

Global Cybersecurity Index 2017 AFRICA

Report



Table of Contents

- 1 Executive Summary 3**
- 2 Introduction 4**
- 3. GCI Scope and Framework..... 6**
- 4. Key Findings 11**
 - 4.1 Heat Map of National Cybersecurity Commitments 12**
 - 4.2 GCI Groups..... 13**
 - 4.3 GCI Africa region commitment in figures 14**
- 5. Global Outlook 15**
 - 5.1 Comparing GCI with ICT Development Index 15**
- 6. Regional Outlook..... 18**
- 7. Illustrative practices by pillar 20**
 - 7.1 Legal 21**
 - 7.2 Technical 24**
 - 7.3 Organizational 27**
 - 7.4 Capacity building 31**
 - 7.5 Cooperation..... 35**
- 8. Conclusion..... 38**
- Annex 1: Abbreviations..... 39**
- Annex 2: ITU African Member states global cybersecurity commitment score..... 40**
- Annex 3: Tables and figures 41**

1 Executive Summary

The regional report 2017 is an analysis of the results of the Global Cybersecurity Index (GCI), a survey that measures the commitment of Member States to cybersecurity.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment.

The GCI was developed through the data collected as a result of survey and consultations with a group of experts in order to analyze the problems and overview the developments of the cybersecurity phenomenon in six regions – Americas, Arab, Africa, Asia-Pacific, CIS and Europe.

The Index provides information regarding the level of development of the different pillars varying from country to country and highlights the challenges Member States experience in the matter of cybersecurity.

A detailed review of the previous GCI surveys is provided to present an accurate picture of the cybersecurity situation in Africa. This includes: a regional outlook and specific characteristics, which distinguish the region and give an insight of the achievements of the pillars employed in the GCI.

The report concludes that cybersecurity has become a matter of urgency and it is essential to collaborate in order to prevent and counter cybercrimes.

2 Introduction

The information and communication technologies' (ICT) networks, devices and services are increasingly critical for day-to-day life. In 2016, almost half of the world's population used the Internet (3.5 billion users¹) and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020². Yet, just as in the real world, the digital space is exposed to a variety of cybersecurity threats that can cause immense damage.

Cybersecurity threats remain at the forefront of the public consciousness, whether it's ransomware attacks, cyber-enabled fraud or State-on-State actions. The ransomware industry continues to affect member states, businesses and consumers, by regularly destabilizing access to the data until a ransom payment is made to cybercriminals. To prevent such misuse of ICT resources, governments, the private sector and civil society need to cooperate and put into effect a cybersecurity system to reduce threats, enhance confidence in the use of electronic devices and services and build mitigation strategies.

Over the past decade, great leaps have been made in the promulgation of international and regional tools aimed at countering cybercrime. Countries increasingly recognize the need for legislation in this area and some conventions related to cybercrime have been adopted. However, there are large regional differences, with some countries reporting insufficient legislation in this regard.

In the African region the issue of the poor state of Internet connectivity and ICT development has emerged due to the economic and demographic transformations and involvement of youth in computer-related crimes. Technologies diffuse rapidly and projects to connect African countries are required to link them with the global communication system and facilitate telecommunication/ICT capabilities in Africa.

Disintegration at the international level and low Internet connectivity in Africa may be caused by the durable armed conflicts in the past and the lack of capacity building in the region.

The geographical majority of the Internet population is concentrated in the north and the south of the continent, associated with the level of economic development in the sub-regions.

Nonetheless, there is still a visible gap between countries in terms of knowledge, awareness and capacity to deploy the strategies, capabilities and programmes in the field of cybersecurity. Sustainable developments in this area should ensure the safe and adequate use of ICTs as well as economic growth. Cybersecurity is no longer only a government concern. Today, the industries, the governments and the citizens need to respond, protect and design strategies toward raising awareness and capacity building.

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

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

The ITU oversees the development of the knowledge, awareness and capacity in member countries. This report specifically relates to the Africa Region. This region comprises of 44 Member States; Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Cote d'Ivoire, Congo, Democratic Republic of the Congo, Ethiopia, Eritrea, Equatorial Guinea, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, South Africa, South Sudan, Swaziland, Tanzania, Togo, Uganda, Zambia, and Zimbabwe.

In this context, under Resolution 130 (Rev. Busan, 2014) the ITU together with Member States have established the Global Cybersecurity Index (GCI) to promote government strategies and the sharing of information on efforts across industries and sectors. This report aims to implement AFR5 from the WDTC and build further confidence and security in the use of Telecommunications/ICTs. This comes under Sustainable Development Goal 7, to ensure access to affordable, reliable, sustainable and modern energy for all.

The methodology used is explained in more detail in the main Global Cybersecurity Index which can be found on the website of the ITU but in sum the GCI is a composite index which combines 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the GCA. The methodology for the GCI tasked the ITU and the expert group with developing a questionnaire for the purpose of information gathering, collecting and analysing data with the key objective of building capacity at the national, regional and international level. An analysis of the data collected is set out in the Report below³.

³ <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx>

3. GCI Scope and Framework

3.1 Background

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

A first iteration of the GCI was conducted in 2013–2014 in partnership with ABI Research¹, and the final results have been published².

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

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

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

3.2 Reference model

The GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the GCA. These pillars form the five pillars of GCI.

The main objectives of the GCI are to measure:

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

- the cybersecurity commitment divide, i.e. the difference between countries in terms of their level of engagement in cybersecurity programmes and initiatives.

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

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

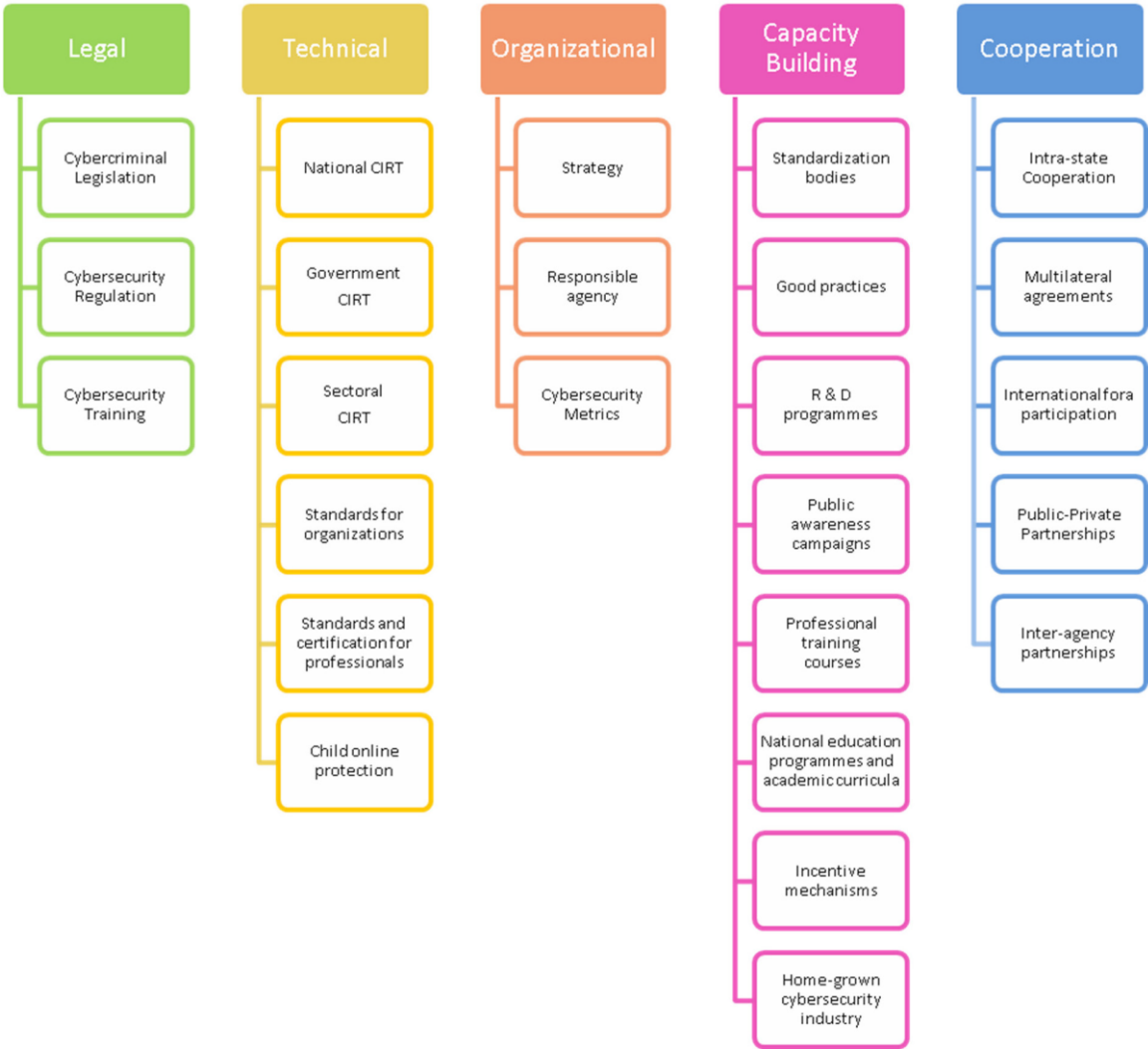
3.3 Conceptual framework

The five pillars of the GCI are briefly explained below:

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

Each pillar was then further divided in sub-pillars (Figure 3.3.1).

