Global Cybersecurity Index 2024

5th Edition



Global Cybersecurity Index 2024

5th Edition



Acknowledgements

The International Telecommunication Union (ITU) would like to thank the Global Cybersecurity Index (GCI) focal points, who have collected data on cybersecurity commitments from across their respective countries. This report would not have been possible without the GCI country focal points.

Particular acknowledgement is given to the members of the ITU GCI Expert Group for their work on improving the questionnaire, providing weighting recommendations and developing the tierbased model, notably Robin Almario, Hamza Bekhti, Alana G. Ramos, Fleur-de-lis A. Nadua, Na'ela Abanda, Aysha Ahmed BinHaji, Abdulla Mohammed Al Boinin, Dana Yousif Al-Abdulla, Noora Yousif Al-Abdulla, Alaidar Amirseiit, Abdulaziz Alfaiz, Ali Ali, Yusuf Mohamed Ali Mothanna, Ruaa AlJassar, Ghada Aljuhaiman, Wassim AlJuneidi, Ali Saeed Alkindi, Aziza Alrashdi, Siham Alrashdi, Aziza Sultan Al Rashdi, Mahran Alsheikh, Palakiyem Assih, Janelle Augustin-Henry, Anthony B Turner, Makarem Mohamed Bamatraf, Tarique Barkatullah, Mohamed Benziane, Wojciech Berezowski, Ahmad Amsyar bin Haji Ariffin, Katia Bonello, Yevhen Bryksin, Vladyslav Bublyk, Emmanuel J. Bwogi, Richard Calderón, Martin Camilleri, Wang Chunhui, Vanessa Copetti Cravo, Luc Dandurand, Daran Park, Aniel de Beer, Elena de la Calle, Miguel De Bruycker, Nangbam Didemana, Stefania Ducci, James Eaton-Lee, Aly Elshekh, Dai Fangfang, M. Rabenjamina Fenonirina Harinanadrianina, Christina Filipovic, Gabriela Gallegos, Carlos Leonardo Garcia, Marco Gercke, Henry Raul Gonzalez Brito, Boyan Grigorov, Alexander Grishchenko, Banchale Gufu, Ahmed Helmy, John Hering, René Andrade Hernández, Cristine Hoepers, Ella Holland, Fabián Iñiguez Matute, Tadas Jakštas, Michelet Jerome, Xiao Jing, Jacobo Bello Joya, Teemu Juujärvi, Dina Kabeel, Mustafa Kamal, Amos Kamugabirwe, Kadri Kaska, Nada Khater, Alan Khubaev, Bita Kiamehr, Elom Klevor, Fodé Kouyate, Igor Kovač, Anissa Kpakpabia, Rizky Hendra Kurniawan, Shadrack Ledwaba, Syntilla Likouni, Lim May-Ann, Charlotte Lindsey, Gosia Loj, Nicte Lopez, Iman Mahmoud, Indra Prasad Mainali, Tadesse Mak, Shafiq Malo, Mukesh Mangal, Dikokole Maqutu, Marcel Garcia Marcel Furtado Garcia, Louise Marie Hurel, Carlos Martins, Sametria McKinney, Tarik Babiker Merghani, Mhd Koudmani, Danylo Mialkovskyi, Molupe Molupe, James Musinguzi, Ngundi Vincent, Héctor Núñez, Doğukan Ömer Gür, Winston Oyadomari, Terrence Park, Nasim Parvez, Arseny Plossky, Nguyen Quy Quyen, Duha Rahahleh, Agria Rhamdhan, Andrea Rigoni, César Moliné Rodríquez, Eraste Rurangwa, Matej Šalmík, Abdelmalek Shafiee, Nizar Shanaah, Rajesh Sharma, Laurent Sliepe, Laura Striegel, Salman Sulaiman, Dr. Sulistyo, Samuel Tew, Marcelo Trindade Pitta, Kaleem Ahmed Usmani, Guillermo Valencia, Francisco Valle, Dinh Van Ket, Nia Wahyu Utami, Leon Wessels, Denys Yashchuk, Mariama Yormah, Heung Youl Youm, Ziad Zubidah, Hanibal Lemma, Simegnew Tizazu, Yirga Badma, Zekarias Getnet, Bruno Halopeau and Albtoul alMuhanna. In particular, we would like to thank Winston Oyadomari for his leadership of the discussion of the transition to a tier-based model.

Disclaimers

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the International Telecommunication Union (ITU) or of the ITU secretariat concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader.

The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of ITU or its membership.

ISBN

978-92-61-38751-8 (Electronic version) 978-92-61-38761-7 (EPUB version) 978-92-61-38771-6 (Mobi version)



Please consider the environment before printing this report.

© ITU 2024

Some rights reserved. This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO license (CC BY-NC-SA 3.0 IGO).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited. In any use of this work, there should be no suggestion that ITU endorse any specific organization, products or services. The unauthorized use of the ITU names or logos is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the International Telecommunication Union (ITU). ITU is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition". For more information, please visit https://creativecommons.org/licenses/by-nc-sa/3.0/igo/

Foreword



Over the past decade since the launch of the first Global Cybersecurity Index in 2015, 2.5 billion people have come online. The past 10 years have witnessed a significant evolution in the cybersecurity landscape, driven in part by the emergence of new technologies like artificial intelligence (AI), blockchain, and the potential of quantum computing. However, one constant remains: the human element. Cybersecurity efforts and the responsible use of digital technologies by individuals are paramount in shaping the future of this domain, and for working towards meaningful connectivity.

Recognizing the centrality of people, ITU Member States adopted the Kigali Action Plan in 2022 and highlighted the need for inclusive and secure telecommunications/ ICTs for sustainable development through supporting components like cybersecurity, in addition to digital literacy, strengthening the security of users online, assisting Member States with national cybersecurity strategies and computer incident response teams (CIRTs), digital skills and digital trainings, and secure infrastructure.

This edition of the Global Cybersecurity Index features record engagement by countries and is our most rigorous yet. Each country submission has been independently verified for accuracy, against consistent baselines and definitions. As a result, users of the Index can feel assured in its quality and applicability. Indeed, we have been encouraged to learn that Member States are incorporating GCI-based metrics into their national plans and activities.

The results of this edition of the GCI highlights significant improvements made by countries such as adding foundational legislation, establishing incident response efforts, developing clearer national plans, training people across society, and working together with national and international partners. In particular, many countries have been increasingly targeting their cybersecurity efforts toward vulnerable and underrepresented populations.

However, while the rise in cybersecurity initiatives is encouraging, a crucial next step for Member States lies in ensuring that these efforts are effective. Simply committing to action is not enough, we need to make sure that cyber commitments are implemented through high-quality, high-impact activities. In the future, we hope to support countries in enhancing the steps they have already been taking through the GCI.

This need is more important than ever, as this edition of the Global Cybersecurity Index shows, given that the gaps between Least Developed Countries (LDCs), Small Island Developing States (SIDS), Land Landlocked Developing Countries (LLDCs), and developed countries continues to persist. As countries work to bridge these gaps on their path towards meaningful connectivity, I hope that they work to draw on good practices, and to develop well-defined, relevant and applicable legal frameworks, set up technical teams in incidence response, to address lack of skilled talent, and to enhance collaboration, particularly around issues impacting vulnerable populations.

Furthermore, international cooperation emerges as an indispensable component in addressing the transnational nature of cyber threats. Collaborative endeavours facilitate the sharing of best practices, intelligence, and resources, strengthening the collective cyber resilience. However, to fully harness the benefits of international cooperation, it is imperative to support the development of requisite capacities to meaningfully engage in collaborative efforts. Building and fortifying national cybersecurity capabilities lays the groundwork for countries to actively contribute to global cybersecurity endeavours and navigate the complexities of cyberspace with confidence and competence.

The Global Cybersecurity Index is only part of the puzzle in improving countries' commitments to cybersecurity. I hope that countries find ways to use the Global Cybersecurity Index in their efforts to develop secure and trustworthy ICTs.

