Cybersecurity Strategy
<b>NCSC</b>	The National Cyber Security Centre
<b>R&amp;D</b>	Research and Development
<b>UN</b>	United Nations

## Annex A: Regional ranking GCI 2018

The countries marked with an \* are countries that did not participate in GCI 2018. They have neither submitted their answers to the questionnaire nor validated the data collected by the GCI team.

### Africa

Member State	Score	Regional Rank	Global Rank
Mauritius	0.880	1	14
Kenya	0.748	2	44
Rwanda	0.697	3	49
South Africa	0.652	4	56
Nigeria	0.650	5	57
Tanzania	0.642	6	59
Uganda	0.621	7	65
Benin	0.485	8	80
Cote d'Ivoire	0.456	9	85
Botswana	0.440	10	87
Ghana	0.437	11	89
Zambia	0.436	12	90
Cameroon	0.432	13	91
Burkina Faso	0.400	14	96
Gabon	0.318	15	100
Senegal	0.305	16	102
Gambia	0.280	17	104
Ethiopia	0.278	18	105
Malawi	0.275	19	106
Seychelles	0.259	20	110
Liberia	0.206	21	117
Madagascar	0.196	22	119
Guinea	0.191	23	122
Zimbabwe	0.186	24	124
Congo	0.167	25	130
Mozambique	0.158	26	132

Member State	Score	Regional Rank	Global Rank
Sierra Leone	0.138	27	136
Eswatini	0.133	28	137
Namibia	0.127	29	141
Chad	0.098	30	147
Angola	0.097	31	148
Niger	0.094	32	150
Burundi	0.087	33	151
Togo	0.087	33	151
Mali	0.085	34	152
South Sudan	0.065	35	157
Sao Tome and Principe	0.064	36	158
Guinea-Bissau	0.055	37	162
Cabo Verde	0.051	38	163
Lesotho	0.051	38	163
Central African Republic	0.036	39	167
Equatorial Guinea	0.031	40	168
Eritrea	0.020	41	171
Democratic Republic of the Congo	0.008	42	174

### Americas

Member State	Score	Regional Rank	Global Rank
United States of America	0.926	1	2
Canada	0.892	2	9
Uruguay	0.681	3	51
Mexico	0.629	4	63
Paraguay	0.603	5	66
Brazil	0.577	6	70
Colombia	0.565	7	73
Cuba	0.481	8	81
Chile	0.438	9	88
Dominican Republic	0.430	10	92



Member State	Score	Regional Rank	Global Rank
Jamaica	0.407	11	94
Argentina	0.407	11	94
Peru	0.401	12	95
Panama	0.369	13	97
Ecuador	0.367	14	98
Venezuela	0.354	15	99
Guatemala	0.251	16	112
Antigua and Barbuda	0.247	17	113
Costa Rica	0.221	18	115
Trinidad and Tobago	0.188	19	123
Barbados	0.173	20	127
Saint Vincent and the Grenadines	0.169	21	129
Bahamas	0.147	22	133
Grenada	0.143	23	134
Bolivia	0.139	24	135
Guyana	0.132	25	138
Nicaragua	0.129	26	140
Belize	0.129	26	140
El Salvador	0.124	27	142
Suriname	0.110	28	144
Saint Lucia	0.096	29	149
Saint Kitts and Nevis	0.065	30	157
Haiti	0.046	31	164
Honduras	0.044	32	165
Dominica	0.019	33	172

#### Arab States

Member State	Score	Regional Rank	Global Rank
Saudi Arabia	0.881	1	13
Oman	0.868	2	16
Qatar	0.860	3	17

Member State	Score	Regional Rank	Global Rank
Egypt	0.842	4	23
United Arab Emirates	0.807	5	33
Kuwait	0.600	6	67
Bahrain	0.585	7	68
Jordan	0.556	8	74
Tunisia	0.536	9	76
Morocco	0.429	10	93
State of Palestine	0.307	11	101
Sudan	0.294	12	103
Iraq	0.263	13	107
Algeria	0.262	14	108
Syrian Arab Republic	0.237	15	114
Libya	0.206	16	117
Lebanon	0.186	17	124
Mauritania	0.107	18	145
Somalia	0.070	19	156
Djibouti	0.063	20	159
Yemen	0.019	21	172
Comoros	0.015	22	173

### Asia-Pacific

Member State	Score	Regional Rank	Global Rank
Singapore	0.898	1	6
Malaysia	0.893	2	8
Australia	0.890	3	10
Japan	0.880	4	14
Republic of Korea	0.873	5	15
China	0.828	6	27
Thailand	0.796	7	35
New Zealand	0.789	8	36
Indonesia	0.776	9	41

Member State	Score	Regional Rank	Global Rank
India	0.719	10	47
Viet Nam	0.693	11	50
Philippines	0.643	12	58
Iran	0.641	13	60
Brunei Darussalam	0.624	14	64
Bangladesh	0.525	15	78
Sri Lanka	0.466	16	83
Mongolia	0.465	17	84
Pakistan	0.407	18	94
Samoa	0.367	19	98
Nepal	0.260	20	109
Tonga	0.208	21	116
Lao	0.195	22	120
Fiji	0.194	23	121
Bhutan	0.181	24	125
Afghanistan	0.177	25	126
Myanmar	0.172	26	128
Cambodia	0.161	27	131
Papua New Guinea	0.131	28	139
Nauru	0.101	29	146
Vanuatu	0.098	30	147
Timor-Leste	0.082	31	153
Marshall Islands	0.072	32	155
Solomon Islands	0.061	33	160
Tuvalu	0.057	34	161
Micronesia	0.040	35	166
Kiribati	0.028	36	169
Democratic People's Republic of Korea	0.020	37	171
Maldives	0.004	38	175

## CIS

Member State	Score	Regional Rank	Global Rank
Russian Federation	0.836	1	26
Kazakhstan	0.778	2	40
Uzbekistan	0.666	3	52
Azerbaijan	0.653	4	55
Belarus	0.578	5	69
Armenia	0.495	6	79
Tajikistan	0.263	7	107
Kyrgyzstan	0.254	8	111
Turkmenistan	0.115	9	143