Figure 3.3.1: GCI pillars and sub-pillars



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

Figure 3.3.2 below represents all the five pillars from GCA with their indicators.

Figure 3.3.2: GCA tree structure illustrating all pillars (simplified)

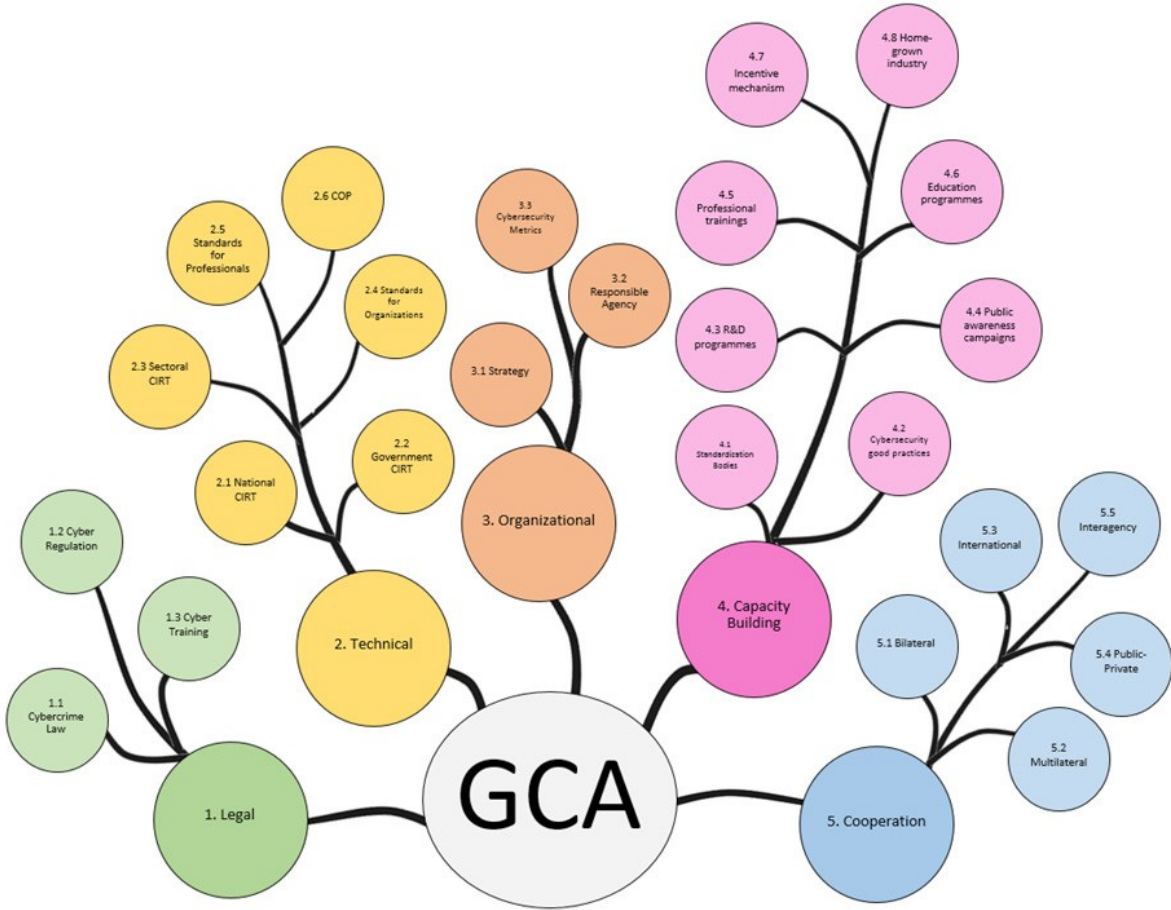
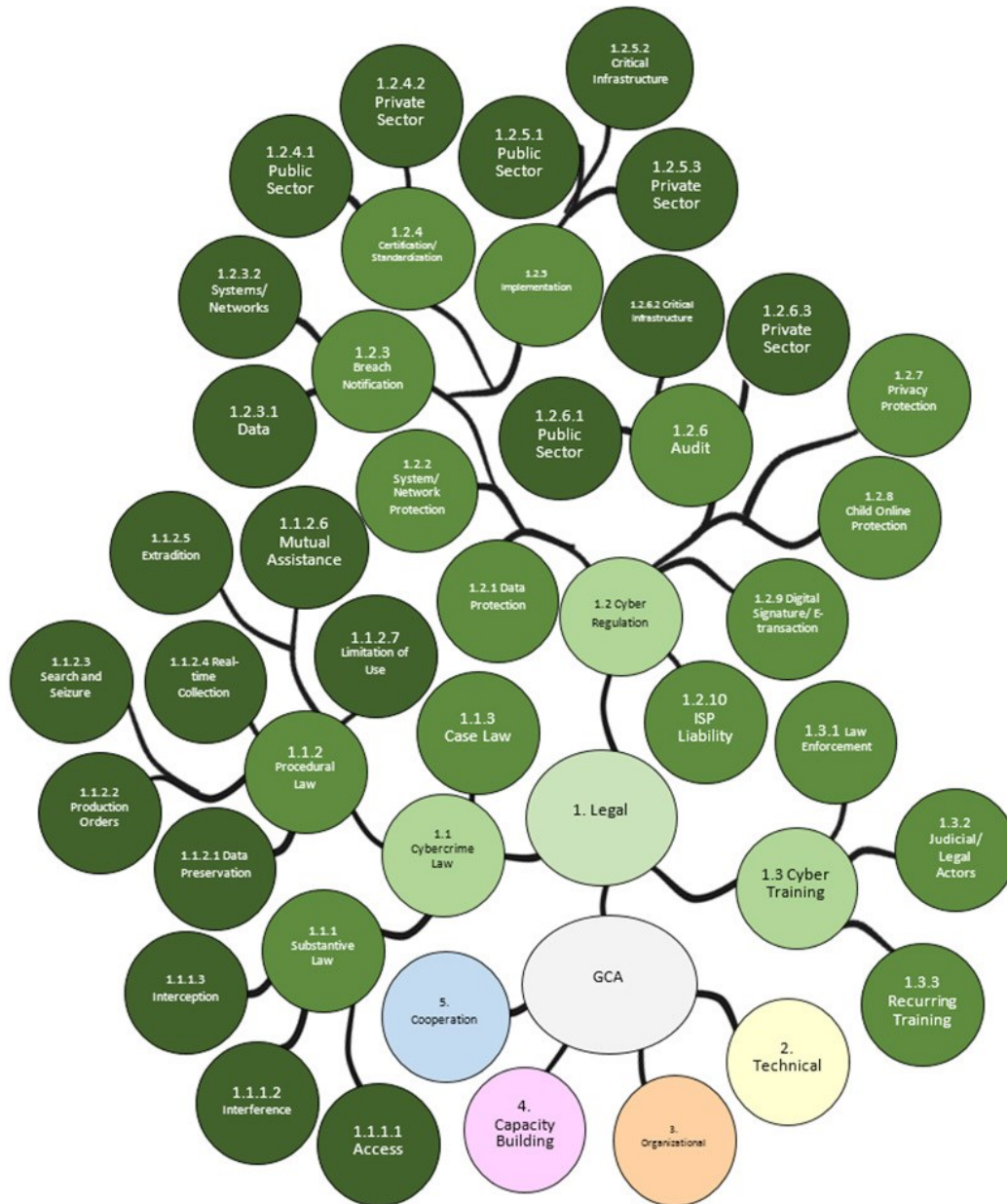


Figure 3.3.3 below illustrates the relationship between the GCA, the pillars, sub-pillars and questions (expanded only for the legal pillar due to space considerations).