Dr Cosmas Luckyson Zavazava

18 / Helong

Director of the Telecommunication Development Bureau International Telecommunication Union

Table of contents

Acknowledgements	ii
Foreword	iv
Report summary	1
Introduction	3
Global view	5
Legal measures	6
Technical measures	8
Organizational measures	12
Capacity-development measures	17
Cooperation measures	20
Conclusion	23
Annexes	24
Tier performance: Global	24
Tier Performance: Africa	26
Tier Performance: Americas	27
Tier Performance: Arab States	27
Tier Performance: Asia and the Pacific	28
Tier Performance: CIS	28
Tier Performance: Europe	29
Country Profiles	30
Africa	30
Americas	52
Arab States	70
Asia and the Pacific	81
Commonwealth of Independent States	100
Europe	105
Methodology	128
Scope and objectives	128
Structure	128
Computational methodology	132
Key changes and limitations in the fifth edition of	the GCI134

GCI report development process	137
Areas for further research	138

List of figures and table

Figures

Figure 1: Tier performance, by region	1
Figure 2: GCI tier performance, by region (with counts)	5
Figure 3: ITU ICT Development Index (2024) as compared to the Global	
Cybersecurity Index	6
Figure 4: Legal measures, by region (one dot = one country)	6
Figure 5: Number of countries with regulations on personal data protection, privacy protection and/or breach notification	7
Figure 6: Technical measures, by region (one dot = one country)	8
Figure 7: Percentage of countries with a CIRT, by region/income group/	9
Figure 8: Percentage of countries with CIRTs and running cyber drills, by region/income group	
Figure 9: Countries with a sectoral CIRT, by region/income group/ development status	
Figure 10: Organizational measures, by region (one dot = one country)	
Figure 11: Overlap of having an NCS with an action plan and conducting national cybersecurity audits	. 14
Figure 12: Percentage of countries which have measures in force related to critical information infrastructure, by region	
Figure 13: Countries with national child online protection strategies, with associated current child online protection initiatives, by region	
Figure 14: Example child online protection initiative, offered by ITU with partners	
Figure 15: Capacity-development measures, by region (one dot = one country)	
Figure 16: Number of countries with targeted cyber-awareness campaigns beyond the general population, global	
Figure 17: Percentage of countries in region with curricula or training, at various stages of education, by region	. 19
Figure 18: Cooperation measures, by region (one dot = one country)	. 20
Figure 19: Percentage of regions part of any bilateral or multilateral agreement that addresses information-sharing or capacity development, by	
region	.21
Figure 20: Intersection of countries with a responsible agency and interagency collaboration (compared to the fourth edition of the GCI in 2021)	. 22

Figure 21: GCI evolution over time through a basic comparis editions	
Figure 22: Structure of the fifth edition of the GCI	
Figure 23: GCI report development process	137
Гable	
Table 1: Tier-based model	137

Report summary

The fifth edition of the Global Cybersecurity Index (GCI) measures the commitment of countries to cybersecurity in the context of measures across the following five pillars:



The GCI, launched in 2015 by the International Telecommunication Union, seeks to help countries to identify areas of improvement and encourage countries to act in building capacity and capabilities under each pillar. The GCI has been continuously adapted across editions to respond to changing risks, priorities and resources, in order to provide a more relevant snapshot of cybersecurity measures taken by countries.

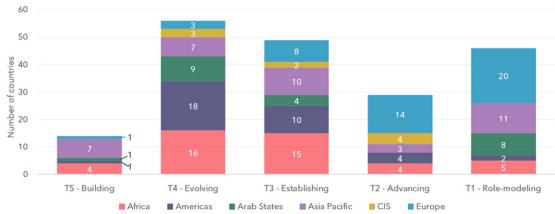
Countries measured	Collection years	Focal points from countries	Average overall score growth since 2020
194	2023-2024	172	27%
83 questions	20 indicators	5 pillars	Overall Score

Since 2021, countries have on average taken more cybersecurity-related actions and improved their commitments to cybersecurity. The global average country score has risen to 65.7/100.

Across the five GCI pillars, most countries are strongest in the legal pillar. By contrast, the average country is weakest in the capacity-development and technical pillars.

Each region has countries that are role-modelling or are advancing, and each region also has countries that are in the beginning stages of building their cybersecurity commitments. To capture these differences, country performance is measured across five tiers, with Tier 1 being the highest and Tier 5 the lowest. These tiers provide peer groups based on scores to help countries to understand and identify role models for improvement.

Figure 1: Tier performance, by region



Source: ITU

Key statistics by pillar



Legal

Measuring the laws and regulations on cybercrime and cybersecurity

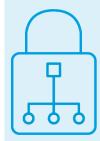
- 177 Countries had at least one regulation on either personal data protection, privacy protection, or breach notification in force or in progress.
- 151 Countries with data protection regulations in force
- 104 Countries with critical infrastructure regulations



Technical

Measuring the implementation of technical capabilities through national and sector-specific agencies

- 139 Countries with active CIRTs
- 83 Countries engaged with a regional CIRT association
- 110 Countries with frameworks to adopt cybersecurity standards



Organizational

Measuring national strategies and organizations implementing cybersecurity

- 132 Countries with national cybersecurity strategies
- 161 Countries with cybersecurity agencies
- 94 Countries with child online protection strategies and initiatives reported



Capacity development

Measuring awareness campaigns, training, education and incentives for cybersecurity capacity development

- 152 Countries conducting cyber-awareness initiatives
- 153 Countries with cybersecurity at some level of national curricula
- 99 Countries with cybersecurity capacity-development incentives



Cooperation

Measuring partnerships between agencies, firms and countries

- 108 Countries engaged or will be engaged in domestic or international cybersecurity public-private partnerships
- 166 Countries with international cybersecurity agreements
- 122 Countries reporting inter-agency collaboration

Introduction

Robust and coordinated cybersecurity efforts by countries have become more important since the previous edition of the Global Cybersecurity Index (GCI). With approximately 5.4 billion people online,¹ even offline populations are impacted by continued acceleration of technological developments with the adoption of artificial intelligence, renewed efforts towards digitalization and widespread advances toward universal and meaningful connectivity.²

Cybersecurity issues have become more prominent, owing inter alia to:

- 1) **Increased ransomware**: growing reports of ransomware attacks targeting government services and other critical sectors in many countries.³
- 2) **Breaches affecting core industries**: the scale, frequency and intensity of cybersecurity incidents or breaches affecting individuals and various sectors including education, manufacturing, energy and IT services, to name but a few.
- 3) **Privacy concerns**: data breaches resulted in European data protection authorities issuing General Data Protection Regulation (GDPR) fines worth over EUR 1.9 billion in 2023,⁴ with total GDPR fines issued since 2018 estimated to be currently worth more than EUR 4.5 billion.⁵
- 4) **Cost to businesses**: the global average cost of a data breach was estimated at USD 4.45 million in 2023.
- 5) **Outages**: information technology disruptions affecting the integrity and availability of systems, services and supply chains.⁶

It has been 35 years since the first International Telecommunication Union (ITU) cybersecurity standard, Recommendation ITU-T X.509, and a decade since the launch of the first GCI. During this time, ITU has worked with over 140 different Member States on their cybersecurity readiness, as cybersecurity has firmly emerged as a strategic imperative for governments, as well as for critical and non-critical sectors of society. Measuring the efforts towards improving cybersecurity has become a crucial touchstone for governments in driving development in the area. The GCI sits at the nexus of cybersecurity metrics, by assessing the measures taken by countries at the national level to improve their cybersecurity commitments. Based on the five work areas established in the 2008 Global Cybersecurity Agenda, i.e. legal measures, technical and procedural measures, organizational structures, capacity building and international cooperation, the GCI scores complement output-based measurements, such as number of cyberattacks and extent of vulnerabilities, among others. By contrasting the efforts taken by countries with cybersecurity outputs, countries, companies and civil society organizations can identify whether existing efforts need to be revisited or strengthened, how to prioritize future interventions, and how to begin to evaluate the effectiveness of these measures.

https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

² Measuring digital development - ICT Development Index 2024, https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-3/

https://www.fortinet.com/resources/cyberglossary/ransomware-statistics

European Data Protection Board, Annual Report 2023, https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2023 en

⁵ <u>https://www.enforcementtracker.com/?insights</u>

⁶ CrowdStrike disruption in July 2024: https://www.wired.com/story/microsoft-windows-outage-crowdstrike.global-it-probems/; https://www.bloomberg.com/news/articles/2024-07-19/microsoft-cloud-service-issues-disrupt-air-travel-operations

The fifth edition of the GCI explores the current level of cybersecurity commitment among 193 Member States and the State of Palestine and the progress made since the last edition. The GCI report examines the implications of the results for governments and policy-makers as they navigate national and regional circumstances, as well as global developments, while planning cybersecurity measures and initiatives. One of the key changes made in this edition is a shift from ranking countries to using a five-level tier for viewing countries' cybersecurity commitments. This tier-based perspective allows for greater focus on the extent of advances in cybersecurity commitments and what this may mean for countries. Moreover, given the nature of the cybersecurity landscape, there is always room for growth, refinement and adaptation regardless of a country's GCI score. While a score of 100/ 100 reflects a strong cybersecurity commitment, it does not mean further work is not required in terms of adopting appropriate cybersecurity measures in response to countries' shifting operating environments and the evolving cybersecurity ecosystem.