## Europe

Member State	Score	Regional Rank	Global Rank
United Kingdom	0.931	1	1
France	0.918	2	3
Lithuania	0.908	3	4
Estonia	0.905	4	5
Spain	0.896	5	7
Norway	0.892	6	9
Luxembourg	0.886	7	11
Netherlands	0.885	8	12
Georgia	0.857	9	18
Finland	0.856	10	19
Turkey	0.853	11	20
Denmark	0.852	12	21
Germany	0.849	13	22
Croatia	0.840	14	24
Italy	0.837	15	25
Austria	0.826	16	28
Poland	0.815	17	29
Belgium	0.814	18	30

Member State	Score	Regional Rank	Global Rank
Hungary	0.812	19	31
Sweden	0.810	20	32
The Republic of North Macedonia	0.800	21	34
Switzerland	0.788	22	37
Ireland	0.784	23	38
Israel	0.783	24	39
Portugal	0.758	25	42
Monaco	0.751	26	43
Latvia	0.748	27	44
Slovakia	0.729	28	45
Bulgaria	0.721	29	46
Slovenia	0.701	30	48
Moldova	0.662	31	53
Ukraine	0.661	32	54
Cyprus	0.652	33	56
Serbia	0.643	34	58
Montenegro	0.639	35	61
Albania	0.631	36	62
Czech Republic	0.569	37	71
Romania	0.568	38	72
Liechtenstein	0.543	39	75
Greece	0.527	40	77
Malta	0.479	41	82
Iceland	0.449	42	86
Bosnia and Herzegovina	0.204	43	118
Andorra	0.115	44	143
San Marino	0.075	45	154
Vatican	0.021	46	170

## Annex B: Global ranking GCI 2018

The countries marked with an \* are countries that did not participate in GCI 2018. They have neither submitted their answers to the questionnaire nor validated the data collected by the GCI team.

Member State	Score	Global Rank
United Kingdom	0.931	1
United States of America*	0.926	2
France	0.918	3
Lithuania	0.908	4
Estonia	0.905	5
Singapore	0.898	6
Spain	0.896	7
Malaysia	0.893	8
Canada*	0.892	9
Norway	0.892	9
Australia	0.890	10
Luxembourg	0.886	11
Netherlands	0.885	12
Saudi Arabia	0.881	13
Japan	0.880	14
Mauritius	0.880	14
Republic of Korea	0.873	15
Oman	0.868	16
Qatar	0.860	17
Georgia	0.857	18
Finland	0.856	19
Turkey	0.853	20
Denmark	0.852	21
Germany	0.849	22
Egypt	0.842	23
Croatia	0.840	24
Italy	0.837	25
Russian Federation	0.836	26

Member State	Score	Global Rank
China	0.828	27
Austria*	0.826	28
Poland	0.815	29
Belgium	0.814	30
Hungary	0.812	31
Sweden*	0.810	32
United Arab Emirates	0.807	33
The Republic of North Macedonia	0.800	34
Thailand	0.796	35
New Zealand*	0.789	36
Switzerland	0.788	37
Ireland	0.784	38
Israel*	0.783	39
Kazakhstan	0.778	40
Indonesia	0.776	41
Portugal	0.758	42
Monaco	0.751	43
Kenya	0.748	44
Latvia	0.748	44
Slovakia	0.729	45
Bulgaria*	0.721	46
India	0.719	47
Slovenia*	0.701	48
Rwanda	0.697	49
Viet Nam	0.693	50
Uruguay	0.681	51
Uzbekistan	0.666	52
Moldova	0.662	53
Ukraine	0.661	54
Azerbaijan	0.653	55
South Africa	0.652	56

Member State	Score	Global Rank
Cyprus*	0.652	56
Nigeria	0.650	57
Philippines	0.643	58
Serbia	0.643	58
Tanzania	0.642	59
Iran	0.641	60
Montenegro	0.639	61
Albania	0.631	62
Mexico	0.629	63
Brunei Darussalam*	0.624	64
Uganda	0.621	65
Paraguay	0.603	66
Kuwait	0.600	67
Bahrain	0.585	68
Belarus	0.578	69
Brazil	0.577	70
Czech Republic	0.569	71
Romania	0.568	72
Colombia	0.565	73
Jordan	0.556	74
Liechtenstein	0.543	75
Tunisia	0.536	76
Greece	0.527	77
Bangladesh	0.525	78
Armenia	0.495	79
Benin	0.485	80
Cuba	0.481	81
Malta	0.479	82
Sri Lanka	0.466	83
Mongolia	0.465	84
Cote d'Ivoire	0.456	85



Member State	Score	Global Rank
Iceland	0.449	86
Botswana	0.440	87
Chile	0.438	88
Ghana	0.437	89
Zambia	0.436	90
Cameroon	0.432	91
Dominican Republic	0.430	92
Morocco	0.429	93
Jamaica	0.407	94
Pakistan	0.407	94
Argentina	0.407	94
Peru	0.401	95
Burkina Faso	0.400	96
Panama	0.369	97
Samoa	0.367	98
Ecuador	0.367	98
Venezuela	0.354	99
Gabon	0.318	100
State of Palestine	0.307	101
Senegal	0.305	102
Sudan	0.294	103
Gambia	0.280	104
Ethiopia*	0.278	105
Malawi	0.275	106
Tajikistan*	0.263	107
Iraq	0.263	107
Algeria	0.262	108
Nepal	0.260	109
Seychelles	0.259	110
Kyrgyzstan	0.254	111
Guatemala	0.251	112

Member State	Score	Global Rank
Antigua and Barbuda	0.247	113
Syrian Arab Republic	0.237	114
Costa Rica*	0.221	115
Tonga	0.208	116
Libya	0.206	117
Liberia	0.206	117
Bosnia and Herzegovina	0.204	118
Madagascar	0.196	119
Lao*	0.195	120
Fiji	0.194	121
Guinea	0.191	122
Trinidad and Tobago	0.188	123
Zimbabwe	0.186	124
Lebanon	0.186	124
Bhutan	0.181	125
Afghanistan	0.177	126
Barbados	0.173	127
Myanmar	0.172	128
Saint Vincent and the Grenadines	0.169	129
Congo	0.167	130
Cambodia	0.161	131
Mozambique	0.158	132
Bahamas	0.147	133
Grenada	0.143	134
Bolivia	0.139	135
Sierra Leone	0.138	136
Eswatini	0.133	137
Guyana	0.132	138
Papua New Guinea*	0.131	139
Nicaragua	0.129	140
Belize	0.129	140

