GCI 2017

Regional report

CIS

Region

Report

Table of Contents

1 Executive Summary 3

2 Introduction 4

3. GCI Scope and Framework 6

4.1 Heat Map of National Cybersecurity Commitments 11

4.2 GCI Groups 11

4.3 GCI Africa region commitment in figures 13

6. Regional Outlook 16

7. Illustrative practices by pillar 18

7.1 Legal 19

7.2 Technical 21

7.3 Organizational 23

7.4 Capacity building 26

7.5 Cooperation 29

8. Conclusion 32

9. Annex 1 Abbreviations 33

Annex 2: ITU CIS Member States Global Cybersecurity Commitment Score 34

Annex 3: List of Tables and Figures 35

Table 35

Figures 35

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 commitment 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 survey is provided to present an accurate picture of the cybersecurity situation in the CIS region. 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 users[1]) and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020[2]. Yet, just as in the real world, the 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.

The Member States from the CIS region have adopted an extensive engagement with the ITU and the IGF on matters of cybersecurity. In 2014 at the World Telecommunication Development Conference (WTDC-14), the CIS countries identified the following five priority areas: child online protection; ensuring access to ICTs for persons with disabilities; using ICTs for human capacity building; development of broadband access; and building confidence and security in the use of ICTs. These priorities, articulated as the CIS key regional initiatives, are not unique to this region and reflect global trends addressed in the Dubai Action Plan in the use of ICTs and cybersecurity.[3]

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.

The ITU oversees the development of the knowledge, awareness and capacity in member countries. This report specifically relates to the CIS Region. This region comprises of 12 Member States; Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kazakhstan, Moldova, Russian Federation, Tajikistan, Turkmenistan, Ukraine and Uzbekistan

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

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

[3] https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2015/03_Chisinau/e-BAT_ITU_CIS_BROCHURE_interactive.pdf

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 CIS5 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 analyzing 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 below[4].

[4] 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 Research[1], and the final results have been published[2].

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

The data collected via GCI 2017 for ITU-D Study Group 2 Question 3 (SG2Q3) surveys have been analyzed 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.

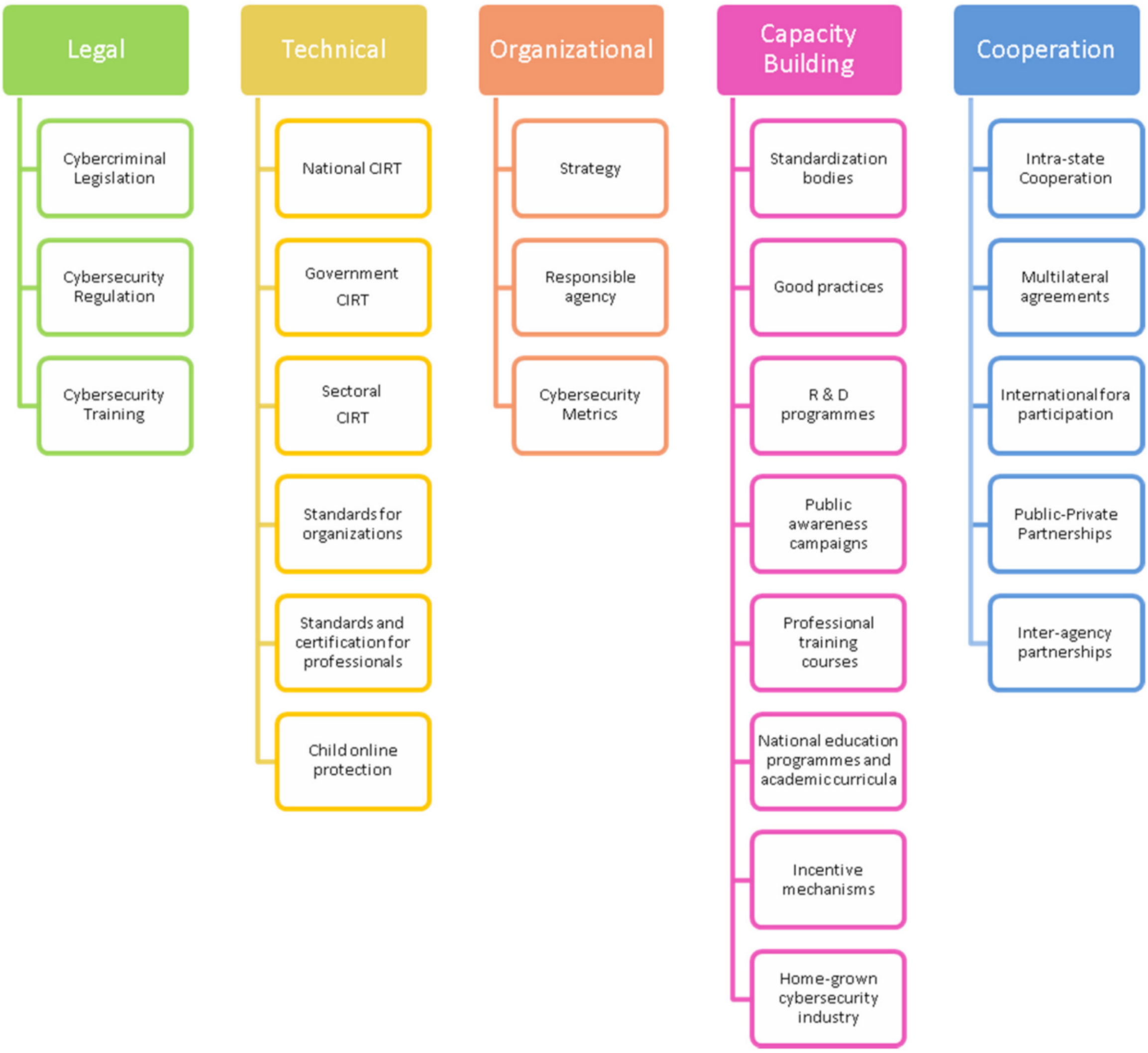
3.3 Conceptual framework

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. 5 Global Cybersecurity Index 2017

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)