Figure 3.3.3: GCI tree structure illustrating Legal pillar

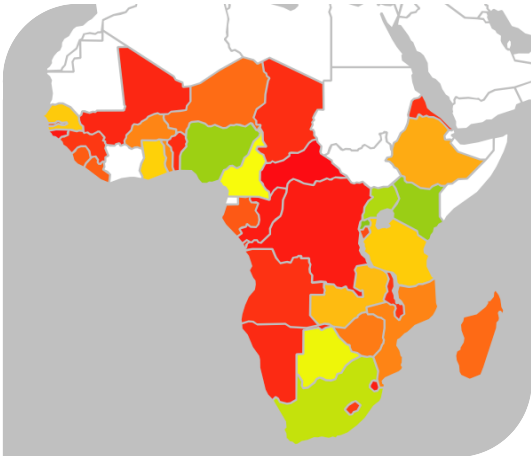


4. Key Findings

This section presents the key findings of the GCI 2017 for the Africa region, which were drawn from the results of the GCI survey conducted in 2016 and presented in 2017 under five pillars of the GCA agenda; Legal, Technical, Organizational, Capacity building and Cooperation measures. These findings indicate how active and committed the Africa region is in cybersecurity and also present some of the new improvements illustrated in each country.

4.1 Heat Map of National Cybersecurity Commitments

Out of the 44 Member States in Africa, a quite low general level of cybersecurity commitment can be observed, as the heat map below illustrates.



Level of commitment: from Green (highest) to Red (lowest) **Figure 4.1.1: GCI Heat Map**

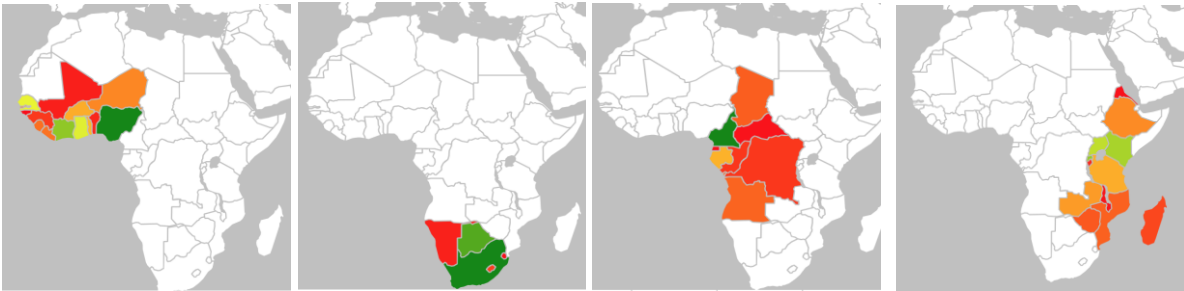


Figure 4.1.2: GCI Heat Map by sub-region

Disintegration at the international level and low commitment in Africa may be caused by conflicts in the past and the lack of capacity building in the region.

4.2 GCI Groups

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

- *Leading stage* refers to the 6 countries (i.e., GCI score in the 50th percentile and higher) that demonstrate high commitment.
- *Maturing stage* refers to the 11 countries (i.e., GCI score between the 20th and 49th percentile) that have developed complex commitments, and engage in cybersecurity programmes and initiatives.
- *Initiating stage* refers to the 27 countries (i.e., GCI score less than the 20th percentile) that have started to make commitments in cybersecurity.

Table 4.2.1: GCI African Tiers

Leading stage			
Mauritius	0.830	Nigeria	0.569
Rwanda	0.602	Uganda	0.536
Kenya	0.574	South Africa	0.502
Maturing stage			
Botswana	0.430	Zambia	0.292
Cote d'Ivoire	0.416	Ethiopia	0.267
Cameroon	0.413	Togo	0.218
Ghana	0.326	Burkina Faso	0.208
Tanzania	0.317	Mozambique	0.206
Senegal	0.314		
Initiating stage			
Zimbabwe	0.192	Chad	0.072
Seychelles	0.184	Benin	0.069
Niger	0.170	South Sudan	0.067
Madagascar	0.168	Namibia	0.066
Liberia	0.149	Mali	0.060
Sierra Leone	0.145	Cape Verde	0.058
Gabon	0.139	Swaziland	0.041
Gambia	0.136	Sao Tome and Principe	0.040
Burundi	0.120	Democratic Republic of the Congo	0.040
Lesotho	0.094	Congo	0.040
Guinea	0.090	Guinea-Bissau	0.034
Malawi	0.084	Central African Republic	0.007
Angola	0.078	Equatorial Guinea	0.000

4.3 GCI Africa region commitment in figures

Below is a table showing how many countries in Africa have a specified cybersecurity indicator out of the 44 countries in the region. This analysis consists of 29 countries that responded to the survey and the 15 that didn't respond and their data was collected through primary research.

<i>Sub-pillars</i>	NO. Of Member States in Africa who has the sub-pillars
<i>Cybercriminal Legislation</i>	31
<i>Cybersecurity Regulation</i>	37
<i>Cybersecurity Training</i>	11
<i>National CIRT</i>	12
<i>Government CIRT</i>	12
<i>Sectoral CIRT</i>	6
<i>Standards implementation framework for organizations</i>	8
<i>Standards and certification for professionals</i>	7
<i>Strategy</i>	12
<i>Responsible agency</i>	20
<i>Cybersecurity Metrics</i>	4
<i>Standardization bodies</i>	18
<i>Good practices</i>	10
<i>R & D programmes</i>	11
<i>Public awareness campaigns</i>	15
<i>Professional training courses</i>	13
<i>National education programmes and academic curricula</i>	11
<i>Incentive mechanisms</i>	9
<i>Home-grown cybersecurity industry</i>	4
<i>Intra-state Cooperation</i>	8
<i>Multilateral agreements</i>	10
<i>International fora participation</i>	40
<i>Public-Private Partnerships</i>	7
<i>Inter-agency partnerships</i>	7

Table 4.3.1: commitment of Africa region in figures

5. Global Outlook

All of the six ITU regions are represented in the top ten commitment level in the GCI. One of them is from Africa. This suggests that being highly committed is not strictly tied to geographic location.