Member State	Score	Global Rank
Namibia	0.127	141
El Salvador*	0.124	142
Turkmenistan*	0.115	143
Andorra	0.115	143
Suriname	0.110	144
Mauritania*	0.107	145
Nauru*	0.101	146
Chad*	0.098	147
Vanuatu	0.098	147
Angola*	0.097	148
Saint Lucia	0.096	149
Niger	0.094	150
Burundi	0.087	151
Togo	0.087	151
Mali*	0.085	152
Timor-Leste*	0.082	153
San Marino*	0.075	154
Marshall Islands*	0.072	155
Somalia	0.070	156
South Sudan*	0.065	157
Saint Kitts and Nevis	0.065	157
Sao Tome and Principe*	0.064	158
Djibouti	0.063	159
Solomon Islands*	0.061	160
Tuvalu*	0.057	161
Guinea-Bissau*	0.055	162
Cabo Verde*	0.051	163
Lesotho*	0.051	163
Haiti	0.046	164
Honduras	0.044	165
Micronesia*	0.040	166

Member State	Score	Global Rank
Central African Republic	0.036	167
Equatorial Guinea	0.031	168
Kiribati	0.028	169
Vatican*	0.021	170
Eritrea*	0.020	171
Democratic People's Republic of Korea*	0.020	171
Dominica	0.019	172
Yemen*	0.019	172
Comoros	0.015	173
Democratic Republic of the Congo*	0.008	174
Maldives*	0.004	175

## Annex C: Definition of indicators

### C.1 Legal measures

#### C.1.1 Cybercriminal legislation

Cybercrime legislation designates laws on the unauthorized (without right) access, interference, interception of computers, systems and data. This also includes procedural law, and any existing articles on the expedited preservation of stored computer data, production orders, real-time collection of computer data, extradition, mutual assistance, confidentiality and limitation on use; as well as any case law on cybercrime or computer misuse.

#### C.1.2 Cybersecurity regulation

Cybersecurity regulation designates laws dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection, digital signatures and e-transactions, and the liability of Internet service providers.

#### C.1.3 Containment/curbing of spam legislation

Refers to legislation/regulations related to the protection against unwanted emails as a result of Internet use.

### C.2 Technical measures

#### C.2.1 National, government, sectorial CERT/CIRT/CSIRT

CIRT refers to a computer incident response team, CSIRT refers to computer security incident response team, and CERT refers to computer emergency response team. A national CERT/CIRT/CSIRT refers to the establishment of a CIRT/CERT/CSIRT with national responsibility that provides the capabilities to identify, defend, respond and manage cyber threats and enhance cyberspace security. This ability needs to be coupled with the gathering of its own intelligence instead of relying on secondary reporting of security incidents whether from the CIRT constituencies or from other sources. A Government CERT/CIRT/CSIRT is an entity that responds to computer security or cybersecurity incidents which affects solely governmental institutions. Apart from reactive services, it may also engage in proactive services such as vulnerability analysis and security audits. Unlike the national CIRT/CERT/CSIRT, which services both the private and public sectors, the Government CERT provides its services to constituents from the public sector only and a sectoral CERT/CIRT/CSIRT is an entity that responds to computer security or cybersecurity incidents that affect a specific sector. Sectoral CERTs are usually established for critical sectors such as healthcare, public utilities, emergency services and the financial sectors. Unlike the Government CERT, which services the public sector, the sectoral CERT provides its services to constituents from a single sector only.

#### C.2.2 Cybersecurity standards implementation framework for organizations

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within the critical infrastructure (even if operated by the private sector). These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.

#### C.2.3 Standardization body

Standardization is a good indicator of the level of maturity of a technology, and the emergence of new standards in key areas underlines the vital importance of standards. Although cybersecurity has always been an issue for national security and treated differently in different countries, common

approaches are supported by commonly recognized standards. These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc. This indicator measures the existence of a national cybersecurity standardization body and activities in the development and implementation of cybersecurity standards.

#### **C.2.4 Technical mechanisms and capabilities deployed to address spam**

Tools and technical measures related to providing cybersecurity such as anti-virus or anti-spam software

#### **C.2.5 Use of cloud for cybersecurity purpose**

A software to ensure data backup in case of unwanted Internet or computer interference apart from the use of antivirus software, Internet security software suits, anti-malware and encryption to improve on governments cybersecurity systems. The cloud system allows one to use and access their documents/data or any saved materials anywhere and at any time without the damages caused by computer interference on one end.

#### **C.2.6 Child online protection mechanisms**

This indicator measure the existence of a national agency dedicated to Child Online Protection, the availability of a national telephone number to report issues associated with children online, any technical mechanisms and capabilities deployed to help protect children online, and any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online.

### **C.3 Organizational measures**

#### **C.3.1 Strategy**

The development of policy to promote cybersecurity is recognized as a top priority. A national strategy for cybersecurity should maintain resilient and reliable information infrastructure and aim to ensure the safety of citizens; protect the material and intellectual assets of citizens, organizations and the State; prevent cyber-attacks against critical infrastructures; and minimize damage and recovery times from cyber-attacks. Policies on National Cybersecurity Strategies or National Plans for the Protection of Information Infrastructures are those officially defined and endorsed by a nation state, and can include the following commitments: establishing clear responsibility for cybersecurity at all levels of government (local, regional and federal or national), with clearly defined roles and responsibilities; making a clear commitment to cybersecurity, which is public and transparent; encouraging private sector involvement and partnership in government-led initiatives to promote cybersecurity; a road-map for governance that identifies key stakeholders.

#### **C.3.2 Responsible agency**

A responsible agency for implementing a national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils or cross-disciplinary centers. Most national agencies will be directly responsible for watch and warning systems and incident response, and for the development of organizational structures needed for coordinating responses to cyber-attacks.

#### **C.3.3 Cybersecurity metrics**

This indicator measures the existence of any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development, risk assessment strategies, cybersecurity audits, and other tools and activities for rating or evaluating resulting performance for future improvements. For example, based on ISO/IEC 27002-2005, a national cybersecurity standard (NCSec) can foster a national response to cybersecurity requirements. This is split into five domains: NCSec Strategy and Policies; NCSec Organizational Structures; NCSec Implementation; National Coordination; Cybersecurity Awareness Activities.

## **C.4 Capacity building**

### **C.4.1 Public awareness campaigns**

Public awareness include efforts to promote widespread publicity campaigns to reach as many people as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centres, computer stores, community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behaviour online. This includes actions such as setting up portals and websites to promote awareness, disseminating support material and establishing cybersecurity adoption.