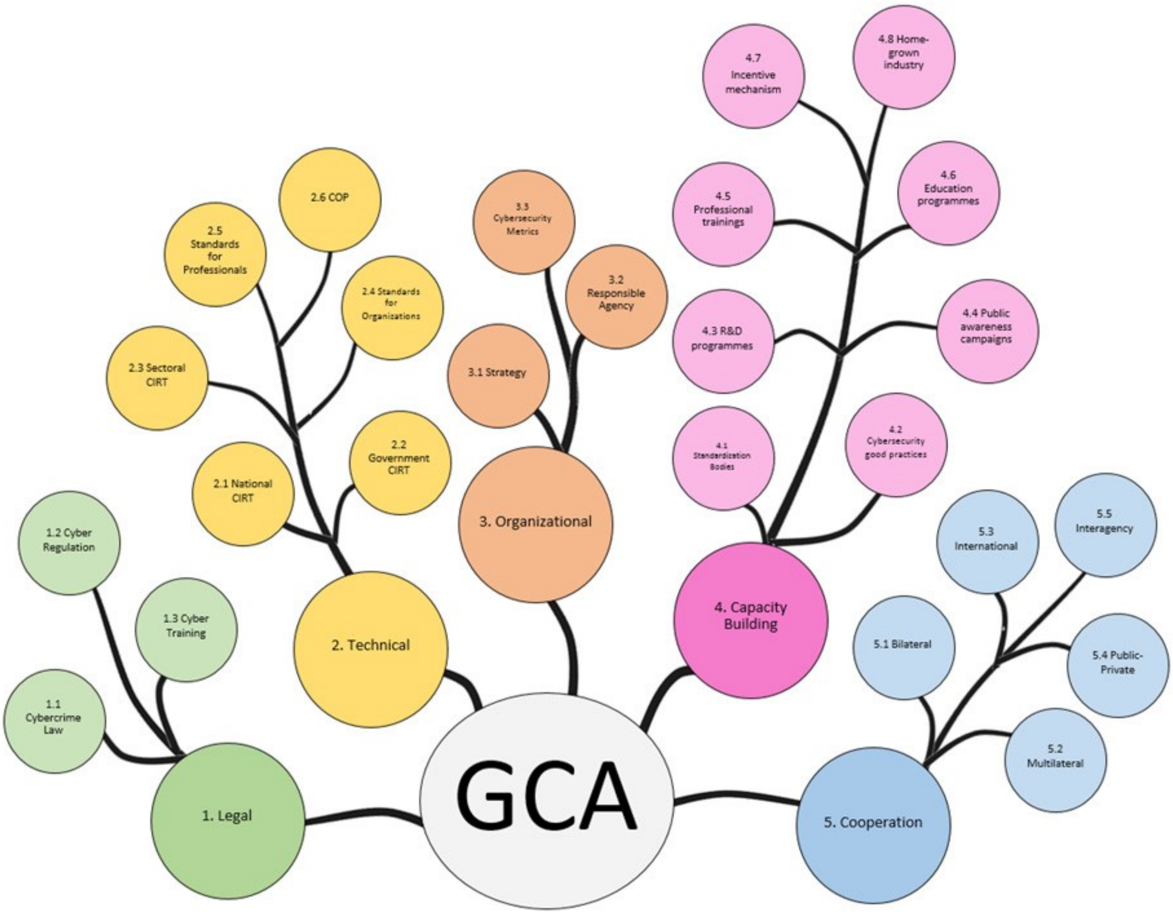
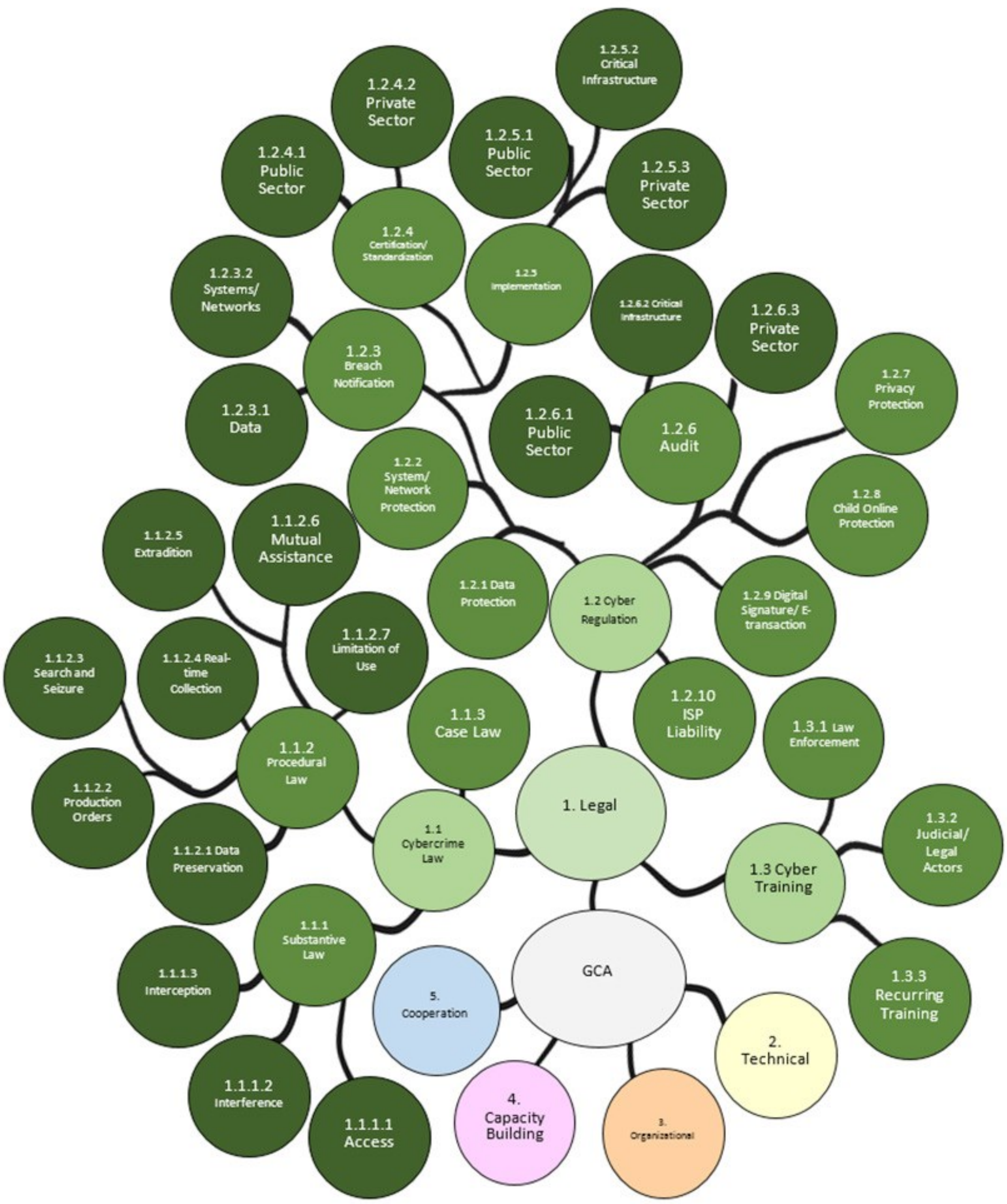


Figure 3.3.3 below illustrates the relationship between the GCA, the pillars, sub-pillars and questions (expanded only for the legal pillar due to space considerations).

Figure 3.3.3: GCI tree structure illustrating Legal pillar



4. Key Findings

This section presents the key findings of the Global Cybersecurity Index 2017 (GCI 2017) for the CIS region, which were drawn from the results of the GCI survey conducted in 2016 and presented in 2017 under the five pillars of the Global Cybersecurity Agenda (GCA): Legal, Technical, Organizational, Capacity building and Cooperation measures. These findings indicate how active and committed the CIS 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 12 Member States in the CIS region, quite a good level of cybersecurity commitment can be observed, as the heat map below illustrates.