The GCI is used by countries, investment groups, development organizations, companies and other actors as an important tool in understanding cybersecurity commitments for several reasons, including:

- Comprehensive evidence-based cybersecurity measures: the GCI takes a multidimensional approach to cybersecurity and relies on either publicly available data or verifiable evidence provided by countries. This approach leads to a trustworthy, more reliable view of cybersecurity commitments. As a result, countries have come to rely on the GCI to inform their national cybersecurity plans.
- **Informing national policies:** countries can better understand their progress in key areas of cybersecurity and identify opportunities for further developments and innovations aligned with their national priorities and situational contexts.
- **Fostering research and development:** the cybersecurity landscape's dynamism necessitates proactive responses that include the identification or collection of data and the investigation and development of relevant cybersecurity artefacts, including new policies, laws and regulations, products and standards, among others.
- **Benchmarking:** countries can assess their level of cybersecurity commitment and progress over time against global and regional averages.
- **Enhancing cooperation:** with cooperation being a central part of good cybersecurity measures, opportunities for various levels of cooperation can be found and leveraged to support mutual strategic, operational and tactical cybersecurity responses.

To help countries consider their cybersecurity commitments considering the above issues, this edition of the GCI aims to be the most robust yet. It features greater clarity and refinement in questions, greater efforts to ensure consistency in verification and validation, while maintaining high-quality analysis. However, the GCI should be used with consideration for its limitations as it does not measure the quality of actions; it only assesses whether they are in place, partially in place/in progress or do not exist. ITU, in collaboration with the GCI Expert Group, will continue actively to seek ways of improving the relevance, rigour and validity of the indicators relied on and to better communicate results.

Global view

Overall, the fifth edition of the GCI presents many countries working to improve their cybersecurity commitments through implementing relevant measures across the five pillars: legal, technical, organizational, capacity development and cooperation. To give a more accurate view of the clusters of performance within the GCI, the GCI has shifted to a tier-based presentation of country scores, using score ranges set by the GCI Expert Group. (For more information on the tiers and their development, see section *Tiers*.)

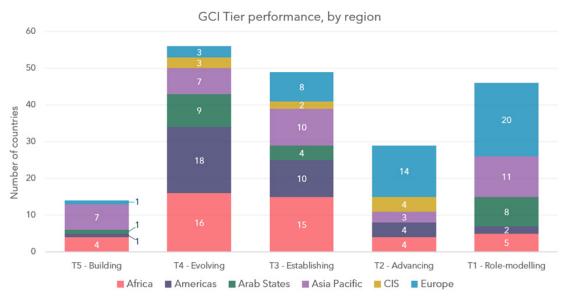


Figure 2: GCI tier performance, by region (with counts)

Source: ITU

Almost every region has high and low performing countries. This edition of the GCI has placed 46 countries in Tier 1 (T1), the highest tier. If the tier-based system had been applied to the fourth edition of the GCI⁷, 30 countries would have been placed in T1. Much of the movement to T1 comes from countries in Europe, Asia and the Pacific, the Arab States and Africa. These countries made significant improvements across the five GCI pillars since the last edition.

Most countries (105) were placed in T3 and T4, representing the many countries that have been expanding digital services and bringing people online but still have work to do to ensure that cybersecurity becomes part of their meaningful connectivity objectives.

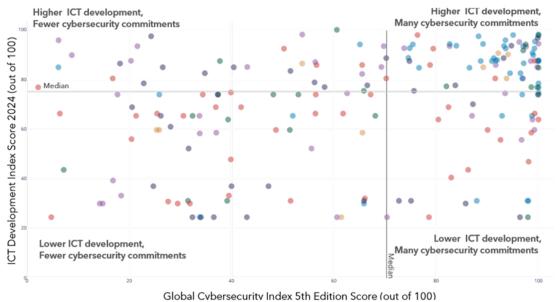
Many of these countries also have a significant cyber-capacity gap: they are looking to enhance their cybersecurity but face resource limitations in terms of staffing, access to equipment and sustainable funding.

When comparing GCI scores against general information and communication technology (ICT) development, it should be noted that the scores do not necessarily trend in line with the ITU ICT Development Index (IDI), which measures universal connectivity and meaningful connectivity. There are many countries that are active on cybersecurity but still have a lower level of overall ICT development, meaning that they are well positioned to create a safe and trustworthy cyberspace as people come online. Inversely, there are many countries which perform above the IDI median

https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

score but lack many cybersecurity measures. While these countries may have prioritized initial ICT development over integrating cybersecurity as they contend with limited resources, they risk a more insecure and less resilient cyberspace for people already online.

Figure 3: ITU ICT Development Index (2024) as compared to the Global Cybersecurity Index



Source: ITU

Legal measures

Legal measures tend to be countries' strongest area of cybersecurity, but more still needs to be done.

Figure 4: Legal measures, by region (one dot = one country)



Source: ITU

Legal measures continue to be countries' strongest pillar on average. More countries have implemented legal measures designating and clarifying cybersecurity-related concerns, from

data protection to illegal online activities. There is evidence of increased harmonization among these laws and regulations, at least in terms of nomenclatures, such as aligning with GDPR or international cybercrime treaties. More countries are also adding or updating measures framed with technology-neutral language, creating increased flexibility in interpretation, and alignment between online and offline offences or obligations.

Efforts are still needed to ensure the specificity and application of laws and regulations. For example, some countries have ambiguities in breach notification requirements and their applications.

Privacy laws and regulations are increasing, and increasingly needed.

Figure 5: Number of countries with regulations on personal data protection, privacy protection and/or breach notification



Source: ITU

With 8 billion records being breached in 2023 across over 2 800 reported breaches, the average cost of a data breach has increased by 15 per cent over the past three years. These incidents can be costly: for small businesses in North America alone, the average breach is estimated to cost USD 3.3 million. Countries also risk users losing trust in ICTs due to these breaches. To provide recourse and rights for users as well as clear expectations for organizations handling data, countries have implemented regulations on personal data protection, privacy protection and/or breach notification.

The previous edition of the GCI noted that GDPR and similar legislation had driven an increase in the number of countries which had adopted privacy legislation and breach notification requirements. While the trend has begun to level out, more countries have also worked to ensure comparability between privacy regimes.

However, many countries can further clarify their privacy, data protection and breach notification laws and regulations. For example, not all countries have clearly defined what is the expected notification period for breaches, or the mandate of competent authorities to monitor and respond to breaches. In addition, these efforts can be complemented by capacity development, to ensure that relevant actors are well trained and aware of current cybersecurity threats.

⁸ https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

https://www.ibm.com/reports/data-breach

https://www.ibm.com/reports/data-breach

Technical measures

The data show a high disparity in implementation of technical measures as a means of supporting cybersecurity efforts at the national level.

20 To the search of the search

Figure 6: Technical measures, by region (one dot = one country)

Source: ITU

Together with legal measures, technology plays a pivotal role as a line of defence against malicious online actors. Robust cybersecurity mechanisms require a combination of competent individuals, well-documented processes and procedures, and technology. These elements prepare and empower countries to prevent, protect and respond effectively to cybersecurity incidents.

Activities to detect, prevent, respond to and mitigate cyberthreats and incidents take place in a variety of structures such as computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and Computer Emergency Response Teams (CERTs). Security operation centres (SOCs) and information-sharing and analysis centres (ISACs) can also perform some or all of these activities.

The relation between CIRTs and other agencies, particularly national cybersecurity coordination centres (NCCCs) or national cybersecurity authorities (NCAs), varies significantly between countries. While many countries have a national CIRT responsible for, *inter alia*, cyber-awareness activities, data collection and standards implementation, numerous NCCCs and NCAs have taken on these duties.

CIRTs are not only domestic focal points on incident response, they also serve as important international nodes to connect transnational cybersecurity incident response efforts. Events like regional and international cyber -drills can be important in this regard, as national CIRTs can interact with peers and establish informal and formal connections.

Moreover, participation in international fora, such as the Forum of Incident Response and Security Teams (FIRST), as well as regional fora, such as the Asia Pacific Computer Emergency Response Team (APCERT), the Pacific Cyber Security Operational Network (PaCSON), AfricaCERT, the European Union Cyber Security Agency (ENISA), the Organisation of Islamic Cooperation and the Organization of American States, is of paramount importance for CIRTs, as it provides a

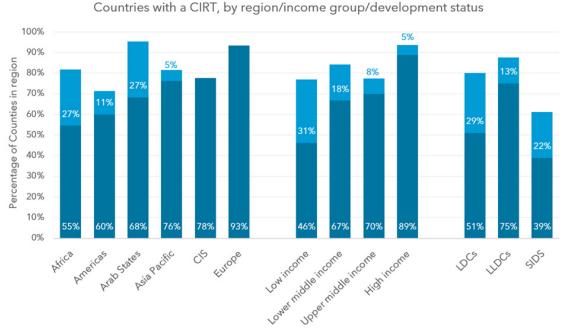
platform for knowledge-sharing, collaboration and capacity development among cybersecurity professionals worldwide. Some 98 countries reported being part of FIRST or listed TF-CSIRT, with six in the process of joining, while 115 reported being part of regional CIRT organizations.