### **C.4.2 Cybersecurity standards and certification for professionals**

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of professionals by internationally recognized cybersecurity standards. These certifications, accreditations and standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC<sup>2</sup>), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), (No Suggestions) Certification, Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute, CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc.

### **C.4.3 Cybersecurity professional training courses**

This indicator measures the existence of short term national or sector-specific educational and professional training programmes for raising awareness with the general public (i.e. national cybersecurity awareness day, week, or month), promoting cybersecurity courses in the workforce (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector.

### **C.4.4 National education programmes and academic curriculums**

This indicator looks at the existence and the promotion of national education courses and programmes to train the younger generation in cybersecurity related skills and professions in schools, colleges, universities and other learning institutes. Cybersecurity related skills include but are not limited to setting strong passwords and not revealing personal information online. Cybersecurity related professions include but are not limited to cryptanalysts, digital forensics experts, incident responders, security architects and penetration testers and general master programmes in cybersecurity.

### **C.4.5 Cybersecurity research and development programmes**

This indicator measures the investment into national cybersecurity research and development programmes at institutions which could be private, public, academic, non-governmental or international. It also considers the presence of a nationally recognised institutional body overseeing the program. Cybersecurity research programmes include but are not limited to malware analysis, cryptography research and research into system vulnerabilities and security models and concepts. Cybersecurity development programmes refer to the development of hardware or software solutions that include but are not limited to firewalls, intrusion prevention systems, honey-pots and hardware security modules. The presence of an overarching national body will increase co-ordination among the various institutions and sharing of resources.

#### **C.4.6 Incentive mechanisms**

This indicator looks at any incentive efforts by government to encourage capacity building in the field of cybersecurity, whether through tax breaks, grants, funding, loans, disposal of facilities, and other economic and financial motivators, including dedicated and nationally recognized institutional body overseeing cybersecurity capacity building activities. Incentives increase the demand for cybersecurity related services and products which improves defences against cyber threats.

#### **C.4.7 Home grown cybersecurity industry**

A favourable economic, political and social environment supporting cybersecurity development will incentivize the growth of a private sector around cybersecurity. The existence of public awareness campaigns, manpower development, capacity building and government incentives will drive a market for cybersecurity products and services. The existence of a home grown cybersecurity industry is testament to such a favourable environment and will drive the growth of cybersecurity start-ups and associated cyber insurance markets.

### **C.5 Cooperation**

#### **C.5.1 Bilateral agreements**

Bilateral agreements (one to one agreements) refer to any officially recognized national or sector-specific partnerships for sharing cybersecurity information or assets across borders by the government with one other foreign government, regional entity or an international organization (i.e. the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether the agreement is legally binding or pending ratification. Information sharing refers to the sharing of threat intelligence while assets designate the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.

#### **C.5.2 Multilateral agreements**

Multilateral agreements (one to multi-party agreements) refers to any officially recognized national or sector-specific programmes for sharing cybersecurity information or assets across borders by the government with multiple foreign governments or international organizations (i.e. the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether the agreement is legally binding or pending ratification. Information sharing refers to the sharing of threat intelligence while assets designate the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.

#### **C.5.3 Participation of international fora/associations**

As part of enhancing collaboration in Cybersecurity, the commitment of governments to participate in Cybersecurity events is hereby measured. Such events include regional and international workshops, conferences and trainings. The World Summit on Information Society, Regional Cybersecurity forum, Regional cyberdrills, FIRST annual summit and technical colloquia, the Global Forum on Cyber Expertise (GFCE), the Internet Governance Forum as well as conferences by AfricaCERT, APCERT, OICCERT, GCC, and OAS are such examples.

#### **C.5.4 Public-private partnerships**

Public-private partnership (PPP) refers to ventures between the public and private sector. This performance indicator can be measured by the number of officially recognized national or sector-specific PPPs for sharing cybersecurity information (threat intelligence) and assets (people, processes, tools) between the public and private sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources), whether nationally or internationally.



### **C.5.5 Interagency/intra-agency partnerships**

This performance indicator refers to any official partnerships between the various government agencies within the nation state (does not refer to international partnerships). This can designate partnerships for information or asset sharing between ministries, departments, programmes and other public sector institutions.

### **C.5.6 Cybersecurity best practices**

This indicator measures the research and publication of best practices and guidelines on cybersecurity technology and its use, management, and application to various scenarios. Best practices are methods or procedures which have a proven track record of success. Adopting best practices will not only reduce the probability of failure but also increase efficiency. Best practices taken based on the achievements/progress and involvement of each country pertaining to all areas of the five pillars of the GCI.

## Annex D: Computational details

The 2018 Index employs, as in 2017, a weighting factor for each question. Unlike in 2017 though, it was decided this year that each pillar would carry the same weight (20% of the points). A group of experts was mandated to fix the weighting for each indicator and question. Each expert gave his/her own weighting and an average was calculated on that basis.

GCI 2018 uses a binary system in the evaluation of questions although for some of them the option "PARTIAL" was admitted (only for the drafts in final stage for the legal part and for the NCS). This was to encourage countries that are implementing laws and a national strategy.

For each question that was answered with "YES" the corresponding weighting was granted. For a "PARTIAL" answer, half of the assigned weighting was granted. The questions added together give the score for the indicator. The indicators added together give the score for the pillar, and the pillars added together give the final score.

Weighting for the pillars was set to 0.2 each. Weighting for the indicators was set by the group of experts:

NO.	Indicators	Weighting
1.	Legal Measures	0.2
1.1	Cybercriminal Legislation	0.079
1.2	Cybersecurity Regulation	0.079
1.3	Containment/curbing of spam legislation	0.042
2.	Technical Measures	0.2
2.1.	National, Government, Sectorial CERT/CIRT/CSIRT	0.065
2.2.	Cybersecurity Standards Implementation Framework for Organizations	0.035
2.3.	Standardization Body	0.030
2.4.	Technical mechanisms and capabilities deployed to address spam	0.024
2.5.	Use of cloud for cybersecurity purpose	0.019
2.6.	Child Online Protection mechanisms	0.027
3.	Organizational Measures	0.2
3.1.	Strategy	0.092
3.2.	Responsible Agency	0.063
3.3.	Cybersecurity Metrics	0.045
4.	Capacity Building	0.2
4.1.	Public Awareness Campaigns	0.036
4.2.	Cybersecurity Standards and Certification for Professionals	0.027
4.3.	Cybersecurity Professional Training Courses	0.032
4.4.	National Education Programs and Academic Curriculums	0.032
4.5.	Cybersecurity Research & Development Programs	0.026