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

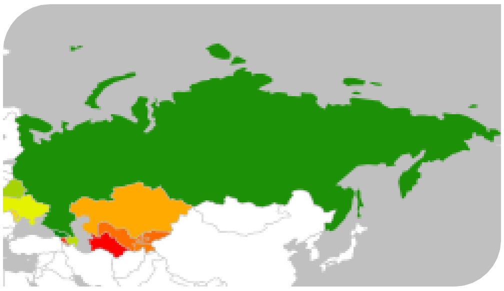


Figure 4.1.1: GCI Heat Map of the CIS region

4.2 GCI Groups

CIS Member States were classified into three categories by their GCI score (table 4.2.1). The commitment to cybersecurity of the CIS region is well illustrated in the heat map and the table, where most countries are in the leading and maturing stages.

These following heat maps show the cybersecurity commitment of countries by the three stages (leading, maturing and initiating). The leading stage is represented in the North, with only one country in the South.

- *Leading stage* refers to the 3 countries (i.e., GCI score in the 60th percentile and higher) that demonstrate high commitment.
- *Maturing stage* refers to the 4 countries (i.e., GCI score between the 30th and 59th percentile) that have developed complex commitments, and engage in cybersecurity programmes and initiatives.
- *Initiating stage* refers to the 5 countries (i.e., GCI score less than the 30th percentile) that have started to make commitments in cybersecurity.

Leading stage	
Russian Federation	0.819
Georgia	0.788
Tajikistan	0.592
Maturing stage	
Moldova	0.559
Ukraine	0.501
Belarus	0.418
Uzbekistan	0.352
Initiating stage	
Azerbaijan	0.292
Kazakhstan	0.277
Kyrgyzstan	0.270
Armenia	0.196
Turkmenistan	0.133

Table 4.2.1: GCI Tiers

4.3 GCI Africa region commitment in figures

Below is a table showing how many countries in the CIS region have a specified cybersecurity indicator out of the 12 countries in the region. This analysis consists of 7 countries that responded to the survey and the 5 that didn't respond and their data was collected through primary research.

Sub-pillars	Number of countries that responded YES at the specified element in the sub-section
Cybercriminal Legislation	11
Cybersecurity Regulation	12
Cybersecurity Training	7
National CIRT	8
Government CIRT	8
Sectoral CIRT	4
Standards implementation framework for organizations	4
Standards and certification for professionals	4
Strategy	6
Responsible agency	11
Cybersecurity Metrics	2
Standardization bodies	8
Good practices	6
R & D programmes	7
Public awareness campaigns	10
Professional training courses	7
National education programmes and academic curricula	8
Incentive mechanisms	3
Home-grown cybersecurity industry	3
Intra-state Cooperation	7
Multilateral agreements	6
International fora participation	10
Public-Private Partnerships	4
Inter-agency partnerships	7

Table 4.3.1: commitment of CIS 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.