Standards also figure among best practices for implementation under the technical pillar. As standards undergo rigorous evaluation by experts, they can provide clear roadmaps on how to structure cybersecurity initiatives, teams and technologies. With a proliferation of relevant standards and qualifications, 110 countries had some sort of framework in place for the implementation of cybersecurity standards.

Standards can also help to bridge certain fundamental security gaps that still persist. Globally, between 14 per cent and 35 per cent of regions' mail services are not using secure sockets layer/transport layer security (SSL/TLS) protocols or ciphers, or are using insecure or weak ones. ¹¹ Between only 1 per cent and 4.6 per cent of mail services use the recommended implementation of SSL/TLS, with the rest using some sort of secure protocol.

CIRTs are playing a key role in the cybersecurity ecosystem.

Figure 7: Percentage of countries with a CIRT, by region/income group/development status



Source: ITU

CIRTs, CSIRTs, CERTs, SOCs, ISACs and other teams monitor threats and help to respond in the event of a cybersecurity incident. With an estimated 68 per cent of organizations suffering a cyberattack in 2023, ¹² CIRTs have become more important than ever. Based on current data, 139 countries have a national CIRT, while 55 do not have a CIRT or national CIRT in progress.

Dreamlab Technologies research data on SSL/TLS implementation for mail protocols (SMTPS, POP3S, IMAPS), November 2023.

https://www.netwrix.com/2023 hybrid_security_trends_report.html

Beyond their immediate function of incident response, CIRTs serve as a catalyst for broader engagement within organizations, fostering a culture of cybersecurity awareness and resilience. By conducting coordinated responses to cyber-incidents, CIRTs not only mitigate immediate risks but also lay the groundwork for proactive security measures and continuous improvement in organizational cybersecurity posture. For example, CIRTs can monitor and drive implementation of best practices, such as Domain Name System Security Extensions (DNSSEC) and security vulnerability disclosure.

For example, to ensure that the domain name system (DNS) is safe and authenticates responses to domain name lookups, only 0.43 per cent of African providers have implemented DNSSEC, compared to a higher adoption rate of 13.13 per cent in the Commonwealth of Independent States (CIS) region. Regions with high numbers of Internet users, such as Asia and the Pacific, only have a 1.52 per cent adoption of DNSSEC, versus 11.28 per cent in Europe.¹³

CIRTs can also drive security disclosures. For example, websites can adopt security.txt, ¹⁴ which includes key contact information in the event of a vulnerability discovery, as well as relevant policies and acknowledgements. Currently, this is underused globally, with less than 0.7 per cent of sites using this mechanism. ¹⁵

The presence of a CIRT is most likely in high-income countries (globally, 89 per cent of such countries have a national CIRT), with upper-middle and lower-middle income countries less likely (70 per cent and 67 per cent, respectively). Some 46 per cent of lower-income countries had an operational national CIRT as of 2024.

The ability to respond to an incident varies based on the country's investment, local capacity and overall organization.

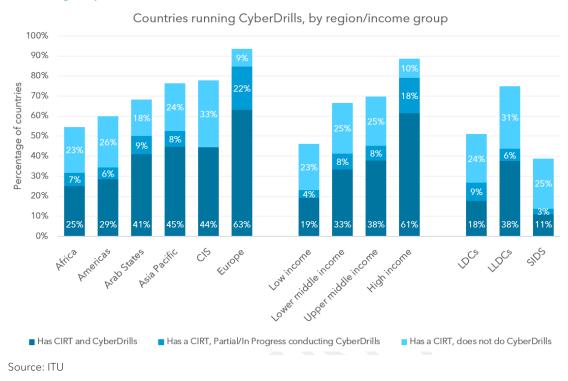
To enhance preparedness and capabilities, CIRTs, as well as cybersecurity authorities, are increasingly running cybersecurity simulation exercises (cyber drills) among stakeholders. While 140 countries participated in regional cyber drills organized by ITU in 2023, running national cyber drills remains important to engage domestic stakeholders in hands-on exercises. National cyber drills can engage a wider set of domestic actors than regional or international cyber drills do and can be better tailored to the national context.

¹³ Dreamlab Technologies research data on global DNSSEC implementation, November 2023

¹⁴ RFC9116. Note that other mechanisms may be used by organizations.

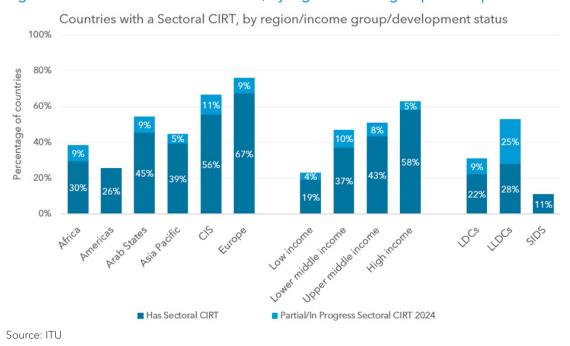
Dreamlab Technologies research data on adoption of security.txt for vulnerability disclosure, January 2023.

Figure 8: Percentage of countries with CIRTs and running cyber drills, by region/income group



Sectoral CIRTs are being implemented to address specific sectoral needs.

Figure 9: Countries with a sectoral CIRT, by region/income group/development status



While some countries choose to rely on national CIRTs to support all sectors, sectoral CIRTs also have an important role to play. Specific sectors of industry face different threats and have different incident-response needs depending on whether they are part of critical infrastructure and on their supply chain, etc. For example, 25.7 per cent of all cyberattacks in 2023 targeted

the manufacturing sector; of those attacks, 45 per cent used malware and 17 per cent used ransomware. By contrast 18.2 per cent of all cyberattacks targeted the finance and insurance sectors, with 38 per cent of the attacks using malware and 25 per cent using ransomware. Sectoral CIRTs can be better positioned than national CIRTs to respond to a particular sector's profile in terms of the technologies used, specific vulnerabilities and remediation needs in the event of an attack.

As was the case in the fourth edition of the GCI, sectoral CIRTs are less common than national CIRTs. A number of countries participate in regional sectoral CIRTs, such as regional financial CIRTs, which allow for the leveraging of joint resources with other countries to tackle common issues.

Not all countries have the capacity and resources to implement sectoral CIRTs. For them, as well as countries with sectoral CIRTs, prioritization is key to ensure that relevant sectors receive the tailored support needed to manage cybersecurity risks. Low-income countries and small island developing States in particular are less likely to have sectoral CIRTs, as many have focused their efforts on the process of developing, or enhancing, their national CIRT. As these countries' ICT infrastructure continues to develop, addressing the cybersecurity needs of sectors can be met domestically or through regional CIRTs.

Organizational measures

Greater coordination and alignment are necessary for shaping more data-driven and inclusive national cybersecurity efforts.

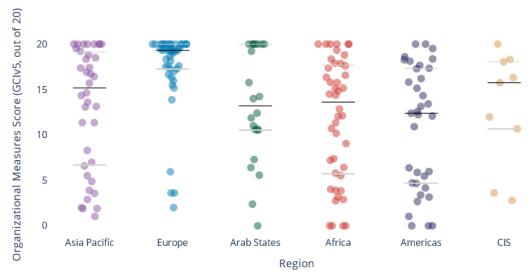


Figure 10: Organizational measures, by region (one dot = one country)

Source: ITU

Organizational measures are necessary for the proper implementation of a national cybersecurity posture and help to guide effective implementation. Many countries have made strides in ensuring that there are clear strategic objectives, with a comprehensive plan in implementation, delivery and measurement. Without a well-defined organizational network of partners, working together across industry, civil society and academia efforts in different sectors and industries

https://www.ibm.com/downloads/cas/L0GKXDWJ

become disparate and unconnected, thwarting efforts towards national harmonization in cybersecurity development.

National cybersecurity strategies are a primary tool towards developing an effective organizational framework. Beyond national cybersecurity strategies, countries have also been working to develop clear metrics and measures to understand how to track outputs of cybersecurity at the national level, and track in-depth inputs of cybersecurity such as audits. Translating these metrics to policy and implementation requires clear roles and responsibilities, as well as responsive organizational frameworks.