NO.	Indicators	Weighting
4.6.	Incentive Mechanisms	0.024
4.7.	Home Grown Cybersecurity Industry	0.023
5.	Cooperation	0.2
5.1.	Bilateral Agreements	0.038
5.2.	Multilateral Agreements	0.038
5.3.	Participation of international fora/associations	0.036
5.4.	Public-private partnership	0.034
5.5.	Interagency/intra-agency partnerships	0.026
5.6.	Cybersecurity best practices	0.028
	Total	1

## Annex E: Index of cybersecurity indices 2018

The increase of recent incidents and breaches of cybersecurity demonstrates the challenge all users (governments, organizations and citizens alike) of the Internet face to keep up with the speed of ICT evolution. Cybersecurity must form an integral and indivisible part of this technological progress. Therefore, various factors must be taken into consideration, as the application of cybersecurity is a continuous process that needs to match ongoing cybercriminal activities and threat campaigns.

Since 2015, ITU compiles and publishes every year some of the outstanding cybersecurity indices. As cybersecurity issues continue to increase with time, new indices regarding cybersecurity challenges need to be established. This year, ITU has identified new indices and has accordingly updated the previous Index of Cybersecurity Indices of 2017.

The index of indices presented below is not an exhaustive list. It is a presentation of existing surveys, indices and publications from private and public organizations. These indexes can be broadly split into three major groups: indices for assessing national postures, indices for assessing organizations, and indices for assessing threats. These three groups are presented in section G2, G3, and G4.

### E.1 Definitions

#### Metrics

**Scores:** The score is based on an individual result using the total score of all indicators. This type of scale allows participants to have a view on their individual status regarding the different capabilities measured. The indices examined use different rating methods- percentages, ratios etc.

**Ranking:** Each participant is ranked compared to the others. The ranking scale allows participants to be aware of their level in relation to the other participants.

#### Content

**Information Society Development score:** Is a society where the creation, distribution, use, integration and manipulation of information is a significant economic, political, and cultural activity. The people who have the means to partake in this form of society are sometimes called digital citizens.

**Cyber maturity:** An assessment providing an in-depth review of an organization's ability to protect its information as well as its efforts and readiness against cyber threats.

**Cyber threats:** The potential of a malicious attempt to damage or disrupt a computer network or system with unauthorized access to a control system device using a data communications pathway. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.

**Cyber vulnerabilities:** Is a weakness which reduces a system's security assurance. Vulnerability is a system susceptibility or flaw that is accessible to an attacker or not otherwise mitigated by a countermeasure.

**Organizational:** The measurement of policy coordination institutions and strategies for cybersecurity development within countries and companies in order to secure the organization's smooth running and longevity while reducing cyber-attacks.

**Technical:** The measurement of technical institutions, terms, or frameworks dealing with cybersecurity. In this aspect, some indices check the commitment of countries/organizations on their available technical measures while others provide a technical guide on software to enhance security.

**Economical:** This notion represents the presence of an economic impact, cost or management measurement in the index while others present it as a business alignment and investment efficiency of an organization in accordance to cybersecurity.

**Legal framework:** The measurement of legal institutions and frameworks dealing with cybersecurity and cybercrime. It also involves rules, legal trainings, standardizations and regulations related to cybersecurity.

**Cooperation:** The existence of partnerships, cooperative frameworks and information sharing networks between countries and organizations.

**Capacity building:** The existence of research and development, good practices, education and training programmes; intended to enforce better understanding, approach and awareness towards cybersecurity.

**Recommendations and best practice:** A recommendation is a proposal or list of suggestions normally provided by competent bodies or authorities. An index may provide recommendations on what measures or steps ought to be taken to better the cybersecurity of the countries/organizations studied.

**Profiles:** The index presents a short description of the activities undertaken by the different organizations and countries examined.

### Presentation format

**Website:** The survey has an official Website where the majority of the information regarding the index can be found.

**PDF:** The survey proposes a Portable Document Format (PDF) with survey's detailed report and outputs.

**Visualization:** The representation of information through graphical references, images, scorecards, interactive images, heat maps, videos or others.

## E.2 Indices for assessing countries

Indices for assessing countries have been developed by international organizations and think tanks, often in partnership with private sector organizations. At the highest level, these indices look at, among others, policy and regulatory aspects, organizational measures, national strategies, and cooperative efforts. Some indices simply compare and contrast measures amongst countries, while others provide an index scoring based on indicators. Others provide rankings based on the scoring. All offer valuable information on cybersecurity practices and gaps at the nation state level.

### E.2.1 Cyber maturity in the Asia-Pacific Region<sup>1</sup> (Australian Strategic Policy Institute)

Number of countries:

25

Research Method:

Secondary data

Rank or Score:

Scores

Indicators:

11

Developer:

The Australian Strategic Policy Institute



<sup>1</sup> <https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017>

The **table** below gives a snapshot of the content and the methods used by the various indexes examined. This content is briefly detailed in the following pages. A short explanation of indicator meaning is presented at the end of this section.

	Metrics		Content											Presentation Format				
	Score	Ranking	Information Society Development Score (ISD) score)	Cyber Maturity	Cyber Threats	Cyber Vulnerabilities	Organizational	Technical	Economical	Legal Framework	Cooperation	Capacity Building	Recommendations/Best practices	Profiles	Website	PDF	Visualization	No. of Iterations
Cyber Maturity in the Asia-Pacific Region	x	x		x					x	x	x				x	x		4
National Cyber Security Index	x	x	x	x	x		x	x	x	x	x				x	x	x	2
Global Cybersecurity Index	x	x					x	x		x	x	x	x	x	x	x	x	3
Cyber Policy Portal							x	x	x	x	x	x		x	x		x	1
Global Cyber Strategies Index						x			x		x							1
CyberGreen Index	x	x			x			x							x		x	1
Kaspersky Cybersecurity Index	x				x				x					x	x	x	x	1
The Accenture Security Index	x	x			x		x	x	x	x			x		x	x	x	2
Global Threat Intelligence report					x								x					
Global Cybersecurity Assurance Report Cards	x				x			x							x		x	1
Cybersecurity Capability Maturity Model				x			x	x	x	x	x				x	x		2
Africa Cyber Security report	x				x		x			x	x					x		5
Cyber Power Index	x	x		x			x	x		x	x				x	x	x	1
IBM X-force Threat Intelligence Index					x			x							x			4
Index of Cybersecurity					x			x							x	x	x	74
Cybersecurity Index					x			x							x	x		1
Microsoft Security Intelligence Report	x				x								x		x	x		2

This index, developed by the Australian Strategic Policy Institute, is the fourth edition of an annual report providing information on levels of cyber maturity of Asia-Pacific region.