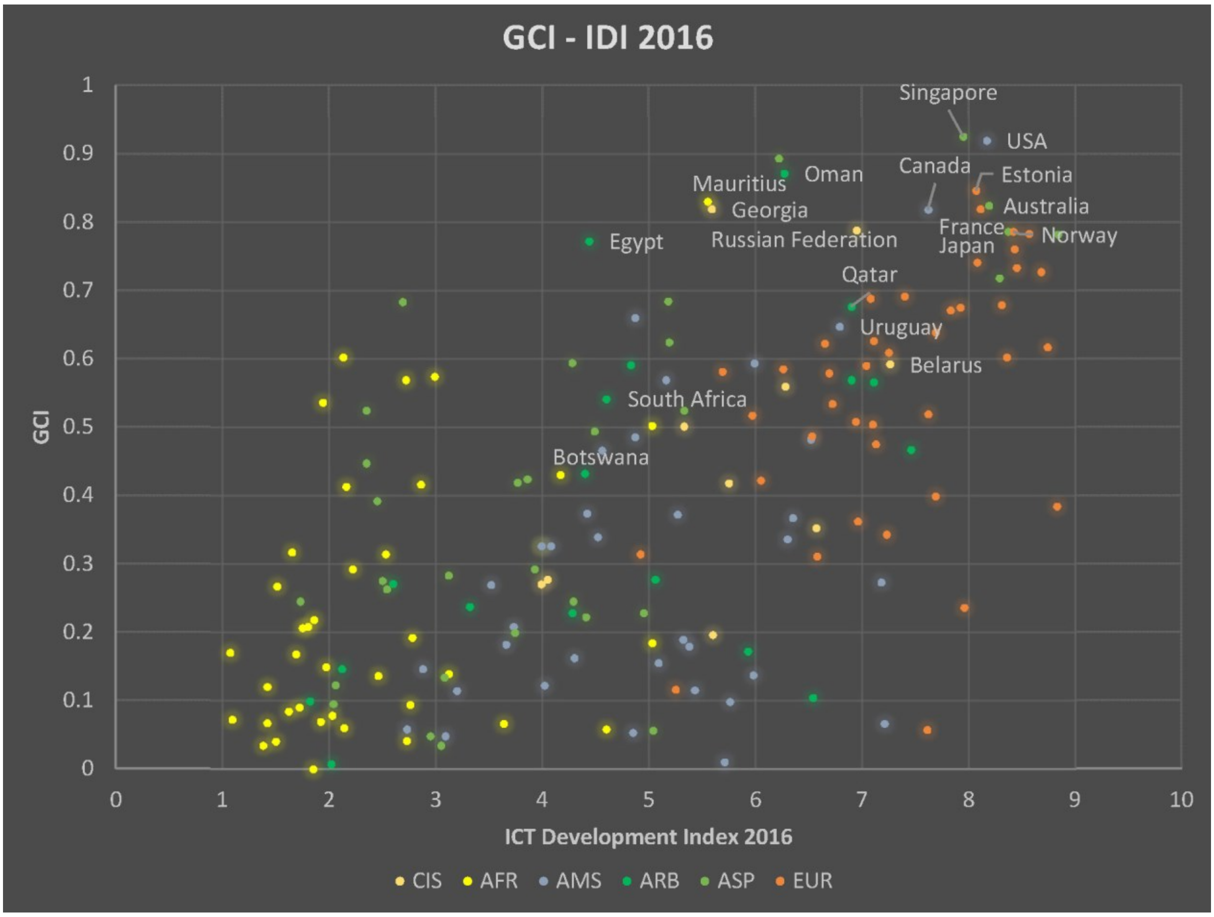


Figure 5.1.1: Global comparison GCI and IDI

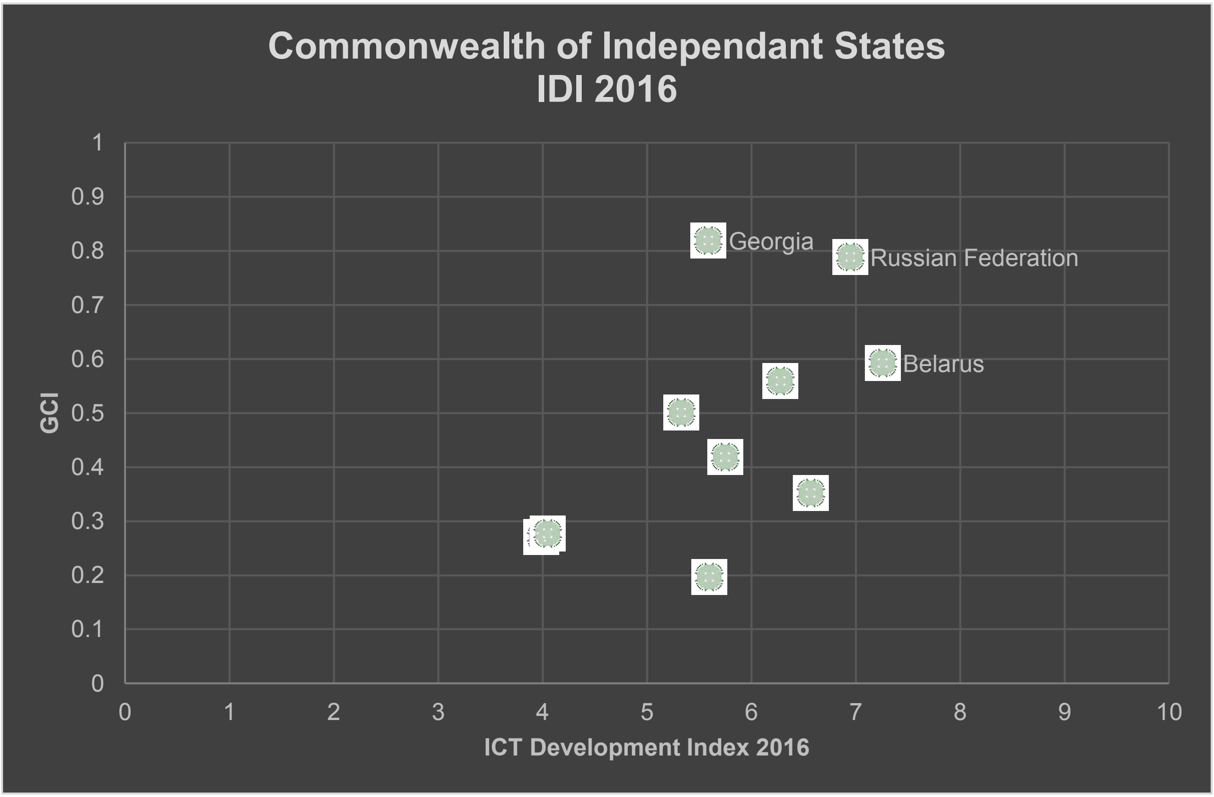


Figure 5.1.2: GCI and IDI comparison in the CIS region

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

Figure 5.1.3: the CIS region scorecard

6. Regional Outlook

During the active data collection phase of the GCI 2017 exercise 7 of the 12 Member States in the CIS 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 CIS region, the average scores are relatively high across all pillars except a lower capacity building pillar.

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
Russian Federation	0.78	0.82	0.67	0.85	0.91	0.70
Belarus	0.59	0.85	0.63	0.33	0.68	0.47

Table 6.1: Top three ranked countries in the CIS region

Georgia is top ranked in the CIS. After large-scale cyber-attacks on the country in 2008, the government has strongly supported protection of the country's information systems[5]. The information Security Law[6] established a Cyber Security Bureau with a particular emphasis on protecting critical information systems in the military sphere.

The Russian Federation, ranked second in the region, scores best in capacity building. Its commitments range from developing cybersecurity standards to R&D and from public awareness to a home-grown cybersecurity industry. An example of the latter is Kaspersky Labs, founded in 1997 and whose software protects over 400 million users and some 270 000 organizations[7].

Belarus is the third ranked country, where child protection initiatives include public and private partnerships. Mobile operator MTS has implemented a project with the Ministry of Education to teach children about safe Internet practices that to date has reached some 6 000 children[8].

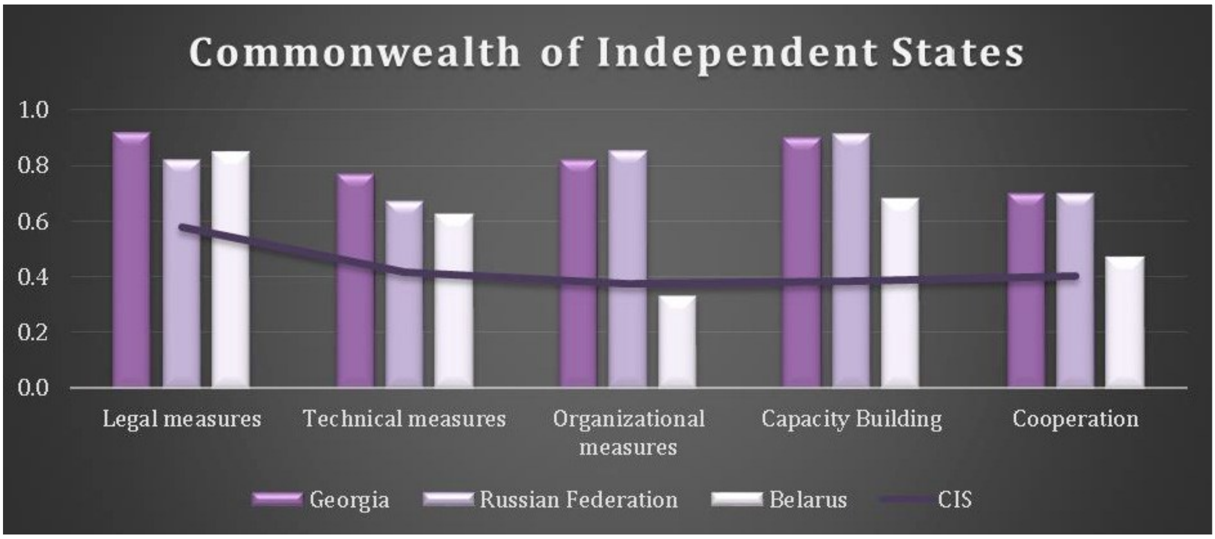


Figure 6.2: Top three ranked countries in the Commonwealth of Independent States

[5] http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx?lang=en-US

[6] https://matsne.gov.ge/en/document/view/1679424

[7] https://usa.kaspersky.com/about

[8] http://www.mts.by/news/97338/

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 CIS region. Examples are drawn from a number of countries and provide an insight on the cybersecurity commitment taken in their focus areas.