More countries have a national cybersecurity strategy.

National cybersecurity strategies (NCSs) have become an increasingly common tool for governments to organize around cybersecurity. As of 2024, 132 countries have an NCS, up from 107 in 2020. Much of this progress can be attributed to the Africa region, where nine countries have ushered in their first NCS. In addition, many countries have worked to revise and update their existing strategies.

The breadth and depth of NCSs vary considerably. The second edition of the Guide to Developing a National Cybersecurity Strategy recommends several key areas for countries to consider incorporating into their NCSs. Only 85 out of the 132 countries with an NCS include the following measures:

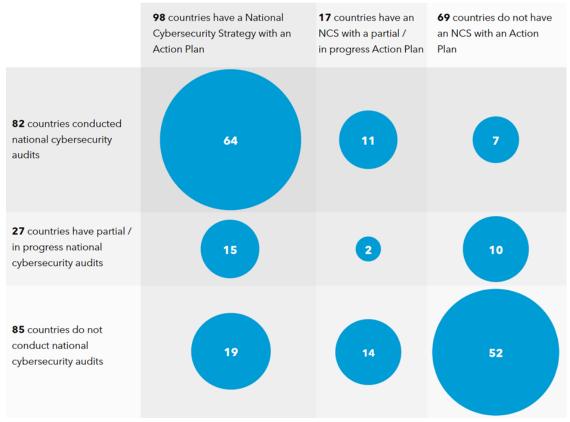
- cybersecurity of critical infrastructure;
- lifecycle management principles;
- stakeholder engagement; and
- an action plan.

The quality of each of these measures can also be addressed. Countries most often implement practices like stakeholder engagement and lifecycle management at the beginning or end of their NCS, instead of integrating these concepts through the NCS lifecycle. As a result, they miss out on valuable feedback related to the NCS, opportunities to ensure that domestic stakeholders are aligned on key priorities and the chance to adapt where necessary to help to ensure that the NCS remains relevant and effective over time.

For example, some countries leveraged their action plans to ensure that best practices and recommended activities were implemented, and used lessons learned from the action plan to update and revise their NCS.

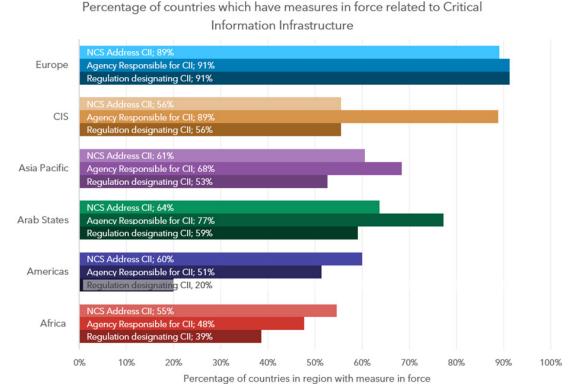
Having an action plan does not guarantee that all best practices are prioritized or incorporated. For example, cybersecurity audits are a commonly accepted best practice to assess and analyse organizations' cybersecurity and cyber-risks. Yet many countries do not have them in their action plan. As shown in Figure 11, while there are 64 countries that have an NCS with an action plan and have carried out national cybersecurity audits, 19 countries with an NCS and an action plan did not do national cybersecurity audits.

Figure 11: Overlap of having an NCS with an action plan and conducting national cybersecurity audits



Critical information infrastructure efforts often lack supporting legal measures.

Figure 12: Percentage of countries which have measures in force related to critical information infrastructure, by region



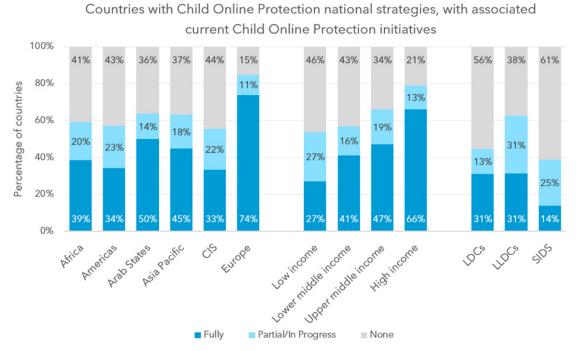
Critical information infrastructure (CII) is tackled in the GCI through questions under the legal, technical, organizational and capacity-development pillars. Developing a synergistic CII ecosystem involves addressing all these pillars in concert and ensuring that the measures reflect current threats and vulnerabilities. Considering the questions on CII under the legal and organizational pillars, the most common feature is to have an agency responsible for CII cybersecurity.

With 54 per cent of countries globally having an agency, ministry or other entity bearing responsibility for CII cybersecurity, only 49 per cent of countries globally have such a framework in place, or being put in place, to implement cybersecurity standards in relation to CII.

To ensure that professionals working on CII, such as those in the telecommunication or energy sectors, are well prepared to manage cybersecurity risks and respond to incidents, training is important. Some 90 per cent of countries with an NCS that addresses CII and with a responsible agency have conducted sector-specific training for cybersecurity professionals.

Implementation of child online protection strategies and initiatives remains limited.

Figure 13: Countries with national child online protection strategies, with associated current child online protection initiatives, by region



It is estimated that every half a second, a child goes online for the first time.¹⁷ In addition, the 2023 Child Online Safety Index (COSI) found that nearly 70 per cent of children and adolescents aged 8-18 years old worldwide have experienced at least one cyber-risk incident in the past year.¹⁸ With this in mind, child online protection has long been a building block for collaboration between law enforcement, policy-makers, educators, parents, advocates and other stakeholders. To coordinate these stakeholders' efforts, child online protection strategies with associated initiatives are needed.

In this edition, 164 countries reported having legal measures on child online protection, compared to 130 countries in the previous edition of the GCI.¹⁹ These measures were sometimes part of other rules and regulations, such as on online crime or sexual exploitation. Despite most countries having laws and regulations on child online protection, only 94 countries globally have strategies with associated current child online protection initiatives in place. Activities included awareness-raising campaigns, training for educators, training for police, and reporting mechanisms, among others. These activities are targeting a wide range of ages, as not only young children are at risk.

https://www.unicef.org/protection/violence-against-children-online

https://www.dqinstitute.org/child-online-safety/

https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Askme
Your online safety friend

www.itu.int/cop/askme

In collaboration with:

Unicef® THE CYBER TRUST

In Collaboration Protection

Figure 14: Example child online protection initiative, offered by ITU with partners

As children continue to come online, they need to be both protected and empowered in order to become active participants in creating a safe and trustworthy cyberspace. For this to happen, parents, teachers, policy-makers, law enforcement, public sector actors and other stakeholders need to be able to support children and youth in their digital journeys and need to understand the risks and challenges facing children online.

Capacity-development measures

Cybersecurity training and awareness efforts vary across regions against the backdrop of efforts to develop a strong industry.

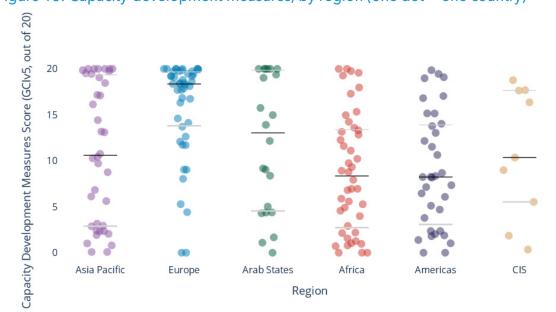


Figure 15: Capacity-development measures, by region (one dot = one country)

Source: ITU

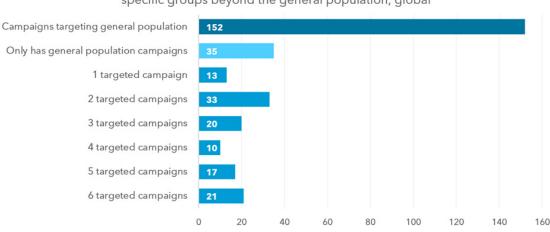
Capacity development is key to building a robust cybersecurity ecosystem. Countries risk eroding progress that has been made in enhancing full and universal connectivity if they do not support cybersecurity skills and awareness-raising. Over 95 per cent of countries have some activity under the capacity-development pillar, with the most activities reported in the awareness-raising campaign category.

Efforts to develop a domestic cybersecurity industry were also present in many countries, taking the form of incentive mechanisms, such as grants and scholarships, and organizations acting to promote the cybersecurity industry. Such initiatives can increase the level of cybersecurity in a country beyond the level that may have developed without government support.

Research and development (R&D) was also tracked as part of efforts to develop domestic capacity. Some 127 countries reported some form of R&D, whether through the private sector, public sector or academia, with academia being the most common centre for R&D.