A total of 25 countries in the Asia-Pacific region have been analysed, with the United States of America used as a reference guide. This index is focused on government policies and legislative structures of cybersecurity. The methodology uses a cyber maturity metric to assess the various facets of nations' cyber capabilities. A set of 11 indicators has been produced and each state level of cyber maturity has been measured against the benchmark provided with each indicator. There was a change in the 2017 methodology where the measures and scores of Internet connectivity was calculated using International Telecommunication Union data for the percentage of the population that uses the Internet. This resulted in a more accurate measure of Internet usage.

The publication includes an overall ranking of cyber maturity for each state within the region, as well as an individual score and short profile. A colour reference base allows for quick assessment. The publication is classified as an index since it has indicators, scoring and ranking mechanisms. The colour-coded reference base is a neat addition. The individual country profiles are helpful and provide a snapshot of national activities. The focus is primarily on organizational structures, legislation, international cooperation, CERTs and military capabilities. However, it is only a regional index based on open source and publicly available information, and could benefit from a survey based data collection exercise.

### E.2.2 National Cyber Security Index<sup>2</sup> (Estonian e-Governance Academy)

Number of countries:

100

Research Method:

Primary & Secondary

Rank or Score:

Rank & Score

Indicators:

46

Developer:

Estonian e-Governance Academy  
& Estonian Foreign Ministry



The National Cyber Security Index 2018 (second edition) is still developed by the Estonian e-Governance Academy in cooperation with the Estonia Foreign Ministry. The index is focused on the public aspects of national cybersecurity, which are implemented by the central government. The aim of the index is to measure the preparedness of countries to prevent cyber threats and readiness to manage and control cyber incidents.

A total of 100 countries have been analysed with data collected using both primary and secondary research. The index has been modified into 3 categories, 12 capacities and 46 indicators. These indicators are measured in points (0 to 100). The indicators have been tied to cybersecurity and information society as e-identity, digital signature and the existence of a secure environment for e-services. The index has a score and ranking mechanism.

The advantage of this index is that it has an online global database and it shows what countries can do to improve their cybersecurity. It also gives an overview of the preparedness of countries to prevent

<sup>2</sup> [https://ega.ee/wp-content/uploads/2018/05/ncsi\\_digital\\_smaller.pdf](https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf)

cyberattacks and crimes as well as how to manage them. In addition, the Index also shows Digital Development Level (DDL) of each country which is calculated according to the ICT Development Index (IDI).

### E.2.3 Global Cybersecurity Index<sup>3</sup> (International Telecommunication Union)

Number of countries:

194

Research Method:

Primary and Secondary

Rank or Score:

Rank and score

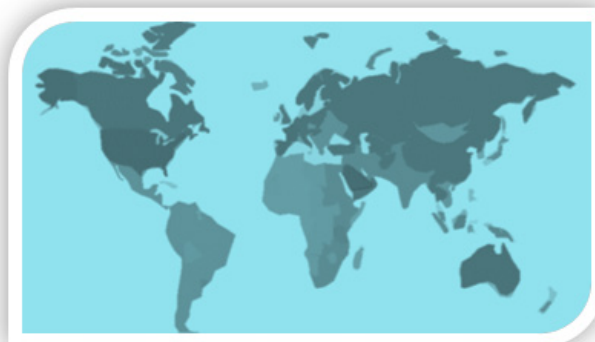
Indicators:

25

Developer:

International

Telecommunication Union



An index developed by the International Telecommunication Union (ITU) that aims at providing insight into the cybersecurity engagement of Member states. Rooted in the ITU's Global Cybersecurity Agenda (GCA), the third version- GCI 2018- still oversees the level of commitment in five areas: legal measures, technical measures, organizational measures, capacity building, and cooperation. The result is a country-level index profile and global ranking of cybersecurity commitment. A total of 194 countries have been analysed, 155 of which have been subjected to both primary and secondary research and only 39 a subject of secondary research. The publication includes an overall ranking, as well as six regional rankings and an individual score for each country.

The publication is classified as an index since it has indicators, scoring and a ranking mechanism. The main advantage of this publication is its global character (the only publication with such a broad geographical range). It is based on both a survey among ITU Member States and open sourced material. It is also worth noting the publication focuses on five broad cybersecurity application areas, which include 25 indicators and is further refined with additional sub-indicators.

In addition, the publication now has a platform presenting a more detailed structure of the survey with detailed country profiles. Countries can compare their value and status to another State or make regional comparisons.

<sup>3</sup> <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>



#### E.2.4 Cyber Policy Portal<sup>4</sup> (United Nations Institute for Disarmament Research)

Number of countries:

194

Research Method:

Publicly available data

Rank or Score:

Non

Indicators:

Unidentified

Developer:

The United Nations Institute for Disarmament Research (UNIDIR)



An online portal developed by the UNIDIR in 2018 as a reference tool that maps the cybersecurity and cybersecurity related policy landscape. The aim is to enhance informed participation in key policy processes by all relevant stakeholders, increasing opportunities for information sharing, capacity-building, and trust and cooperation in cyberspace.

The cyber policy portal is compiled from publicly available online open-source material that connects critical information in an interactive and systematized format hence providing a thorough, available and up-to-date analysis of the cyber capacity of the UN Member States and a selected group of intergovernmental organizations. It also provides a feedback mechanism to ensure the veracity of information and allow accurate and timely updates.

The advantage of the portal is that it traces information back to the official documentation disseminated by the State or intergovernmental organization in its original language.

#### E.2.5 Global Cyber Strategies Index<sup>5</sup> (Centre for Strategic International Studies (CSIS))

Number of countries:

196

Research Method:

Publicly available sources

Rank or Score:

Non

Indicators:

6

Developer:

The Centre for Strategic International Studies (CSIS)



An index produced by the Centre for Strategic International Studies (CSIS) under the technology programme. The aim is to provide policymakers and diplomatic officials a consolidated, database

<sup>4</sup> <https://cyberpolicyportal.org/en/>

<sup>5</sup> <https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index>

of global legal and policy frameworks to assist the global community grasp, track, and harmonize regulations internationally.