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

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

5.1 Comparing GCI with ICT Development Index

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

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

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

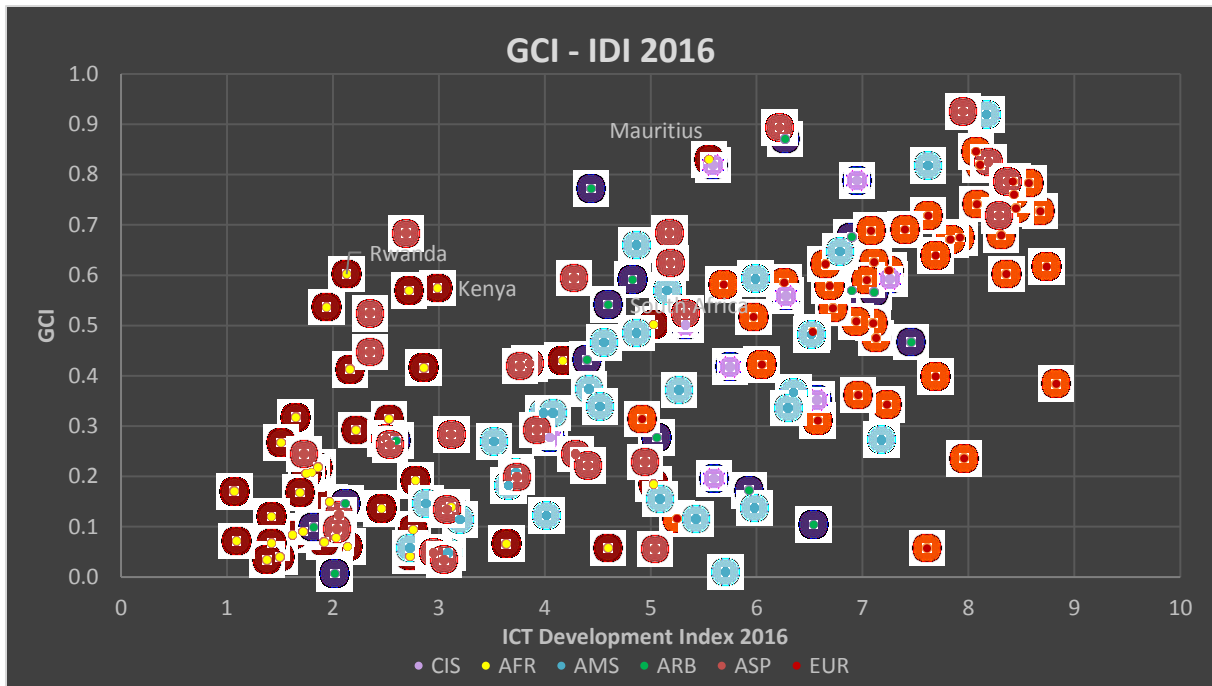


Figure 5.1.1: Global comparison GCI and IDI

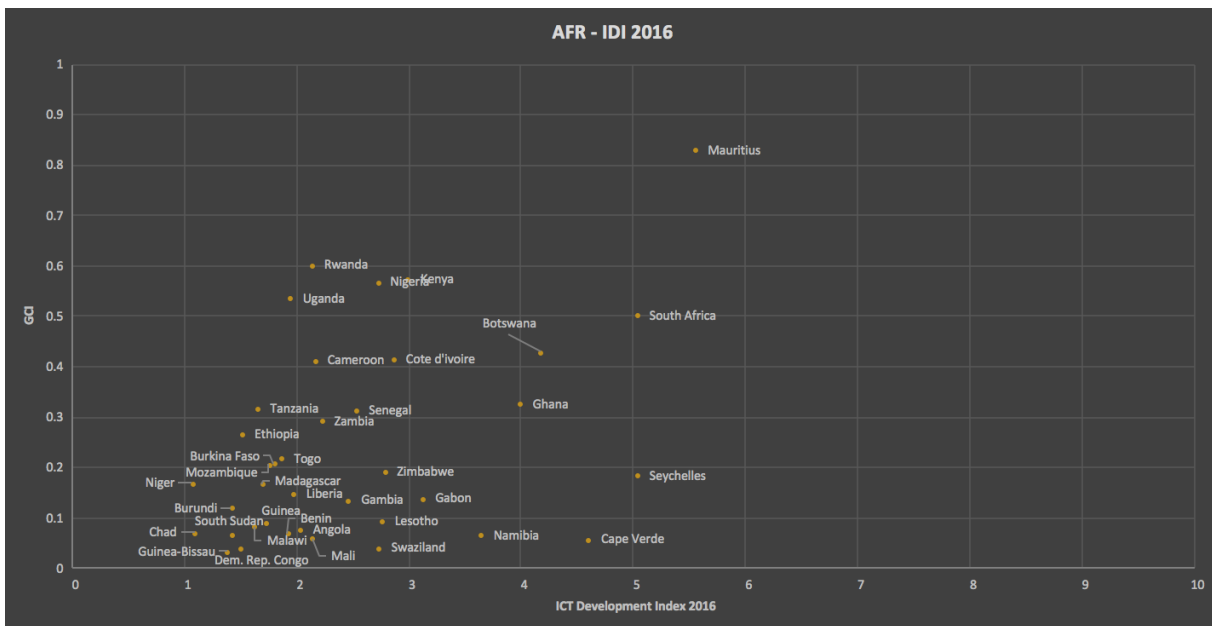


Figure 5.1.2: Comparison GCI and IDI in the Africa region

The geographical majority of the Internet population is concentrated in the north and the south of the Africa continent that is associated with the level of economic development in the sub-regions.

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

Figure 5.1.3: Africa region scorecard

6. Regional Outlook

During the active data collection phase of the GCI 2017 exercise 29 out of 44 Member States in the Africa region responded to the survey.

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

Region	Legal	Technical	Organizational	Capacity Building	Cooperation
AFR	0.29	0.18	0.16	0.17	0.25
AMS	0.40	0.30	0.24	0.28	0.26
ARB	0.44	0.33	0.27	0.34	0.29
ASP	0.43	0.38	0.31	0.34	0.39
CIS	0.58	0.42	0.37	0.38	0.40
EUR	0.62	0.61	0.45	0.50	0.47

Figure 6.1: Average GCI score for each region

As the GCI shows, there is a wide gulf in cyber preparedness around the globe. This gap exists between and within regions. Cybersecurity related commitments are often unequally distributed with countries performing well in some pillars and less so in others. Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective.

In the Africa region, the average for each pillar stays lower than in other regions, especially in the technical, organisational and capacity building fields. Almost half the countries do not meet the elements proposed by the defined categories. However, the legal aspect plays the key role in cybersecurity protection. This statistic indicates the major reasons behind the lack of developments in the cybersecurity area which are the geographical features, socio-economic and cultural aspects. The following sub-sections show the findings for Africa, highlighting the top-scoring countries in that region.

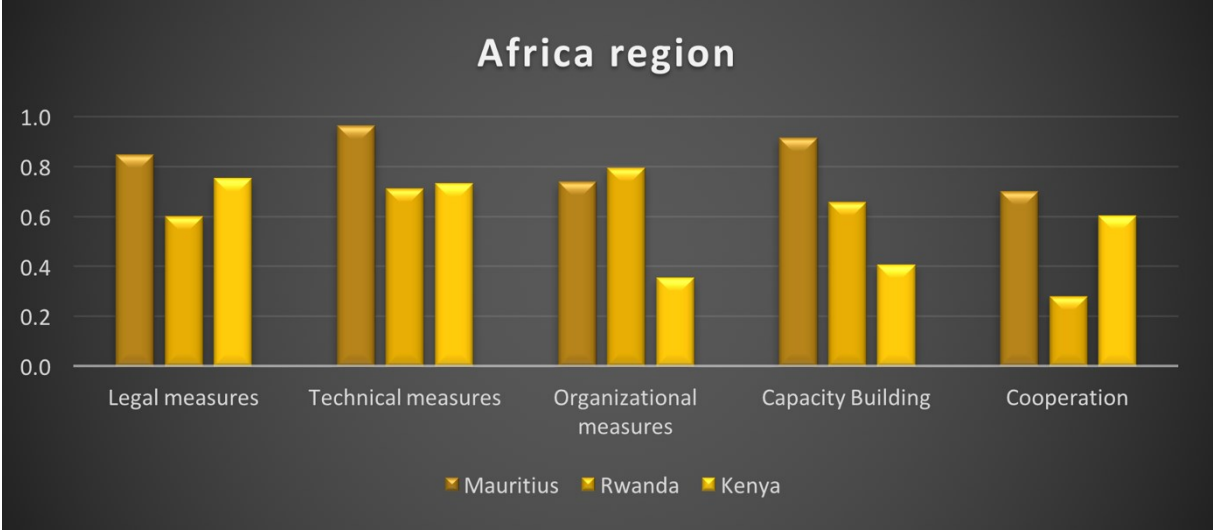





Figure 6.2: Average of Top three ranked countries in Africa

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

Table 6.2: top three Member States in the African region

 **Mauritius** is the top ranked country in the Africa region. It scores particularly high in the legal and the technical areas. The Botnet Tracking and Detection project allows Computer Emergency Response Team of Mauritius (CERT-MU) to proactively take measures to curtail threats on different networks within the country. Capacity building is another area where Mauritius does well. The government IT Security Unit has conducted 180 awareness sessions for some 2000 civil servants in 32 government ministries and departments.

 **Rwanda**, ranked second in Africa, scores high in the organizational pillar and has a standalone cybersecurity policy addressing both the public and private sector⁴. It is also committed to develop a stronger cybersecurity industry to ensure a resilient cyber space.

 **Kenya**, ranked third in the region, provides a good example of cooperation through its National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC)⁵. The CIRT coordinates at national, regional and global levels with a range of actors. Nationally this includes ISPs and the financial and educational sectors; regionally it works with other CIRTs through the East African Communications Organization; and internationally it liaises with ITU, FIRST, and bi-laterally with the United States and Japan CIRTs among others.

⁴ http://www.myict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf

⁵ <http://www.ke-cirt.go.ke/index.php/members/>

7. Illustrative practices by pillar

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

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

<i>Sub-pillars</i>	NO. Of Member States who has the item	Maximum score	Regional score (Member States who answered)	% of item fulfil
<i>Cybercriminal Legislation</i>	31	7.82	4.35	55.56
<i>Cybersecurity Regulation</i>	37	6.84	2.60	37.99
<i>Cybersecurity Training</i>	11	6.28	3.51	55.95
<i>National CIRT</i>	12	4.65	3.08	66.27
<i>Government CIRT</i>	12	3.03	3.03	100.00
<i>Sectoral CIRT</i>	6	2.71	2.03	75.00
<i>Standards implementation framework for organizations</i>	8	3.12	2.95	94.55
<i>Standards and certification for professionals</i>	7	2.71	2.35	86.72
<i>Strategy</i>	12	7.47	2.47	33.10
<i>Responsible agency</i>	20	6.57	4.76	72.50
<i>Cybersecurity Metrics</i>	4	5.63	3.43	60.89
<i>Standardization bodies</i>	18	1.40	1.05	74.84
<i>Good practices</i>	10	3.03	3.03	100.00
<i>R & D programmes</i>	11	2.77	1.49	53.69
<i>Public awareness campaigns</i>	15	2.43	1.44	59.31
<i>Professional training courses</i>	13	2.51	1.95	77.81
<i>National education programmes and academic curricula</i>	11	2.67	1.13	42.46
<i>Incentive mechanisms</i>	9	2.20	1.71	77.78
<i>Home-grown cybersecurity industry</i>	4	1.92	0.76	39.79
<i>Intra-state Cooperation</i>	8	4.14	1.95	47.13
<i>Multilateral agreements</i>	10	5.04	3.30	65.52
<i>International fora participation</i>	40	3.37	3.37	100.00
<i>Public-Private Partnerships</i>	7	4.82	3.51	72.73
<i>Inter-agency partnerships</i>	7	3.97	3.97	100.00