Countries are increasingly targeting specific demographics as part of cyber-awareness campaigns.

Figure 16: Number of countries with targeted cyber-awareness campaigns beyond the general population, global



Number of countries with targeted cyber awareness campaigns targeting specific groups beyond the general population, global

Source: ITU

Creating a culture of cybersecurity is an ongoing challenge for all countries. Awareness-raising campaigns, which seek to inform users and change behaviours, are developed or supported, with 152 countries reporting having a cybersecurity awareness-raising campaign aimed at the general public. In addition, 130 countries had some form of targeted cyber-awareness campaign carried out or planned, with 52 per cent of those targeting four or more different demographic groups. Some 20 countries reported upcoming, planned or in-progress targeted cybersecurity awareness campaigns.

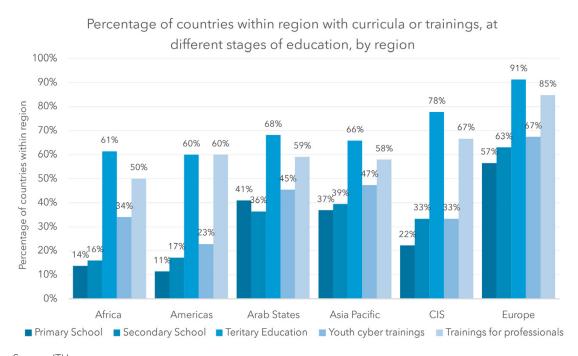
Number of countries

Targeted awareness-raising campaigns serve as vital tools in identifying specific threats and educating individuals and organizations about cybersecurity threats and best practices. The effectiveness of such campaigns, however, often hinges on the metrics used to track impact, particularly when the campaigns are primarily conducted on social media platforms. While social media offer extensive reach and engagement potential, relying solely on metrics such as likes, shares and comments may not accurately gauge the campaigns' true efficacy

in raising awareness and changing behaviour. Instead, there is a growing recognition of the need for human-centred approaches that resonate with people's realities and address their specific concerns and challenges in navigating the digital landscape securely. This requires the tailoring of awareness-raising campaigns to diverse audiences, considering factors such as cultural context, digital literacy levels and socio-economic backgrounds. By adopting a more nuanced approach that prioritizes meaningful engagement and behavioural outcomes over superficial metrics, organizations can ensure that their awareness campaigns effectively empower individuals to protect themselves against cyberthreats and contribute to building a safer online environment for all.

Many countries still lack cybersecurity skill development programmes across educational levels.

Figure 17: Percentage of countries in region with curricula or training, at various stages of education, by region



Source: ITU

While the cybersecurity workforce grew 8.7 per cent from 2022 to 2023, the gap between the workers needed and the number available has also grown, by 12.6 per cent.²⁰ To address this gap, countries are increasingly seeking to develop cybersecurity skills within their population by incorporating cybersecurity into school curricula at the primary (61 countries) and secondary (68 countries) levels, as well as in university-level courses and programmes (137 countries).

Beyond formal schooling, countries are offering training programmes that target youth (85 countries) and cybersecurity professionals (123 countries).

To ensure that a domestic cybersecurity industry can flourish, countries can work to ensure that the variety of educational opportunities available at different ages sufficiently prepare students and professionals for their careers.

https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity Workforce Study 2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

Cooperation measures

Operationalization and impact of agreements and frameworks remains a challenge.

OOO Asia Pacific Europe Arab States Africa Americas CIS
Region

Figure 18: Cooperation measures, by region (one dot = one country)

Source: ITU

Cybersecurity is a complex, interconnected challenge necessitating a holistic, multistakeholder approach. Given its transnational character, effective response demands cooperation across public, private and government sectors. The past decades have been characterized by a variety of efforts to build international cooperation and coordination, including the Budapest Convention on Cybercrime, which entered into force in 2004; the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which came into effect in 2023; and the Commonwealth of Independent States Agreement on Cooperation in the Fight Against Crimes in the Field of Information Technologies (Dushanbe Agreement), which came into force in 2020. In addition, cybersecurity efforts have increased in the context of many other international, regional and sectoral agreements around cybersecurity. Still, many countries are not part of these agreements, whether due to conflict, lack of human resourcing or unclear benefits.

On the domestic front, working with the private sector offers governments a chance to leverage private sector insights and expertise to improve cybersecurity. Almost 63 per cent of countries reported having inter-agency processes for cybersecurity within their governments. However, collaboration is less common with the private sector, with less than half of countries reported being part of public-private partnerships (PPPs) with domestic or foreign companies.

The test of success of these agreements, partnerships and processes will be whether they move beyond paper and promote action. By fostering information sharing, capacity building and joint threat assessment, the international community can more effectively address the evolving cyberlandscape, including the increasing intersection of cybersecurity and artificial intelligence.

Many countries are part of international cybersecurity agreements.

Figure 19: Percentage of regions part of any bilateral or multilateral agreement that addresses information-sharing or capacity development, by region

Percentage of regions that part of any bilateral or multilateral agreement that

addresses information sharing or capacity development, by region cybersecurity capacity development; 98% Europe rsecurity information sharing; 98% cybersecurity capacity development; 100% cybersecurity capacity development; 84% Asia Pacific rsecurity information sharing; 87% cybersecurity capacity development; 77% **Arab States** security information sharing; 77% cybersecurity capacity development; 91% Americas bersecurity information sharing; 94% ersecurity capacity development; 95% Africa curity information sharing; 93% 0% 10% 20% 60% 70% 80% 90% 100% 50%

Source: ITU

In verifying data for this edition of the GCI, many countries were found to be party to, or in the process of becoming party to, international agreements of which their focal points were not aware. Policing was a common area in the development of cybersecurity agreements, often done with organizations such as INTERPOL, or regional organizations. The types of agreements related to cybersecurity and their specifics varied significantly; some countries used general agreements to form a basis for further projects and implementation related to cybersecurity capacity development and information-sharing, while other countries developed more specific agreements from the start.

Percentage of Countries

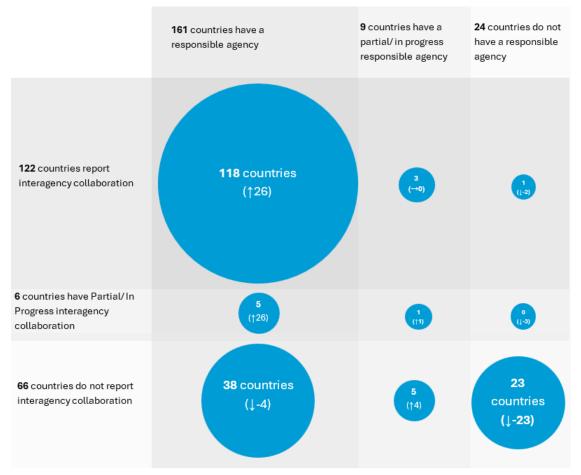
Building domestic collaboration remains an area for improvement.

Cybersecurity is more than simply a hardware or software issue: coordination between capable domestic actors is an important component for coherent commitments. Effective coordination requires the clear identification of roles and responsibilities: the second edition of the Guide to Developing a National Cybersecurity Strategy recommends that countries should ensure that all stakeholders, including various government agencies, ministries and entities, the private sector and civil society, involved in cybersecurity "should have a clear understanding of their respective roles and responsibilities."²¹

In 2020, 136 countries had an agency designated as responsible for cybersecurity at the national level, 95 reported having inter-agency cooperation, and 92 were found to have both. By this edition of the GCI, 161 countries had an agency designated as responsible for cybersecurity at the national level, 122 reported having inter-agency cooperation, and 118 reported having both. This upward trend is encouraging as responsible agencies can help to drive more cohesive and collaborative approaches to cybersecurity.

https://ncsquide.org/the-quide/principles/

Figure 20: Intersection of countries with a responsible agency and inter-agency collaboration (compared to the fourth edition of the GCI in 2021)



Conclusion

There has been much improvement since the previous edition of the Global Cybersecurity Index (GCI). Still, more needs to be done to meet the evolving digital threat landscape. Cyberattacks are perceived to be the fifth most likely risk to present a material crisis on a global scale in 2024.²² Recent global technical outages demonstrated the world's dependency on the digital infrastructure and the need for resilience. If countries want to benefit from the promise of information and communication technologies (ICTs), they need to think about cybersecurity.