The index includes national strategies addressing civilian and military national cyber defense, digital content, data privacy, critical infrastructure protection, e-commerce, and cybercrime. The collection of the data is based on publicly available sources, and is updated as necessary.

The index traces back the data from its initial implementation and shows continuous updates that have been carried out. In addition, it highlights a global presentation of countries and territorial strategies.

### E.2.6 The CyberGreen Index<sup>6</sup> (CyberGreen Initiative)

Number of countries:

Research Method:  
Secondary

Rank or Score:  
Rank and Score

Indicators:  
6

Developer:  
CyberGreen initiative



An index developed in 2017 by CyberGreen Initiative supported by JPCertCC, CSA Singapore and the Foreign and Commonwealth Office. The CyberGreen Initiative is a global non-profit organization helping to improve the health of the global cyber ecosystem. The project aims to gather and present data on infections for vulnerable systems on the Internet.

CyberGreen Index is based on open source intelligence (secondary data) collection then put into the framework (CIF – collective intelligence framework) and stored in an elastic search database. The metrics are defined by the number of infected and vulnerable systems within the six risk indicators.

The publication includes ranking and scoring mechanisms presented at a global level that can be read as an incremental snapshot. The second version is being elaborated, which takes into account different limitations observed in the first version.

<sup>6</sup> <http://www.cybergreen.net/statistics/>

## E.2.7 Kaspersky Cybersecurity Index<sup>7</sup> (Kaspersky Lab in cooperation with B2B International)

Number of countries:

21

Research Method:

Primary

Rank or Score:

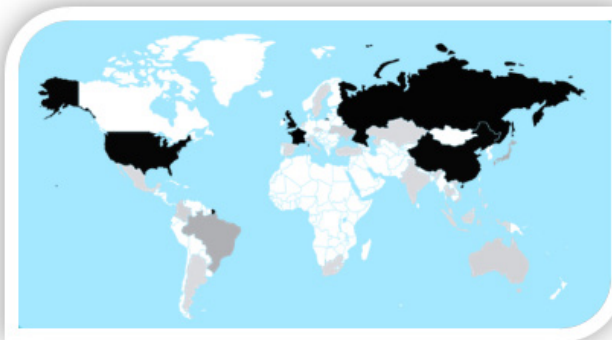
Score

Indicators:

3

Developer:

Kaspersky Lab & B2B  
International



An index developed by Kaspersky Lab in cooperation with B2B International. The focus is to evaluate, through a multi-dimensional concept, the level of risk Internet users are exposed to on a daily basis in cyber space. The Kaspersky Cybersecurity Index is a survey that occurs twice a year. Twenty-one countries across the globe have been analysed and a total of 17 377 respondents participated in the survey in the second half of 2017.

The sample includes thousands of adult Internet users around the world classified by age and gender. The index has three key indicators, namely: “Unconcerned” (the proportion of people not believing that they could be a target for cybercrime), “Unprotected” (the number of users who fail to protect themselves from cyber threats with the help of antivirus or Internet security software across all their desktops, laptops and mobile devices) and the “Affected” (the people who have experienced different cybersecurity incidents during the previous months). These indicators provide information needed to monitor the degree of risk to the average Internet user. The selected countries are scored by percentage in each of the categories.

To evaluate the online environment for Internet users, some additional statistics are presented in a variety of graphs such as user online behaviour, their concerns, what issues they face and how they defend themselves against possible threats.

<sup>7</sup> [https://www.kaspersky.no/about/press-releases/2016\\_21-29-60-kaspersky-lab-presents-the-first-cybersecurity-index](https://www.kaspersky.no/about/press-releases/2016_21-29-60-kaspersky-lab-presents-the-first-cybersecurity-index)

### E.3 Indices for assessing organizations

#### E.3.1 Accenture-The State of cyber resilience 2018<sup>8</sup> (Accenture)

Number of countries:

15

Research Method:

Primary

Rank or Score:

Score

Indicators:

33

Developer:

Accenture



Another index developed by Accenture, a leading global professional services company providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. The aim of the survey is to provide support to organizations and companies to build resilience using cybersecurity from the inside out, so they can confidently focus on innovation and growth. This year, it surveyed 4 600 executives from 19 industries and 15 countries across the Americas region, Europe, and the Asia-Pacific region.

The publication includes 33 cybersecurity capabilities classified into seven cybersecurity domains: business alignment, cyber response readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem. Each respondent is required to rate their performance level according to individual capabilities.

The advantage of this survey is that it highlights five steps that can support heads of businesses not only to close the gap on cyber intruders but also to revamp and install security into the systems of their organizations.

#### E.3.2 Global Threat Intelligence Report<sup>9</sup> (NTT Security)

The 2018 Global Threat Intelligence report is a publication produced by NTT Security featuring remarkable threats, incidents and trends detected during the previous year. The aim of the report is to enable organizations to adjust their strategic vision, improve their daily security practices, and help them with data points and citations in their business communications.

Attacks in 18 highly targeted industry sectors were analysed in the regions of Europe, Middle East and Africa (EMEA). A follow-up of each region by industry sector is explored and an audit of what they consider to be the enormous regional impacts in 2018.

#### E.3.3 Global Cybersecurity Assurance report cards<sup>10</sup> (Tenable Network Security in partnership with Cyber Edge Group)

A publication developed by Tenable Network Security in partnership with Cyber Edge Group. The Global Cybersecurity Assurance report cards measures the attitudes and perception of 700 IT security practitioners employed by an organization with more than 1 000 employees in 2017, including

<sup>8</sup> <https://www.accenture.com/us-en/insights/security/2018-state-of-cyber-resilience-index>

<sup>9</sup> [https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-gtir-summary-uea.pdf?sfvrsn=e8c7f625\\_4](https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-gtir-summary-uea.pdf?sfvrsn=e8c7f625_4)

<sup>10</sup> <https://www.tenable.com/lp/2017-global-cybersecurity-assurance-report-card/>

and comparing the findings of the 504 participants from the Risk Assessment Index of 2016. The 2017 sample comes from 19 industries across nine countries from three different regions. The Index consists of a 12-question web-based assigning the indices and grades by country and industry. A minimum of 25 responses was required to appear in the details of the report. Information contained in questionnaires with less than 25 responses was reported in the global and by countries data. This survey assesses how security professionals rate the ability to assess cybersecurity risks and threats and how they mitigate them in their enterprise.