Sub-pillars	Number of countries that responded YES at the specified element in the sub-section	Maximum score	Average for countries responded positively to the elements	Global % of the element in the sub-pillar
Cybercriminal Legislation	11	7.82	5.10	65.22
Cybersecurity Regulation	12	6.84	4.98	72.81
Cybersecurity Training	7	6.28	4.25	67.68
National CIRT	8	4.66	3.69	79.18
Government CIRT	8	3.03	3.03	100.00
Sectoral CIRT	4	2.71	2.71	100.00
Standards implementation framework for organizations	4	3.13	3.13	100.00
Standards and certification for professionals	4	2.71	1.77	65.31
Strategy	6	4.55	2.94	64.62
Responsible agency	11	6.57	5.38	81.89
Cybersecurity Metrics	2	5.62	3.62	100.00
Standardization bodies	8	1. 39	1.11	79.86
Good practices	6	3.03	3.03	100.00
R & D programmes	7	2.77	1.72	62.09
Public awareness campaigns	10	2.44	1.45	59.43
Professional training courses	7	2.50	1.72	68.80
National education programmes and academic curricula	8	2.67	1.40	52.43
Incentive mechanisms	3	2.20	1.83	83.18
Home-grown cybersecurity industry	3	1.91	1.62	84.82
Intra-state Cooperation	7	1.64	1.26	76.83
Multilateral agreements	6	5.04	2.75	54.56
International fora participation	10	3.37	3.37	100.00
Public-Private Partnerships	4	4.82	4.16	86.31
Inter-agency partnerships	7	3.97	3.97	100.00

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

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 particularly for professionals who are handling cybersecurity crimes.

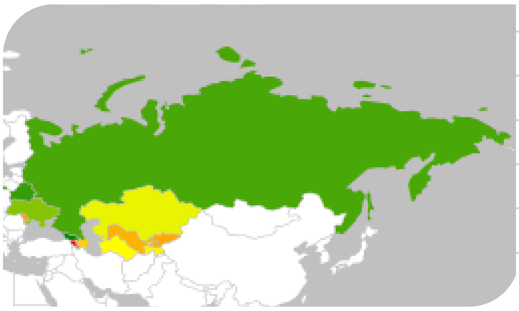
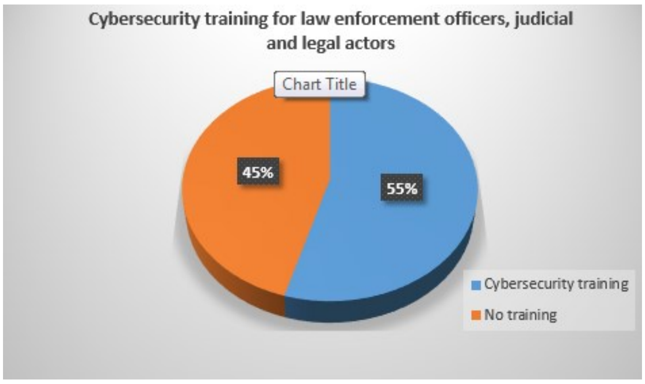


Figure 7.1.1: GCI Heat Map showing level of legal commitment in the CIS region

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 to the element	Global % of the specified element
Cybercriminal Legislation	11	7.82	5.10	65.22
Cybersecurity Regulation	12	6.84	4.98	72.81
Cybersecurity Training	7	6.28	4.25	67.68

Table 7.1.1: Global average in legal sub-pillars



In the CIS region, more than 50 % of the Member States have programs for law enforcement and the judicial system (Figure 7.1.2).

Figure 7.1.2: Cybersecurity training commitments

7.1.1 Cybercrime legislation

Kazakhstan has the Criminal Code that highlights the illegal access to computer information, and the creation, use, and distribution of harmful programmes for computers. In particular, cyber-dependent and cyber-enabled crimes entailed serious consequences including a fine or imprisonment for a period up to five years[9].

7.1.2 Cybersecurity regulation

Belarus adopted a law concerning regulations provided at the regional level on the sphere of information, informatization and protection of information. The specific articles included: the use of informational resources; technical normalization and standardization in the sphere of informatization, informational technologies, networks and their maintenance tools; data abuse[10].

7.1.3 Cybersecurity training

Russia has reported the establishment of a cyber-specific faculty at the Moscow University of the Ministry of Internal Affairs of the Russian Federation, aimed at the development and implementation of new training practices in the field of information security for the law enforcement agencies[11].

Armenia	0.209	Moldova	0.42
Azerbaijan	0.486	Russia	0.817
Belarus	0.847	Tajikistan	0.53
Georgia	0.915	Turkmenistan	0.546
Kazakhstan	0.581	Ukraine	0.728
Kyrgyzstan	0.432	Uzbekistan	0.446

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

[9] https://www.unodc.org/cld/legislation/kaz/criminal_code_of_the_republic_of_kazakhstan/special_part_-_chapter_7/article_227/article_227.html?lng=en

[10] http://www.pravo.by/document/?guid=3871&p0=H10800455

[11] https://xn--l1aeji.xn--b1aew.xn--p1ai/document/3333760

7.2 Technical

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

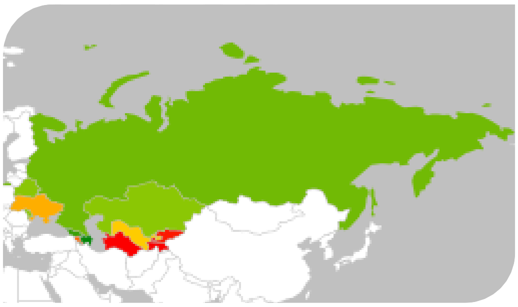


Figure 7.2.1: GCI Heat Map showing level of technical commitment in the CIS region

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**
National CIRT	8	4.66	3.69	79.18
Government CIRT	8	3.03	3.03	100.00
Sectoral CIRT		2.71	2.71	100.00
Standards implementation framework for organizations	4	3.13	3.13	100.00
Standards and certification for professionals	4	2.71	1.77	65.31

Table 7.2.1: Global average in technical sub-pillars

In this pillar, the CIS region is performing better in the CERT area, especially in the National CERT that provides information and assistance related to cyberspace in all national structures. Overall, it shows that most countries have a national, a governmental and a sectoral CERT.

Cybersecurity certification is an important component in today's world where hacking has become more and more dangerous and inevitable. It is a way of protecting IoT's, networks and data. Special criteria given by a certification body enhances the protection of products and services against cyber threats. More standards, however, are needed 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.

In effect, only 4 countries dispose of such a framework while more than half of the CIS countries have an emergency response team (i.e., CIRT, CSRIT, and CERT) with national responsibility (**Table 7.2.1**).

National CERT/CIRT/CSIRT

Azerbaijan benefits from the Electronic Security Center (CERT), a government body, which identifies and prevents cybersecurity threats; and raises national awareness of existing and emerging cybersecurity threats. CERT, in collaboration with the national operator, Ministry of Transport, Communications and High Technologies and other authorities, conducts preventive measures to counter cyber related threats and secure digital space[12].