Table 7.1: Average and global percentage of all the five GCI pillars (25 indicators) of the Africa region

7.1 Legal

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

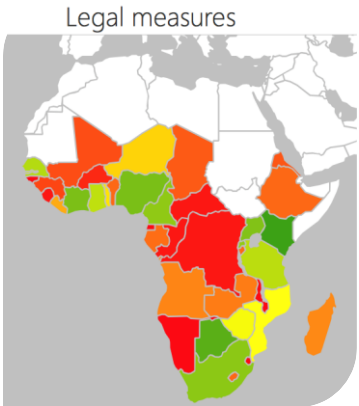


Figure 7.1.1: GCI Heat Map showing level of legal commitment in Africa region

<i>Sub-pillars</i>	NO. of Member States that responded YES at the specified element in the sub-section	Maximum score	Regional average for Member States having said YES	Global % of the specified element
<i>Cybercriminal Legislation</i>	31	7.82	4.35	55.56
<i>Cybersecurity Regulation</i>	37	6.84	2.60	37.99
<i>Cybersecurity Training</i>	11	6.28	3.51	55.95


Table 7.1.1: Global average in legal sub-pillars

In the area of training, efforts need to be enhanced particularly for the professionals who are handling cybersecurity crimes. In Africa, only a quarter of the Member States have programs for law enforcement or the judicial system (table 6.1.1) and only 11 countries f have regular trainings both for judicial and legal actors and for law enforcement such as police officers and enforcement agents. The remaining 9 countries have professional trainings in one of these two fields only or do not provide the trainings regularly.




Figure 7.1.2: Cybersecurity training commitments


7.1.1 Cybercrime legislation

 **Tanzania** has recently finalized a complete and robust legislation in order to repress and protect against cybercrime. The Cybercrime Act from 2015 and the Electronic Transaction act are covering many sector of cybercrime related to substantive and procedural laws.

7.1.2 Cybersecurity regulation

 **Uganda** has established a legislation in 2015 in cybersecurity related to the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. Also, the legislation imposes Audits to critical national Information Infrastructure by the office of National Security Adviser⁶.

7.1.3 Cybersecurity training

 **Mauritius** makes available training for law enforcement and judiciary which has been conducted under the GLACY Project since 2013 and is still ongoing. CERT-MU also carried out cybersecurity trainings on digital forensic investigator professional and network forensic (packet analysis) for law enforcement officers. Training on information security standards and best practices is given to the technical officers of the IT Security Unit (ITSU) of the Ministry of Technology, Communication and Innovation⁷.

⁶ https://cert.gov.ng/images/uploads/CyberCrime_%28Prohibition,Prevention,etc%29_Act,_2015.pdf

⁷ http://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/glacy-support-to-mauritius-judicial-training-courses-on-cybercrime-delivered

Mauritius	0.848	Ghana	0.523	Gabon	0.176	Burkina Faso	0.062
Kenya	0.753	Seychelles	0.508	Ethiopia	0.168	Sierra Leone	0.031
Botswana	0.701	Gambia	0.488	Burundi	0.168	Sao Tome and Principe	0.031
Nigeria	0.643	Zimbabwe	0.424	Benin	0.168	Democratic Republic of the Congo	0.031
Cote d'Ivoire	0.640	Mozambique	0.408	Lesotho	0.167	Congo	0.031
Uganda	0.629	Togo	0.364	Chad	0.143	Central African Republic	0.031
South Africa	0.610	Niger	0.336	Eritrea	0.137	Swaziland	0
Cameroon	0.605	Liberia	0.274	Mali	0.125	Guinea-Bissau	0
Rwanda	0.600	Madagascar	0.219	South Sudan	0.121	Namibia	0
Senegal	0.540	Angola	0.212	Cape Verde	0.117	Equatorial Guinea	0
Tanzania	0.531	Zambia	0.199	Guinea	0.110	Malawi	0

Table 6.1.2: Global average in legal pillar by countries in the Africa region

7.2 Technical

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

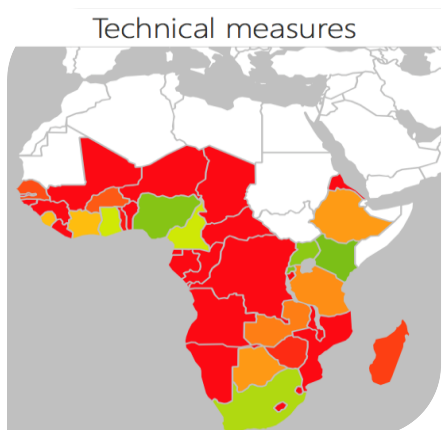


Figure 7.2.1: GCI Heat Map showing level of technical commitment in the Africa region


<i>Sub-pillars</i>	Number of countries that responded YES at the specified element in the sub-section	Maximum score	Regional average for countries having said YES	Global % of the specified element
<i>National CIRT</i>	12	4.65	3.08	66.27
<i>Government CIRT</i>	12	3.03	3.03	100.00
<i>Sectoral CIRT</i>	6	2.71	2.03	75.00
<i>Standards implementation framework for organizations</i>	8	3.12	2.95	94.55
<i>Standards and certification for professionals</i>	7	2.71	2.35	86.72

Table 7.2.1: Global average in technical sub-pillars


In this pillar, many African countries encounters difficulties, especially with the establishment of sectoral CIRT and in the implementation of professional standards and certifications. In effect, only 7 countries have framework for professionals and only 6 countries have sectoral CIRT or equivalent structures.

Cybersecurity certification is an important component in today's world where hacking has becomes more and more dangerous and inevitable. It is a way of protecting IoT's, networks and data. Special criteria given by a certification body enhance the protection of products and services against cyber threats. Standards, however, are needed more to establish a common language through different cultures and countries. A standard is a file recognized by a normalization body that provides a consensus on a service or a product that details also its quality and security.


National CERT/CIRT/CSIRT

 **Ghana** benefits from its computer emergency response team (CERT.GH) sponsored by the Ministry of Communication, the National Communication Authority and the National IT Agency. CERT.GH helps implementing proactive measures to reduce the risks of cybersecurity incidents in different sectors such as Governmental authorities, law enforcement, ISPs, financial institutions, private enterprises and companies etc. CERT.GH is affiliated with FIRST and other CERTs⁸.


7.2.1 Government CERT/CIRT/CSIRT

 **Cameroon** established a National Agency for Information and Communication Technologies (ANTIC). ANTIC is a Public Administrative Establishment with legal personality and is financially autonomous. Their missions are for instance to promote ICT, and to regulate activities in cybersecurity and certification such as audits. This institution has two main objectives. The first is to facilitate and accelerate the development of ICTs and to harmonize its exploitation and the second is to contribute to the development of Cameroon through the safe use of ICTs⁹.

7.2.2 Sectoral CERT/CIRT/CSIRT

 **Sierra Leone's** Act of Parliament to regulate the telecoms sector, protect consumers and ensure fair competition among providers established "The National Telecommunications Commissions" (NATCOM) in 2006¹⁰.

7.2.3 Cybersecurity standards implementation framework for organizations

 **Botswana** Bureau of Standards (BOBS) offers technical services in the standardization sector and coordinates and improves the quality of life of the population, in both the private and the public sectors. It is the official body responsible for providing standards at a national level and adopting the international standards for its nation BOBS is a member of the "International Organization for Standardization" (ISO).