Across the GCI and its legal, technical, organizational, capacity-development and cooperation pillars, countries need to carefully prioritize high-impact activities in their efforts, rather than surface-level documents or campaigns. Countries may want to consider efforts to:

- implement legal measures that can be clearly and fairly applied across all sectors;
- foster cross-functional efforts that address more than just information technology;
- maintain well-trained and responsive national institutions, including computer incident response teams;
- engage a wide range of stakeholders across all cybersecurity initiatives;
- develop and regularly update the national cybersecurity strategy with an implementable action plan;
- implement effective child online protection measures;
- address cybersecurity challenges faced by critical infrastructure;
- run cyber-awareness campaigns that address relevant issues;
- provide training opportunities for cybersecurity professionals, critical infrastructure actors and youth in order to build and enhance cybersecurity skills;
- create incentive mechanisms to encourage cybersecurity capacity development and research and development; and
- foster domestic and international cooperation and collaboration in information-sharing and capacity development.

Cybersecurity is continuing to evolve. For countries working to achieve cybersecure meaningful connectivity, the GCI offers a clear picture of where they are and a roadmap of activities to make progress. Countries must, however, be willing to engage in the ongoing processes of enhancing cybersecurity and working to enhance the quality and impact of their activities. The GCI will continue to capture countries' work and progress as they strive to meet future challenges and bring meaningful connectivity to all.

https://www.weforum.org/publications/global-risks-report-2024/digest/

Annexes

Tier performance: Global

Tier 1 - Role-modelling (score of 95-100)

Australia Ghana Singapore Bahrain Greece Netherlands (Kingdom Slovenia Iceland Bangladesh of the) Spain India Belgium Norway Sweden Brazil Indonesia Oman Tanzania Pakistan Thailand Cyprus Italy Denmark Japan Portugal Türkiye Egypt Jordan Qatar United Arab Emirates Estonia Korea (Republic of) United Kingdom Kenya Finland **United States** Luxembourg Rwanda France Saudi Arabia Viet Nam Malaysia Germany Mauritius Serbia

Tier 2 - Advancing (score of 85-95)

Albania Ecuador Mexico Switzerland Austria Georgia **Philippines** Togo Azerbaijan Hungary Poland Uruguay Ireland Romania Uzbekistan Benin Russian Federation Zambia Canada Israel China Kazakhstan Slovakia Croatia Lithuania South Africa

Tier 3 - Establishing (score of 55-85)

Malta

Czech Republic

Algeria Cuba Libya Papua New Guinea Andorra Dem. Rep. of the Congo Malawi Paraguay Belarus Dominican Rep. Moldova Peru Bhutan Eswatini Monaco Senegal Botswana Ethiopia Mongolia Sierra Leone Brunei Darussalam Gambia Montenegro Trinidad and Tobago Bulgaria Guinea Mozambique Tunisia Burkina Faso Iran (Islamic Republic of) Myanmar Uganda

Sri Lanka

(continued)

Cameroon Jamaica Nepal (Republic of) Ukraine
Chile Kiribati New Zealand Vanuatu

Colombia Kuwait Nigeria

Costa Rica Kyrgyzstan North Macedonia

Côte d'Ivoire Latvia Panama

Tier 4 - Evolving (score of 20-55)

AngolaDominicaLiechtensteinSeychellesArgentinaEl SalvadorMadagascarSomalia

Armenia Equatorial Guinea Mali South Sudan

Bahamas Fiji Mauritania State of Palestine

Barbados Gabon Namibia Sudan
Belize Grenada Nauru Suriname

Bolivia (Plurinational Guatemala Nicaragua Syrian Arab Republic

State of) Guyana Niger Tajikistan Bosnia and Herzegovina Haiti Saint Kitts and Nevis Tonga

Cabo Verde Honduras Saint Lucia Turkmenistan

CambodiaIraqSaint Vincent andTuvaluChadLao P.D.R.the GrenadinesVenezuelaComorosLebanonSamoaZimbabwe

Congo (Rep. of the) Lesotho San Marino

Djibouti Liberia Sao Tome and Principe

Tier 5 - Building (score of 0-20)

Afghanistan Dem. People's Rep. of Maldives Timor-Leste
Antigua and Barbuda Korea Marshall Islands Vatican

Burundi Eritrea Micronesia Yemen

Central African Rep. Guinea-Bissau Solomon Islands

Tier Performance: Africa

T5	T4	T3	T2	T1
Building	Evolving	Establishing	Advancing	Role-modelling
Burundi Central African Rep. Eritrea Guinea-Bissau	Angola Cabo Verde Chad Congo (Rep. of the) Equatorial Guinea Gabon Lesotho Liberia Madagascar Mali Namibia Niger Sao Tome and Principe Seychelles South Sudan Zimbabwe	Botswana Burkina Faso Cameroon Côte d'Ivoire Dem. Rep. of the Congo Eswatini Ethiopia Gambia Guinea Malawi Mozambique Nigeria Senegal Sierra Leone Uganda	Benin South Africa Togo Zambia	Ghana Kenya Mauritius Rwanda Tanzania

Tier Performance: Americas

T5	T4	T3	T2	T1
Building	Evolving	Establishing	Advancing	Role-modelling
Antigua and Barbuda	Argentina Bahamas Barbados Belize Bolivia (Plurinational State of) Dominica El Salvador Grenada Guatemala Guyana Haiti Honduras Nicaragua Saint Kitts and Nevis Saint Lucia Saint Vincent and the Grenadines Suriname Venezuela	Chile Colombia Costa Rica Cuba Dominican Rep. Jamaica Panama Paraguay Peru Trinidad and Tobago	Canada Ecuador Mexico Uruguay	Brazil United States

Tier Performance: Arab States

T5 Building	T4 Evolving	T3 Establishing	T2 Advancing	T1 Role-modelling
Yemen	Comoros	Algeria	(none)	Bahrain
	Djibouti	Kuwait		Egypt
	Iraq	Libya		Jordan
	Lebanon	Tunisia		Morocco
	Mauritania			Oman
	Somalia			Qatar
	State of Palestine			Saudi Arabia
	Sudan			United Arab Emir-
	Syrian Arab Republic			ates

Tier Performance: Asia and the Pacific

T5 Building	T4 Evolving	T3 Establishing	T2 Advancing	T1 Role-modelling
Afghanistan	Cambodia	Bhutan	China	Australia
Dem. People's Rep. of	Fiji	Brunei Darussalam	Philippines	Bangladesh
Korea	Lao P.D.R.	Iran (Islamic	Sri Lanka	India
Maldives	Nauru	Republic of)		Indonesia
Marshall Islands	Samoa	Kiribati		Japan
Micronesia	Tonga	Mongolia		Malaysia
Solomon Islands	Tuvalu	Myanmar		Pakistan
Timor-Leste		Nepal (Republic of)		Republic of
		New Zealand		Korea
		Papua New Guinea		Singapore
		Vanuatu		Thailand
				Viet Nam

Tier Performance: CIS

T5	T4	T3	T2	T1
Building	Evolving	Establishing	Advancing	Role-modelling
(none)	Armenia Tajikistan Turkmenistan	Belarus Kyrgyzstan	Azerbaijan Kazakhstan Russian Feder- ation Uzbekistan	(none)

Tier Performance: Europe

T5 Building	T4 Evolving	T3 Establishing	T2 Advancing	T1 <i>Role-modelling</i>
Vatican	Bosnia and Herzegovina Liechtenstein San Marino	Andorra Bulgaria Latvia Moldova Monaco Montenegro North Macedonia Ukraine	Albania Austria Croatia Czech Republic Georgia Hungary Ireland Israel Lithuania Malta Poland Romania Slovakia Switzerland	Belgium Cyprus Denmark Estonia Finland France Germany Greece Iceland Italy Luxembourg Netherlands (Kingdom of the) Norway Portugal Serbia Slovenia Spain Sweden Türkiye United Kingdom

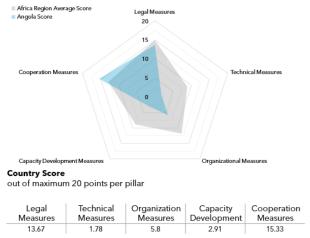
Country Profiles

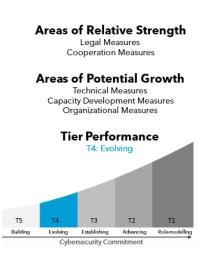
Africa

Angola

Angola

GCI 5th Edition CountryPerformance



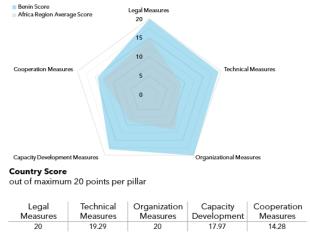


Benin

Benin

GCI 5th Edition CountryPerformance

Areas of Relative Strength

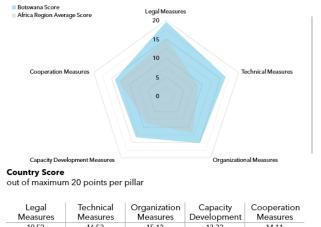




Botswana

Botswana

GCI 5th Edition CountryPerformance



19.52 16.53 15.12 13.32 14.11



Burkina Faso

Burkina Faso

Burkina Faso
Africa Region Average Score Legal Measures 20 10 Cooperation Measures Technical Measures Organizational Measures Capacity Development Measures **Country Score** out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
14.18	12.7	15.16	11.61	16.58