7.2.1 Government CERT/CIRT/CSIRT

Georgia has a computer emergency team (CERT.GOV.GE), which operates under the Data Exchange Agency of the Ministry of Justice and is responsible for handling critical incidents that occur within Georgian governmental networks and critical infrastructure. CERT.GOV.GE specializes in identifying, registering and analysing critical computer incidents, issues recommendations and conducts prompt responses to such occurrences[13].

7.2.2 Sectoral CERT/CIRT/CSIRT

Azerbaijan established the AzScienceCERT, an information security incidents response group in the Internet network (AzScienceNet) of Azerbaijan National Academy of Sciences (ANAS). The main objective of AzScienceCERT is maintaining the information security risks in AzScienceNet at an acceptable level. For this purpose AzScienceCERT helps ANAS organizations and AzScienceNet users in detecting, preventing and informing the actions that violate information security[14].

7.2.3 Cybersecurity standards implementation framework for organizations

Armenia adopted the Information security management system (ISO/IEC 27000) dedicated to the development of international management systems standards for information security (ISMS)[15].

[12] http://www.cert.az/haqqimizda

[13] http://www.cert.gov.ge/

[14] http://www.sciencecert.az/en/index.html

[15] http://www.sarm.am/en/standarts/view/129408

Armenia	0.164	Moldova	0.62
Azerbaijan	0.86	Russia	0.67
Belarus	0.625	Tajikistan	0
Georgia	0.767	Turkmenistan	0
Kazakhstan	0.622	Ukraine	0.282
Kyrgyzstan	0.04	Uzbekistan	0.33

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

7.3 Organizational

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

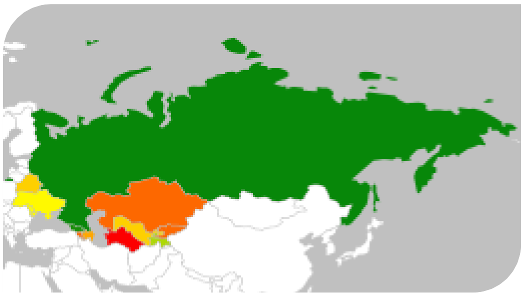


Figure 7.3.1: GCI Heat Map showing level of organizational commitment in the CIS region

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 to the element	Global % of the specified element
Strategy	6	4.55	2.94	64.62
Responsible agency	11	6.57	5.38	81.89
Cybersecurity Metrics	2	5.62	5.62	100.00

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 the CIS region, half of all countries have a dedicated strategy (Figure 6.3.2).

Many responding countries across the region noted the lack of metrics on cybersecurity incidents. This challenges countries to objectively assess incidents based on the evidence and determine if protection measures are working.

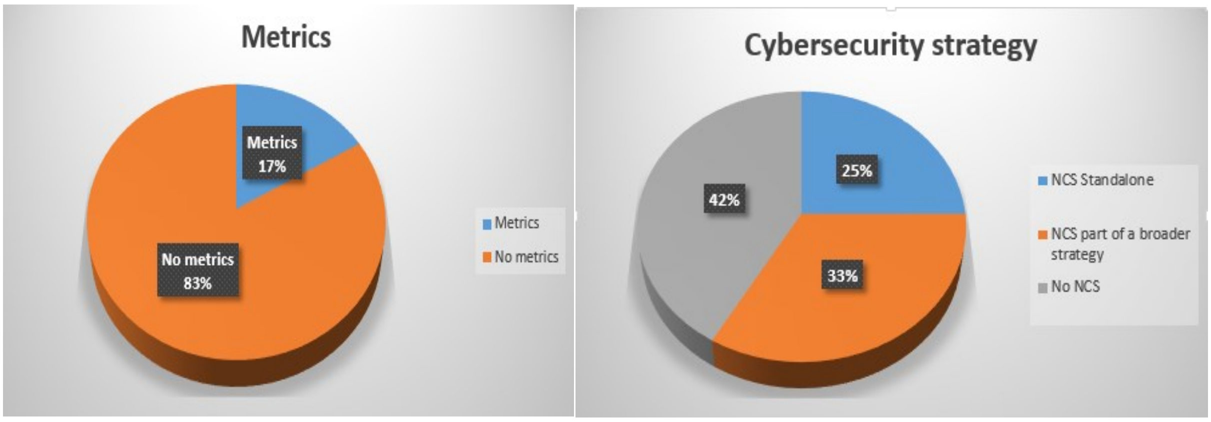


Figure 7.3.2: Cybersecurity strategy and training commitments

7.3.1 Strategy

Tajikistan has issued a Concept of Information Security in 2003. The document stresses the importance of information for economic, political, cultural and social development of the country, and the information sphere is designated as a pivotal factor of society. The Concept is widely used to determine many of the terms and mechanisms for providing security in the information sphere[16].

Ukraine adopted its National Cybersecurity Strategy in 2016 in response to the global and national cybersecurity challenges. The Strategy aims to create the conditions that ensure safe cyberspace and its use in the interests of individuals, the society and the Government[17].

7.3.2 Responsible agency

Georgia created LEPL Data Exchange Agency of Ministry of Justice, the main objective of which is developing E-governance. The Agency is committed to establish an infrastructure for data exchange for both public and private sectors and implement an information security policy[18]. Additionally CERT.GOV.GE operates under the Agency and is responsible for handling critical incidents that occur within Georgian

[16] http://nansmit.tj/20968-2/?id=15325

[17] http://zakon5.rada.gov.ua/laws/show/96/2016

[18] http://www.justice.gov.ge/Ministry/Index/390

Governmental Networks and critical infrastructure[19]. The Cyber Security Bureau, appointed by the Minister of Defence, is responsible for handling cyber security in the defense sector[20]. There is also a coordination body at national security level – the Council for State Security and Crisis Management, operating under the Prime Minister[21].

7.3.3 Cybersecurity metrics

Russia employs metrics annually in order to measure cybersecurity development at a national level, summarized in the National Standard of the Russian Federation[22]. The Standard contains recommendations for the development and use of measurements to assess the efficiency of implemented information security management system[23].

Armenia	0.167	Moldova	0.414
Azerbaijan	0.268	Russia	0.851
Belarus	0.334	Tajikistan	0.553
Georgia	0.821	Turkmenistan	0
Kazakhstan	0.167	Ukraine	0.399
Kyrgyzstan	0.167	Uzbekistan	0.334

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

[19] http://www.dea.gov.ge/?action=page&p_id=120&lang=eng

[20] http://csbd.gov.ge/bureau.php?lang=ge

[21] http://www.sscmc.gov.ge/ge

[22] http://docs.cntd.ru/document/gost-r-iso-27004-2011

[23] http://docs.cntd.ru/document/gost-r-iso-27004-2011

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, advancing already existing cybersecurity standards and institutional bodies, best practices guides, research, and education initiatives.