⁸ <https://www.cert-gh.org>

⁹ <https://www.antic.cm/index.php/en/agence-3/presentation-2>

¹⁰ <http://natcom.gov.sl/index.php/operations>

Mauritius	0.964	Botswana	0.278	Guinea	0	Mali	0
Kenya	0.731	Tajikistan	0.257	Swaziland	0	South Sudan	0
Rwanda	0.712	Zambia	0.228	Gabon	0	Cape Verde	0
Nigeria	0.708	Burkina Faso	0.164	Gambia	0	Sao Tome and Principe	0
Uganda	0.690	Seychelles	0.158	Niger	0	Democratic Republic of the Congo	0
South Africa	0.622	Senegal	0.142	Liberia	0	Congo	0
Cameroon	0.560	Madagascar	0.115	Angola	0	Central African Republic	0
Ghana	0.558	Zimbabwe	0.078	Benin	0	Guinea-Bissau	0
Sierra Leone	0.346	Togo	0.038	Lesotho	0	Namibia	0
Cote d'Ivoire	0.343	Mozambique	0	Chad	0	Equatorial Guinea	0
Ethiopia	0.282	Burundi	0	Eritrea	0	Malawi	0

Table 7.2.2: Global average in technical pillar by countries in the Africa region

7.3 Organizational

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

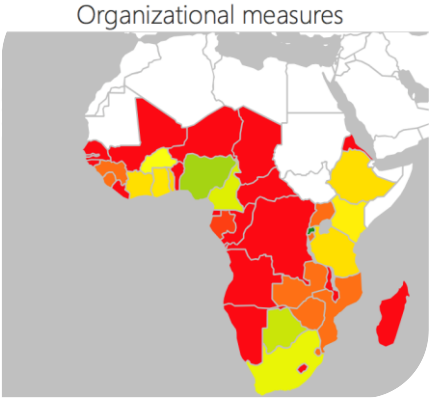


Figure 7.3.1: GCI Heat Map showing level of capacity building commitment in Africa region

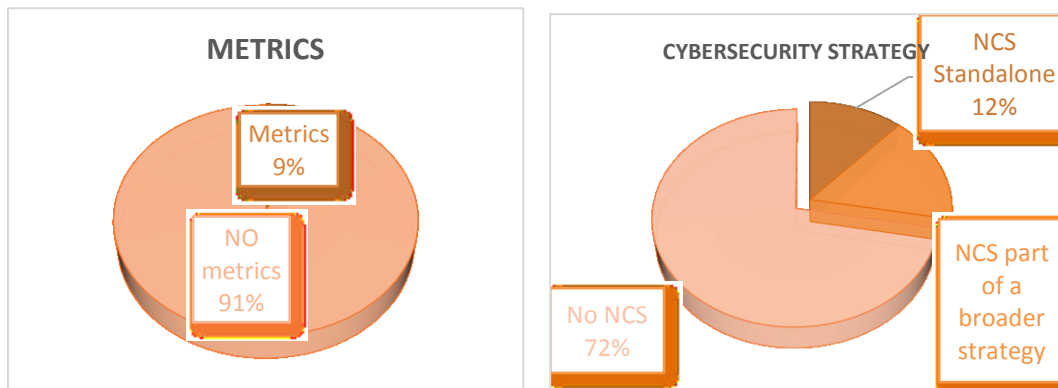
Sub-pillars	Number of countries that responded YES at the specified element in the sub-section	Maximum score	Regional average for countries having said YES	Global % of the specified element
Strategy	12	7.47	2.47	33.10
Responsible agency	20	6.57	4.76	72.50
Cybersecurity Metrics	4	5.63	3.43	60.89

Table 7.3.1: Global average in organizational sub-pillars


One of the strongest commitments is to outline a cybersecurity strategy describing how the country will prepare and respond to attacks against its digital networks. In Africa, more than 72% of all countries have no cybersecurity strategy and only 12% of all countries have a dedicated standalone strategy (Figure 6.3.1). Improvement needs to be done in that sub-pillar. A NCS is more efficient when it is standalone and includes a section on the protection of CII as they are vulnerable to cyber attacks and can be highly damaging to both the private and public sectors. In addition, a National Cyber Security strategy should include a resilience plan to foresee externalities/danger in a world of rapidly changing and alarming technologies.

In African countries, just 4 of 44 countries release metrics on cybersecurity incidents. In addition, only half possess a strong, regular risk assessment, with benchmarks that are rated and with mandatory regular audits. This challenges countries to objectively assess incidents based on the evidence and determine if protection measures are working.


Figure 7.3.2: Cybersecurity strategy and training commitments




7.3.1 Strategy

 **Nigeria** published a standalone National Cyber Security Strategy addressing private and public sector as well as CII in December 2016. This strategy provides a roadmap for industries including a specific chapter related to child online protection against abuses and sexual exploitations¹¹. This strategy is divided into different chapters with varied objectives depending on the approach and issues.

7.3.2 Responsible agency

 **Zambia** created the Zambia Information and Communications Technology Authority (ZICTA) in order to help the nation to become a digital society by ensuring the quality, security and access to ICT services and products. This ICT regulatory body falls under various Ministries and derives its mandate from different Acts. ZICTA is mandated to regulate, monitor the performance of electronic communication services, set standards for ICT area, promote competition and regulate tariffs of providers and protect the rights of consumers, providers etc.¹².

7.3.3 Cybersecurity metrics

 **Rwanda** has established the “SMART Rwanda Master Plan”, which is a strategic approach of various objectives in order to transform its economy through ICT’s from 2015 to 2020. To evaluate the efficiency of this project, they use Smart KPI (a metric to evaluate the efficiency). These KPIs are used to monitor the project as well as annual assessments¹³.

¹¹ [http://www.itu.int/en/ITU-](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Nigeria_2014_NATIONAL_CYBESECURITY_STRATEGY.pdf)

[D/Cybersecurity/Documents/National_Strategies_Repository/Nigeria_2014_NATIONAL_CYBESECURITY_STRATEGY.pdf](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Nigeria_2014_NATIONAL_CYBESECURITY_STRATEGY.pdf)

¹² <https://www.zicta.zm>

¹³ http://www.myict.gov.rw/fileadmin/Documents/Strategy/SRMP__GCIO_FAQ_s.pdf

Rwanda	0.794	Ethiopia	0.333	Senegal	0	Mali	0
Mauritius	0.739	Togo	0.317	Seychelles	0	South Sudan	0
Nigeria	0.531	Zimbabwe	0.167	Gambia	0	Cape Verde	0
Botswana	0.470	Mozambique	0.167	Niger	0	Sao Tome and Principe	0
Cameroon	0.435	Zambia	0.167	Liberia	0	Democratic Republic of the Congo	0
South Africa	0.416	Burundi	0.167	Madagascar	0	Congo	0
Burkina Faso	0.391	Guinea	0.167	Angola	0	Central African Republic	0
Kenya	0.357	Sierra Leone	0.167	Benin	0	Guinea-Bissau	0
Ghana	0.344	Swaziland	0.167	Lesotho	0	Namibia	0
Cote d'Ivoire	0.334	Uganda	0.165	Chad	0	Equatorial Guinea	0
Tajikistan	0.334	Gabon	0.095	Eritrea	0	Malawi	0

Table 7.3.2: Global average in organizational pillar by countries in the Africa region

7.4 Capacity building

Examples of practices for capacity building include the aspects of developing the technical and human resources for countering cybercrime. This includes raising public awareness on cybersecurity issues, advance already existing cybersecurity standards and institutional bodies, best practices guides, research and education initiatives.

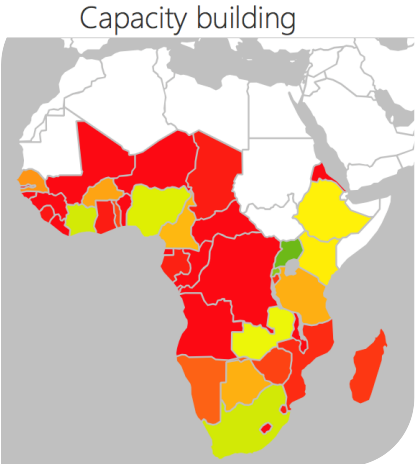


Figure 7.4.1: GCI Heat Map showing level of capacity building commitment in Africa region

The heap map reveals that there is a strong need for capacity building programs and capabilities in most countries in Africa, except for Uganda which scores well.

<i>Sub-pillars</i>	Number of countries that responded YES at the specified element in the sub-section	Maximum score	Regional average for countries having said YES	Global % of the specified element
<i>Standardization bodies</i>	18	1.40	1.05	74.84
<i>Good practices</i>	10	3.03	3.03	100.00
<i>R & D programmes</i>	11	2.77	1.49	53.69
<i>Public awareness campaigns</i>	15	2.43	1.44	59.31
<i>Professional training courses</i>	13	2.51	1.95	77.81
<i>National education programs and academic curricula</i>	11	2.67	1.13	42.46
<i>Incentive mechanisms</i>	9	2.20	1.71	77.78
<i>Home-grown cybersecurity industry</i>	4	1.92	0.76	39.79

Table 7.4.1: Global average in capacity building sub-pillars

In all sub-pillars of the capacity building section, less than 20 countries out of 44 have been indicated. This demonstrates the low response rate in this section. Having a standardization body is more relevant when it develops its own standards and adopts international ones. It is advantageous to have a body overseeing research and development programs as well, as it is also fundamental to develop and provides training courses for professional and educational programs for all the different sectors within the country.