“Security by The Numbers” is a collaborative online forum for simple, practical, real-world metrics, and enables its members to take part in discussion to help understand IT good practices compared to other peers.

The Security Measurement Index is based on ISO 27000 international standards and input from an advisory board of security professionals. It provides benchmarking tools for assessing organizations’ security practices, a global assessment of IT and a basis for developing security measurement best practices to help make cybersecurity more effective and efficient.

#### **E.3.4 Cybersecurity Capability Maturity Model<sup>11</sup> (University of Oxford Global Cyber Security Capacity Centre)**

A publication developed by the University of Oxford Global Cyber Security Capacity Centre. This report, now deployed in over 60 countries and revised in 2016, is a version of its 2014 prototype. The report is not intended to be a static exercise. Its aims are to increase the effectiveness of capacity-building regarding cybersecurity internationally, assist nations to improve their cybersecurity capacity and help promote an innovative and healthy cyberspace for all. The publication defines five capacity dimensions related to cybersecurity, namely: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training, and skills; legal and regulatory framework; and organizations, technologies, and standards. The publication identifies a set of 49 indicators depicting varying levels of cybersecurity capacity development. The publication is mainly focused on policy and organizational aspects of cybersecurity.

#### **E.3.5 Africa cybersecurity report-demystifying the Africa cybersecurity poverty line<sup>12</sup> (Africa Immersion Research Centre for Innovation and Training Facilities)**

A report developed by the Africa Immersion Research Centre for Innovation and Training Facilities. The publication aims to bring an understanding of the right level of cybersecurity required by an organization. The 2017 survey was carried out within 10 countries and 12 industry sectors in Africa with about 700 business respondents.

The survey focuses on eight key areas; top attack, cyber intelligence, survey analysis, home security, top trends, sector risk ranking, industry analysis and an anatomy of cyber heist, and using Africa maturity frame work. They also indicate five levels of cyber maturity: ignorant, informed, engaged, intelligent and excellent.

The publication provides a broad understanding of African businesses that are operating below the ‘cybersecurity poverty line’ with most companies falling in the low level of cybersecurity category. It also focuses on building capacity and creating awareness to organizations to help implement good cybersecurity measures.

<sup>11</sup> <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition>

<sup>12</sup> <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>

## E.4 Indices for assessing other aspects

### E.4.1 IBM X-Force Threat Intelligence Index 2018<sup>13</sup> (IBM security services)

The threat intelligence index is developed by IBM security services. The publication includes an overview and comparison of cybersecurity threats in 2016 and 2017 based on cyberattack event data gathered by the company. X-Force uses both data from monitored security clients and data derived from non-customer assets such as spam sensors and honeynets. The publication provides a broad overview of technical challenges, case studies, and best cybersecurity practices in five main industries namely: Financial services, health care, manufacturing, retail, and information and communication.

The index does not score organizations or countries, nor does it include any specific indicators or formula for the calculation of an index but gives ranking of industries that were most attacked in 2017. It also provides the overall number of the most dangerous attacks and incidents in the given year, as well as distribution by industry, category of incidents and category of attacks. The publication is updated periodically.

### E.4.2 Index of Cybersecurity<sup>14</sup> (Dan Geer and Mukul Pareek)

This is an individual effort developed by Dan Geer and Mukul Pareek and is focused on the technical aspects of cybersecurity. Published monthly since April 2011, the aggregate index value is updated on the public website. However, detailed statistics and individual sub-indices are shared only with respondents in a separate report.

It is an opinion-based measure of perceived risk to information infrastructures from a wide range of cybersecurity threats. It assesses, communicates the perceived level of risk of security practitioners and provides some key best practices for practitioners to compare. The survey gathers the views of information security professionals on the most current and most interesting threats.

A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite. The report is based on six key dimensions including 25 questions on a scale of five multiple choice answers from “falling fast” to “rising fast”.

### E.4.3 Cybersecurity Index<sup>15</sup> (Dell SecureWorks)

An index developed by Dell SecureWorks. The aim of the publication is to notify customers about threats and malicious activities, which may require the implementation of protective measures. The index uses a four-level scoring system of overall network cybersecurity status, which in a simple and readable manner informs customers about the current level of overall cybersecurity threat. The index is evaluated daily by Counter Threat Unit researchers and updated when necessary. The index is not numerical but simply color-coded based on the following four cybersecurity levels: Guarded, Elevated, High and Critical. The threats are determined by a panel of experts at the Dell SecureWorks Counter Threat Unit Research Team and are based on information such as the release of security updates by companies such as Microsoft and Adobe. The publication is focused on technical aspects of cybersecurity.

### E.4.4 Microsoft Security Intelligence Report<sup>16</sup> (Microsoft)

A publication produced on a bi-annual basis by Microsoft, a trusted security advisor and partner to large global organizations. The aim of the report is to educate organizations about the current state of threats, recommended best practices, and solutions for cyber threats.

<sup>13</sup> <https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-research-report-77014377usen-20180329.pdf>

<sup>14</sup> <http://cybersecurityindex.org/>

<sup>15</sup> <https://www.secureworks.com/about/counter-threat-unit>

<sup>16</sup> [https://info.microsoft.com/rs/157-gqe-382/images/en-us\\_cntnt-ebook-sir-volume-23\\_march2018.pdf](https://info.microsoft.com/rs/157-gqe-382/images/en-us_cntnt-ebook-sir-volume-23_march2018.pdf)

The analysed data is collected from a wide range of Microsoft products and services that the users willingly provide hence delivering a comprehensive and detailed perspective on the threat landscape in the software industry.

In 2017, Microsoft analysed the threat intelligence gathered from its worldwide clients in more than 100 countries and millions of computers and analysed three studies: Botnets continuing to affects millions of computers globally, hackers going for the easy mark and Ransomware a force that still needs to be evaluated.

The publication is focused on technical aspects of cybersecurity.

**International  
Telecommunication  
Union**

Place des Nations  
CH-1211 Geneva 20  
Switzerland  
[www.itu.int](http://www.itu.int)

ISBN: 978-92-61-28201-1



9 789261 282011

Published in Switzerland  
Geneva, 2018

Photo credits: Shutterstock