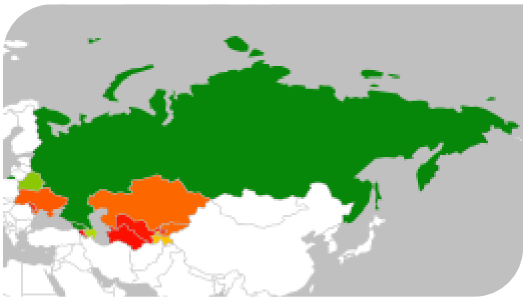


Figure 7.4.1: GCI Heat Map showing level of capacity building commitment in the CIS region

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
Standardization bodies	8	1.39	1.11	79.86
Good practices	6	3.03	3.03	100.00
R & D programmes	7	2.77	1.72	62.09
Public awareness campaigns	10	2.44	1.45	59.43
Professional training courses	7	2.50	1.72	68.80
National education programmes and academic curricula	8	2.67	1.40	52.43
Incentive mechanisms	3	2.20	1.83	83.18
Home-grown cybersecurity industry	3	1.91	1.62	84.82

Table 7.4.1: Global average in capacity building sub-pillars

Very few countries were able to provide data on the home-grown section, which demonstrates an exceptionally low response rate. In this regard, CIS countries are highly encouraged to support a home-grown industry and their civil society in building and developing start-ups and cybersecurity industry itself.

Over 70 per cent of countries reported the existence of bilateral and multilateral instruments due to the naturally important role of cooperation in cybersecurity matters.

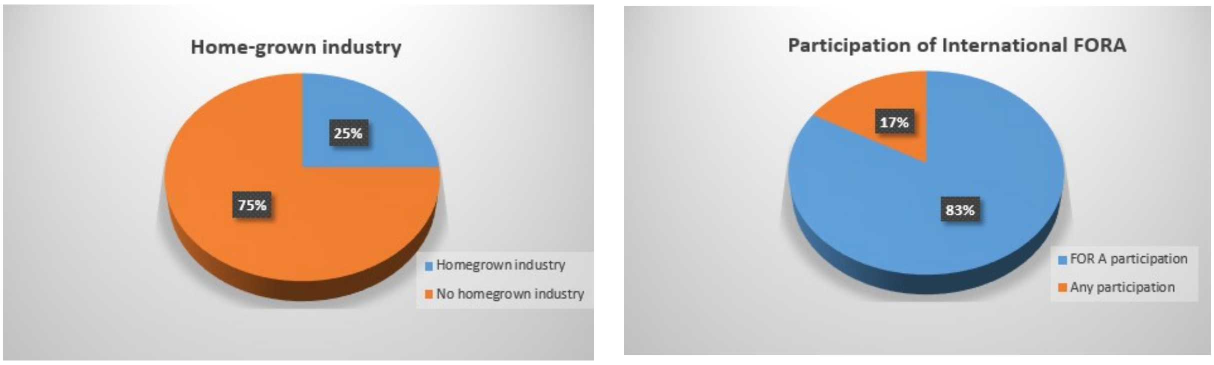


Figure 7.4.2: Home-grown industry and international participation

7.4.1 Standardization bodies

Ukraine adopted the Law of Ukraine[24] to establish legal and organizational principles of standardization and which aims at ensuring the formation and implementation of state policy in the relevant field.

7.4.2 Best practices

Kyrgyzstan possesses Standards on Information Security Institutions of the Banking System which focus on development and strengthening of national banking and payment systems through the necessary and sufficient level of information security[25].

7.4.3 Cybersecurity research and development programs

The Training Innovation Center in **Azerbaijan** organizes courses on various areas of information technology for business and organizations employees, as well as for ordinary citizens[26].

The **Belarusian** State University and the Tajik National University have a joint faculty in the field of computer science and computer security with a particular focus on information technology[27].

7.4.4 Cybersecurity professional training courses

The NATO-**Georgia** Professional Development Programme (PDP) hosts a training session on cybersecurity. The participants of the training are representatives from the Data Exchange Agency (DEA) and the State Security Service of Georgia. Its mission is to strengthen the incident handling methodologies in the country[28].

[24] http://zakon4.rada.gov.ua/laws/show/1315-18

[25] http://cbd.minjust.gov.kg/act/view/ru-ru/31410?cl=ru-ru

[26] http://ict.az/en/content/70

[27] http://news.tj/ru/news/belorusskii-i-tadzhikskii-universitet-otkroyut-sovmestnyi-fakultet-informatsionnykh-tekhnologii

[28] http://www.dea.gov.ge/?action=search&lang=eng

7.4.5 Incentive mechanisms

The Moscow School of Management SKOLKOVO has established the Information Cluster (ITC) to create an environment in **Russia** where new ITC projects may be developed and commercialized[29].

7.4.6 Home-grown cybersecurity industry

Kaspersky Lab is a **Russian** multinational cybersecurity and anti-virus provider with a range of services including security training and security awareness. The Kaspersky Global Research and Analysis Team (GReAT) produces annually the Global IT Security Risks Survey[30].

Armenia	0.077	Moldova	0.143
Azerbaijan	0.614	Russia	0.91
Belarus	0.679	Tajikistan	0.381
Georgia	0.898	Turkmenistan	0.1
Kazakhstan	0.239	Ukraine	0.217
Kyrgyzstan	0.239	Uzbekistan	0.113

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

[29] http://sk.ru/foundation/itc/f/192.aspx

[30] https://www.kaspersky.co.uk/

7.5 Cooperation

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

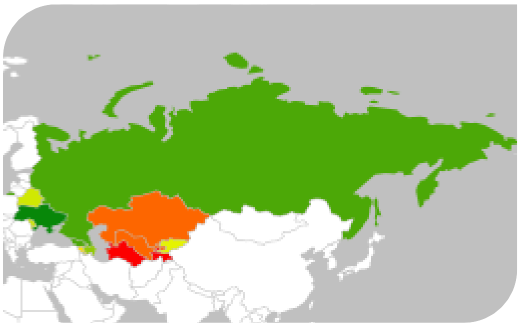
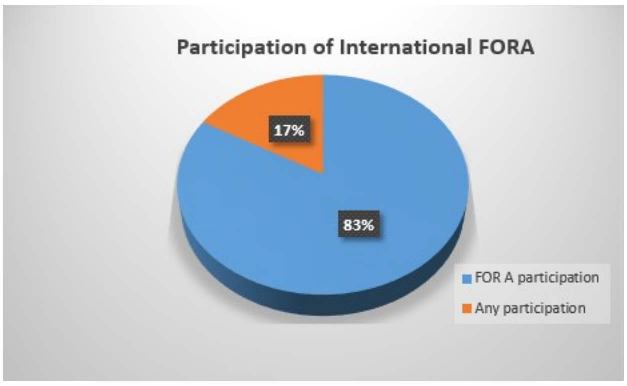


Figure 7.5.1: GCI Heat Map showing level of cooperation commitment in the CIS region

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
Intra-state Cooperation	7	1.64	1.26	76.83
Multilateral agreements	6	5.04	2.75	54.56
International fora participation	10	3.37	3.37	100.00
Public-Private Partnerships	4	4.82	4.16	86.31
Inter-agency partnerships	7	3.97	3.97	100.00

Table 7.5.1: Global average in cooperation sub-pillars

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. The scope of digital space is enormous. Therefore international cooperation is required to further facilitate management of cybersecurity systems and make the process durable.