Publishing awareness campaigns is exceptionally important but needs to be adapted for the different target audiences. Public campaigns are more effective if they deliver free accessible protection programs and software or service based solutions.

Also, improvements need to be made in the areas of national education programs, academic curricula and research and development programs as they reached only 42% of the items of that sub-pillar and only 11 countries established that kind of capacity building activity.

Finally, a government needs to encourage the development of a homegrown industry and support society to build or develop a start-up cybersecurity industry, to be more resilient and facilitate access, by some monetary advantages. In Africa, more than 90% of countries replied negatively to the existence of a homegrown cybersecurity industry (figure 6.4.1).

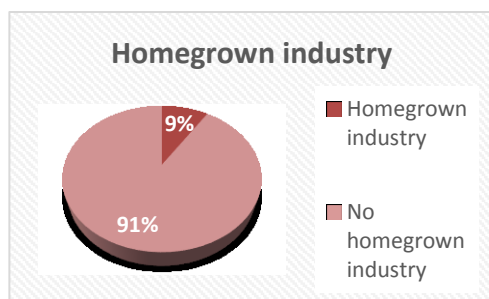




Figure 7.4.1: Home-grown industry

7.4.1 Standardization bodies

 **Nigeria** established the National Information Technology Development Agency (NITDA) in 2001. The Agency implements and coordinates IT development and policies in the country. It has various objectives but in particular, one of its function is to create a framework for standardization, evaluation and regulation of IT practices, systems and activities where regulatory standards, guidelines and policies are created¹⁴.


7.4.2 Good practice

 **Cote d'Ivoire** created ARCTI, Autorité des régulations des télécommunications de Côte d'Ivoire in 2012. ARTCI is an administrative body with a legal personality and financial autonomy, the missions of which are legally determined. It is an independent body that defines principles about telecommunication services and products, and regulates the market. It also protects the consumers in both private and public sectors¹⁵.


¹⁴ <http://nitda.gov.ng/about-nitda/>

¹⁵ <http://www.artci.ci/index.php/en/about-artci/Foundation-and-Missions/establishment-and-missions.html>


7.4.3 Cybersecurity research and development programs

 **Kenya** Education Network, (KENET), is the National Research and Education Network (NREN) of Kenya. KENET is the computer emergency response team (CERT) for the academic community and is licensed by the Communications Authority of Kenya (CA)¹⁶ as a not-for-profit operator serving the education and research institutions. They most notably provide affordable, cost-effective and low-congestion Internet bandwidth services to member institution campuses in Kenya.


7.4.4 Public awareness campaigns

 **South Africa** has a dedicated website for raising cybersecurity awareness to all groupings of populations. Every year, South Africa Cyber Security Academic Alliance conducts a National Cyber Security Week where various workshops are proposed around the theme of cybersecurity for primary schools in collaboration with universities. Also, the NMMU Institute for ICT Advancement makes flyers with general guidelines to help parents and children to be protected against cyber threat. It organizes an annual poster contest, open to everyone in South Africa, for raising awareness on a security matter¹⁷.


7.4.5 Cybersecurity professional training courses

 **Rwanda** Development Board ICT Skills MIS provides multiples courses and ICT certifications to ICT professionals, graduates, students and employers. Courses are selected by the type of position. Rwanda Development Board has various partners in the public and private sector such as ministries, Public Service Commission, Private Sector Federation, Institutions of learning, Private ICT training center and ICT Testing centre.

7.4.6 National education programmes and academic curricula

 **Burundi** University, in its Engineering Institute, proposes two different education programs in ICT development. The first one is on communications and the second in informatics¹⁸.

7.4.7 Incentive mechanisms

 **Zimbabwe** has a body coordinating country-wide cybersecurity capacity building activities named The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ).

POTRAZ's mission is legally binding by the Postal and Telecommunication Act {Chapter 12:05} which defines the functions and powers of the Authority to ensure the provision of domestic and international telecommunication and postal services throughout Zimbabwe¹⁹.


¹⁶ <http://www.ca.go.ke>

¹⁷ http://www.cyberaware.org.za/?page_id=537

¹⁸ <http://www.ub.edu.bi/wp-content/uploads/2015/01/7.-FSI-Maquettes.pdf>

¹⁹ <http://www.potraz.gov.zw/index.php/about-us/>

7.4.8 Home-grown cybersecurity industry

 **Gabon** has established a project on Mandji Island where the ICT companies operating in the CMI are exempted from taxes during the first 10 years and are taxed only 10 % from the 11th year. Also, these ICT's companies will have a facilitated access to a fast registration and no restriction on funds transfer²⁰.

Mauritius	0.914	Tajikistan	0.302	Ghana	0.044	Eritrea	0
Uganda	0.717	Burkina Faso	0.282	Chad	0.044	Mali	0
Rwanda	0.657	Senegall	0.257	South Sudan	0.044	Cape Verde	0
South Africa	0.525	Namibia	0.169	Swaziland	0.044	Guinea	0
Cote d'Ivoire	0.523	Togo	0.132	Sierra Leone	0.033	Sao Tome and Principe	0
Nigeria	0.501	Zimbabwe	0.116	Gambia	0	Dem. Rep. of the Congo	0
Zambia	0.475	Madagascar	0.096	Niger	0	Congo	0
Ethiopia	0.416	Burundi	0.096	Liberia	0	Central African Republic	0
Kenya	0.408	Seychelles	0.073	Angola	0.000	Guinea-Bissau	0
Cameroon	0.317	Mozambique	0.073	Benin	0.000	Equatorial Guinea	0
Botswana	0.304	Gabon	0.055	Lesotho	0.000	Malawi	0

Table 7.4.2: Global average in capacity building pillar by countries in the Africa region

²⁰ <http://www.cto.int/media/events/pst-ev/2012/>

ICT%20Finance/Telecom%20Policy%20and%20Regulation%20for%20Next%20Generation%20Networks%20Gabon.pdf

7.5 Cooperation

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

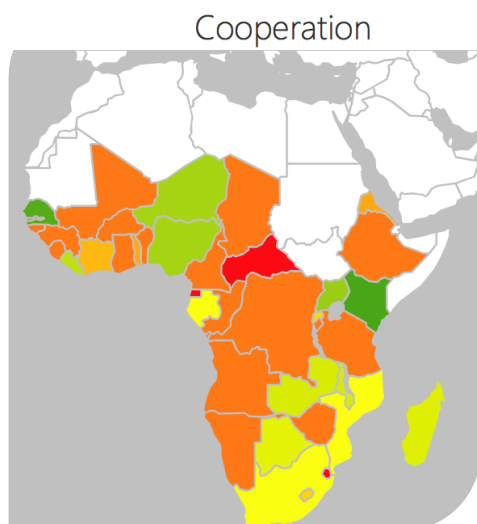


Figure 7.5.1: GCI Heat Map showing level of cooperation commitment in Africa region

<i>Sub-pillars</i>	Number of countries that responded YES at the specified element in the sub-section	Maximum score	Regional average for countries having said YES	Global % of the specified element
<i>Intra-state Cooperation</i>	8	4.14	1.95	47.13
<i>Multilateral agreements</i>	10	5.04	3.30	65.52
<i>International fora participation</i>	40	3.37	3.37	100.00
<i>Public-Private Partnerships</i>	7	4.82	3.51	72.73
<i>Inter-agency partnerships</i>	7	3.97	3.97	100.00

Table 7.5.1: Global average in cooperation sub-pillars

The potential for cooperation is enhanced by participation in international cybersecurity events with 93% of countries replying affirmatively.

The strengthening of international, regional and national partnerships regarding cybersecurity issues with a view to sharing knowledge and best practices to prevent and combat cybercrime is essential and only possible with cooperation among nations. The scope of digital space is enormous therefore international cooperation is required to further facilitate management of cybersecurity systems and make the process durable.

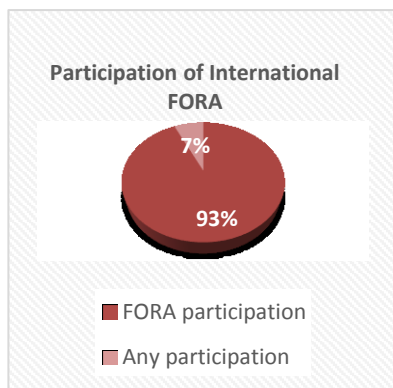



Figure 7.5.2: participation of International FORA)

Overall, the importance of cooperation in Africa region is mitigated. Almost 93% of responding countries report participation in International fora while only 7% do not have any bilateral agreements with other regional nations, nor multilateral or international mechanisms with more than two parties. Along with this, the majority of African countries have no partnerships with public and private sectors including local and foreign companies.

 **Malawi** has adopted the reference framework for Harmonization of the Telecommunication and ICT Policies and Regulation in Africa with ITU and the European Commission. The project aimed to develop a strong, integrated and efficient communication in the Africa continent. HIPSSA provides guidelines for ICT market as well as building human and institutional capacities in ICT fields and is legally binding²¹.

7.5.1 Participation in international fora

Participation in international cybersecurity events, workshops and training is a single indicator where Member States give favorable consideration to the GCI.

Additionally, ITU collaborates closely with FIRST, Interpol, UNODC, and World Bank to ensure effective coordination with Member States and information exchange relevant to measuring cybersecurity.

7.5.2 Public-private partnerships

 **Madagascar** is working with local and foreign companies, and international and non-governmental institutions such as UNICEF, Orange and Arozaza.

²¹ <http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/Launching-Meeting-HIPSSA.aspx>

7.5.3 Interagency partnerships


 **South Africa** established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF), passed by Cabinet in 2012. The hub enhances interaction and consultation as well as promoting a coordinated approach regarding engagements with the private sector and civil society²².

Table 7.5.2: Global average in cooperation pillar by countries in the Africa region

Mauritius	0.700	South Africa	0.346	Burkina Faso	0.158	Benin	0.158
Kenya	0.604	Mozambique	0.344	Namibia	0.158	Mali	0.158
Senegal	0.588	Gabon	0.344	Zimbabwe	0.158	Cape Verde	0.158
Uganda	0.485	Rwanda	0.281	Burundi	0.158	Guinea	0.158
Niger	0.468	Lesotho	0.278	Seychelles	0.158	Sao Tome and Principe	0.158
Nigeria	0.467	Cote d'Ivoire	0.244	Ghana	0.158	Democratic Republic of the Congo	0.158
Liberia	0.432	Togo	0.223	Chad	0.158	Congo	0.158
Zambia	0.394	Eritrea	0.223	South Sudan	0.158	Guinea-Bissau	0.158
Malawi	0.394	Ethiopia	0.158	Sierra Leone	0.158	Swaziland	0
Madagascar	0.384	Cameroon	0.158	Gambia	0.158	Central African Republic	0
Botswana	0.375	Tajikistan	0.158	Angola	0.158	Equatorial Guinea	0

²² <http://www.apre.it/media/183485/martinelli.pdf>

8. Conclusion

The new generation of cybercriminals do not need our approval or awareness to access valuable data, which could lead to the leak of personal data or theft of a large amount of money. As more people are now getting access to Internet all over the world specifically in Africa, governments and private sector tend to increase their online presence due to a competitive market and the rapidly changing international scene. However, misuse of computers and communications systems comes every day. The explosion in global connectivity has given rise to questions such as how to ensure a state's security and how to protect businesses in a highly technological age.

Due to the shifts in the Africa region influenced by the rapid technical progress, some challenges posed by cybercrime have emerged. Although there is a steady development of a cybersecurity culture, only 6 out of 44 countries have reached the level that allows a safe use of technologies. This shows a huge gap between the different nations in the continent. Therefore, the few prosperous economies in Africa ought to contribute to the elaboration of the poorest, hence increasing connectivity within the region and globally. Collaboration with Member States and business entities is essential to cultivate awareness and security in the digital space.

It is essential for the Global Cybersecurity Index to raise awareness of the importance of cybersecurity and promote knowledge exchange on the best practices in the field. In this regard, ITU invites all Member States and industry stakeholders in Africa region to actively participate in future efforts to enhance the current reference model. A lack of a common approach may largely challenge the quality of the GCI and cooperation in cybercrime matters, therefore ITU calls on Member States to take part in the coming GCI survey. Additionally, ITU would like to thank all Member States and international partners for their valuable contribution to the GCI survey and the publication of this report.

Annex 1: Abbreviations

CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GOVCERT	Governmental Computer Emergency Response Team
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
ITU	International Telecommunication Union
ISP	Internet Service Provider
NCS	National Cybersecurity Strategy
R&D	Research and Development
IDI	ICT Development Index
NITDA	National Information Technology Development Agency
UNODC	The United Nations Office on Drugs and Crime
HIPSSA	Harmonization of ICT Policies in Sub-Saharan Africa
UNICEF	The United Nations Children's Fund

Annex 2: ITU African Member states global cybersecurity commitment score

Country	Normalised score	Global rank	Regional rank
Mauritius	0.830	6	1
Rwanda	0.602	36	2
Kenya	0.574	45	3
Nigeria	0.569	46	4
Uganda	0.536	50	5
South Africa	0.502	58	6
Botswana	0.430	69	7
Cote d'Ivoire	0.416	74	8
Cameroon	0.413	75	9
Ghana	0.326	87	10
Tajikistan	0.317	88	11
Senegal	0.314	89	12
Zambia	0.292	91	13
Ethiopia	0.267	99	14
Togo	0.218	107	15
Burkina Faso	0.208	108	16
Mozambique	0.206	109	17
Zimbabwe	0.192	113	18
Seychelles	0.184	115	19
Niger	0.170	120	20
Madagascar	0.168	121	21
Liberia	0.149	124	22
Sierra Leone	0.145	126	23
Gabon	0.139	128	24
Gambia	0.136	130	25
Burundi	0.120	135	26
Lesotho	0.094	143	27
Guinea	0.090	144	28
Malawi	0.084	145	29
Angola	0.078	146	30
Eritrea	0.076	147	31
Chad	0.072	148	32
Benin	0.069	149	33
South Sudan	0.067	150	34
Namibia	0.066	151	35
Mali	0.060	152	36
Cape Verde	0.058	153	37
Swaziland	0.041	160	38
Sao Tome and Principe	0.040	161	39
Democratic Republic of the Congo	0.040	161	39
Congo	0.040	161	39
Guinea-Bissau	0.034	162	40
Central African Republic	0.007	164	41
Equatorial Guinea	0.000	165	42

Annex 3: Tables and figures

Tables

Table 4.2.1: GCI African Tiers

Table 4.3.2: Commitment of Africa region in figures

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

Table 6.2: Top three ranked countries in the Africa region

Table 7.1: Average and global percentage of all the five GCI pillars (25 indicators) of the Africa region

Table 7.1.1: Global average in legal sub-pillars

Table 7.1.2: Global average in legal pillar by countries in the Africa region

Table 7.2.1: Global average in technical sub-pillars

Table 7.2.2: Global average in technical pillar by countries in the Africa region

Table 7.3.1: Global average in organizational sub-pillars

Table 7.3.2: Global average in organizational pillar by countries in the Africa region

Table 7.4.1: Global average in capacity building sub-pillars

Table 7.4.2: Global average in capacity building pillar by countries in the Africa region

Table 7.5.1: Global average in cooperation sub-pillars

Table 7.4.2: Global average in cooperation pillar by countries in the Africa region

Figures

Figure 3.3.1: GCI pillars and sub-pillars

Figure 3.3.2: GCA tree structure illustrating all pillars (simplified)

Figure 3.3.3: GCI tree structure illustrating Legal pillar

Figure 4.1.1: GCI Heat Map showing Africa commitment

Figure 4.1.2: GCI Heat Map by sub-region

Figure 4.1.1: Global comparison GCI and IDI

Figure 4.1.2 Global comparison of GCI and IDI with other regions.

Figure 4.1.3: GCI and IDI comparison in Africa region

Figure 4.1.4: Africa region scorecard

Figure 5.1: Top three ranked countries and an average score of all the Africa region

Figure 5.1.1: Global comparison GCI and IDI

Figure 5.1.2: Comparison GCI and IDI in the Africa region

Figure 5.1.3: Africa region scorecard

Figure 6.1: Average GCI score for each region

Figure 6.2: Average of Top three ranked countries in Africa

Figure 7.1.1: GCI Heat Map showing level of legal commitment in the Africa region

Figure 7.1.2: Cybersecurity training commitments

Figure 7.2.1: GCI Heat Map showing level of technical commitment in the Africa region

Figure 7.3.1: GCI Heat Map showing level of organizational commitment in the Africa region

Figure 7.3.2: Cybersecurity strategy and metrics

Figure 7.4.1: GCI Heat Map showing level of capacity building commitment in the Africa region

Figure 7.4.2: Home-grown industry and international participation

Figure 7.5.1: GCI Heat Map showing level of cooperation commitment in the Africa region

Figure 7.5.2: participation of International FORA)