Overall, the importance of cooperation in the CIS region is relatively high, 83% of responding countries report participation in International fora while only 17% do not have any bilateral agreements with other regional nations, nor multilateral or international mechanisms with more than two parties. The potential for cooperation is enhanced by participation in international cybersecurity events.

(**Figure 7.5.2: participation of International FORA)**

Georgia's CERT.GOV.GE is an active member of ITU, FIRST, TI and the Cybersecurity Executing Arm of the UN**.** As a result of productive cooperation with its foreign partners, CERT.GOV.GE has become a fully accredited member of the European CERT's Union in 2012. This acknowledgment confirms the important success achieved by CERT.GOV.GE on international level[31].

The Collective Security Treaty Organization (CSTO) was signed by **the Russian Federation, Armenia, Belarus, Kazakhstan, Kyrgyzstan** and **Tajikistan** to collaborate on the matter of international and regional security and stability including information technologies[32]. Another example is The Shanghai Cooperation Organization (SCO) that has become a valuable tool for enhancing cooperation in the field of international information security between China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan[33].

7.5.1 Participation in international fora

Participation in international cybersecurity events, workshops and training is the one indicator where almost all countries score high on the GCI. Most countries of the CIS region are members of the International Multilateral partnership Against Threats (IMPACT) [34] and participate in international fora organized by the International Telecommunication Union.

Government of **Azerbaijan** supports the NATO International School of Azerbaijan (NISA) which initiates biannual trainings and forums on international security issues**[35]**. Through collaboration with the Cybersecurity Alliance for Mutual Progress

[31] http://www.cert.gov.ge/?action=page&p_id=24&lang=eng

[32]https://tengrinews.kz/zakon/prezident_respubliki_kazahstan/mejdunapodnyie_otnosheniya_respubliki_kazahstan/id-U1400000982/

[33] https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf

[34] http://www.impact-alliance.org/home/index-countries.html

[35] http://www.nisa.az/?page_id=2299

(CAMP) Azerbaijan cooperates with other countries on ways to enhance their cybersecurity capacity[36].

7.5.2 Public -private partnerships

Tajikistan is willing to provide all kinds of assistance to enable capacity building for public-private partnership on the issue of ICT by carrying out regular special workshops and events[37].

7.5.3 Interagency partnerships

The development of the information society is one of the national priorities of the **Kyrgyz Republic.** The Council for Information-Communication Technologies (ICT Council) promotes public-private partnership in public administration reform and implementation of the "Electronic Government"[38]. The National Strategy, "Information and Communication Technologies for Development in the Kyrgyz Republic" sets out main priorities, objectives and tasks, main principles, provisions and directions of the national ICT policy[39].

Armenia	**0.344**	Moldova	**0.481**
Azerbaijan	**0.58**	Russia	**0.7**
Belarus	**0.474**	Tajikistan	**0**
Georgia	**0.7**	Turkmenistan	**0**
Kazakhstan	**0.158**	Ukraine	**0.818**
Kyrgyzstan	**0.437**	Uzbekistan	**0.158**

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

[36] https://www.cybersec-alliance.org/camp/membership.do

[37] http://www.gki.tj/ru/novosti/23/

[38] http://www.gov.kg/?page_id=27337&lang=ru

[39] http://cbd.minjust.gov.kg/act/view/ru-ru/97135?cl=ru-ru

8. Conclusion

The new generation of cybercriminals does 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 the internet all over the world, 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 state's security and how to protect businesses in a highly technological age.

Due to shifts in the CIS region influenced by rapid technical and economic progress, some challenges posed by cybercrime have emerged. Overall, there is a steady development of a cybersecurity culture, where almost all countries in this region have reached the level that allows a safe use of technologies.

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 welcomes all Member States and industry stakeholders in the CIS region to actively participate in future efforts to enhance the current reference model. A lack of common approach may largely challenge the quality of the GCI. Cooperation in cybercrime is important, and for this reason 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.

9. Annex 1 Abbreviations

CERT	**Computer Emergency Response Team**
CIRT	Computer Incident Response Team
CIIP	Critical Information Infrastructure Protection
CIS	Commonwealth of Independent States
CREST	Council of Registered Ethical Security Testers
CSIRT	Computer Security Incident Response Team
COP	Child Online Protection
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GOVCERT	Governmental Computer Emergency Response Team
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
ITU	International Telecommunication Union
ISP	Internet Service Provider
NCS	National Cybersecurity Strategy
UN	United Nations
R&D	Research and Development
PIPEDA	Personal Information Protection and Electronic Documents Act
ANSSI	National Agency for Information System Security
ISCB	Information Security Certification Body
NCSC	The National Cyber Security Centre
ISACA	Information Systems Audit and Control Association
ICP	Internet Content Provider
IASPs	Internet Access Service Provider
NCSC	Nation Cyber Security Centre
MSIP	Ministry of Science, ICT and Future Planning
IDI	ICT Development Index
GDP	Gross Domestic Product
FINCSIRT	Financial Sector Computer Security Incident Response Team

Annex 2: ITU CIS Member States Global Cybersecurity Commitment Score

Member State	Score	Rank	Regional ranking
Georgia	0.819	8	1
Russian Federation	0.788	10	2
Belarus	0.592	39	3
Azerbaijan	0.559	48	4
Ukraine	0.501	59	5
Moldova	0.418	73	6
Kazakhstan	0.352	83	7
Tajikistan	0.292	91	8
Uzbekistan	0.277	93	9
Kyrgyzstan	0.270	97	10
Armenia	0.196	111	11
Turkmenistan	0.133	132	12

Annex 3: List of Tables and Figures

Table

Table 3.2.1: GCI Tiers

Table 4.2.1: GCI Tiers stages

Table 4.3.2: Commitment of CIS region in figures

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

Table 6.1: Top three ranked countries in the CIS

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

Table 7.1.1: Global average in legal sub-pillars

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

Table 7.2.1: Global average in technical sub-pillars

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

Table 7.3.1: Global average in organizational sub-pillars

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

Table 7.5.1: Global average in cooperation sub-pillars

Table 7.4.2: Global average in capacity building pillar by countries in the CIS 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 CIS commitment

Figure 5.1.1: Global comparison GCI and IDI

Figure 5.1.2: GCI and IDI comparison in CIS region

Figure 5.1.3: CIS region scorecard

Figure 6.1: Average GCI score for each region

Figure 6.2: Top three ranked countries and an average score of all the CIS

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

Figure 7.1.2: Cybersecurity training commitments

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

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

Figure 7.3.2: Cybersecurity strategy and training commitments

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

Figure 7.5.2: Participation of International fora