*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Burundi

Burundi

GCI 5th Edition CountryPerformance



9.9 1.03 5.84

*Countries are classified according to www.itu.int



Cabo Verde

Cabo Verde

 Africa Region Average Score
 Cabo Verde Score Legal Measures 15 10 Cooperation Measures Technical Measures Capacity Development Measures **Country Score** out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
17.36	7.92	12.05	2.19	12.02

*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Т3

Establishing

T2

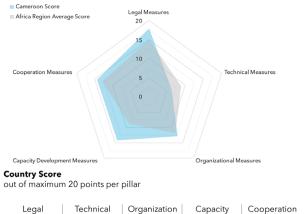
Advancing

T5

Cameroon

Cameroon





Legal
MeasuresTechnical
MeasuresOrganization
MeasuresCapacity
DevelopmentCooperation
Measures17.926.1812.8614.2414.33

*Countries are classified according to www.itu.int



Central African Republic

Central African Republic

 Africa Region Average Score
 Central African Republic Score Legal Measures 20 15 Cooperation Measures Technical Measures Capacity Development Measures Organizational Measures **Country Score** out of maximum 20 points per pillar Legal Organization Capacity Cooperation Development Measures Measures 4.76 Measures Measures 0

*Countries are classified according to www.itu.int

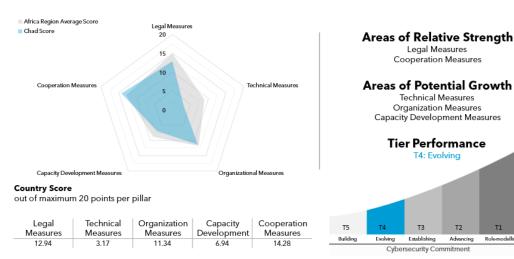
GCI 5th Edition CountryPerformance



Chad

Chad

GCI 5th Edition CountryPerformance



*Countries are classified according to www.itu.int

Congo (Republic of the)

Congo (Republic of the)



*Countries are classified according to www.itu.int

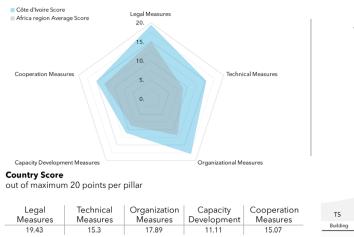
GCI 5th Edition CountryPerformance



Côte d'Ivoire

Côte d'Ivoire

GCI 5th Edition CountryPerformance



*Countries are classified according to www.itu.int

Areas of Relative Strength Legal Measures Organization Measures Areas of Potential Growth Technical Measures Capacity Development Measures Cooperation Measures Tier Performance T4: Evolving

Cybersecurity Commitment

Democratic Republic of the Congo

Democratic Republic of the Congo

Africa Region Average Score
Democratic Republic of the Congo Score

Legal Measures
20

15

10

Cooperation Measures
5
0

Capacity Development
Measures
Organizational Measures

Country Score out of maximum 20 points per pillar

Legal
MeasuresTechnical
MeasuresOrganization
MeasuresCapacity
DevelopmentCooperation
Measures17.285.4514.518.9210.45

*Countries are classified according to www.ltu.int

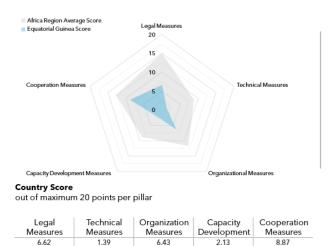
GCI 5th Edition CountryPerformance



Cybersecurity Commitment

Equatorial Guinea

Equatorial Guinea



*Countries are classified according to www.itu.ini

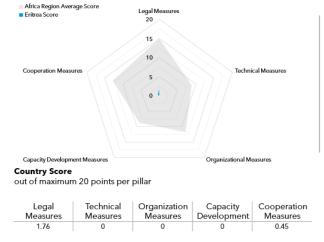
GCI 5th Edition CountryPerformance



Cybersecurity Commitment

Eritrea

Eritrea



*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Eswatini

Eswatini

GCI 5th Edition CountryPerformance



 Legal Measures
 Technical Measures
 Organization Measures
 Capacity Development
 Cooperation Measures

 18.2
 14.96
 18.36
 10.21
 17.7

*Countries are classified according to www.itu.int



Ethiopia

Ethiopia

Ethiopia Score
Africa Region Average Score
Legal Measures
20
15
10
Cooperation Measures
5
0
Capacity Development Measures
Capacity Score

Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
18.83	14.37	12.12	15.33	15.69

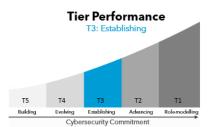
*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance

Areas of Relative Strength Legal Measures Capacity Development Measures Cooperation Measures

Areas of Potential Growth

Technical Measures Organization Measures



Gabon

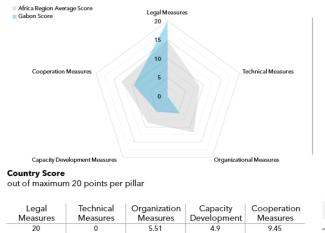
Gabon

GCI 5th Edition CountryPerformance

Area of Relative Strength Legal Measures

Areas of Potential Growth

Capacity Development Measures Technical Measures Cooperation Measures Organization Measures **Tier Performance** T4: Evolving



T5 Establishing Advancing Cybersecurity Commitment

*Countries are classified according to www.itu.int

Gambia

Gambia

Africa Region Average Score 15 Cooperation Measures Technical Measures Organizational Measures **Country Score**

out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
	10.01	45.77		40.45
14.77	10.34	15.77	8.77	12.15

*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance

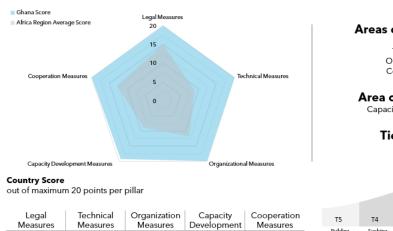
T2



Ghana

Ghana

GCI 5th Edition CountryPerformance



19.27

20

20

Areas of Relative Strength Legal Measures Technical Measures Organization Measures Cooperation Measures **Area of Potential Growth** Capacity Development Measures **Tier Performance** T1: Role-modelling

T3

Building

Establishing

Cybersecurity Commitment

T2

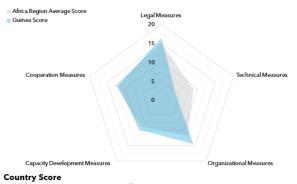
Advancing

Guinea

Guinea

20

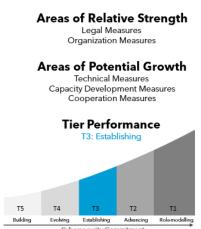
GCI 5th Edition CountryPerformance



20

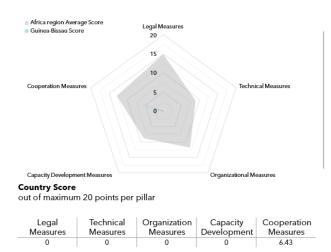
out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
16.27	3.98	14.38	9.74	12.02



Guinea-Bissau

Guinea-Bissau



*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Cybersecurity Commitment

Kenya

Kenya

■ Kenya Score
■ Africa Region Average Score Legal M 20 15 10 **Country Score** out of maximum 20 points per pillar Legal Technical Organization Capacity Cooperation Measures Development Measures Measures Measures 19.52 19.07 20 20 20

*Countries are classified according to www.itu.int

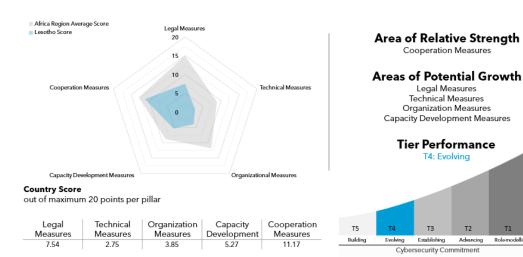
GCI 5th Edition CountryPerformance



Lesotho

Lesotho

GCI 5th Edition CountryPerformance



Liberia

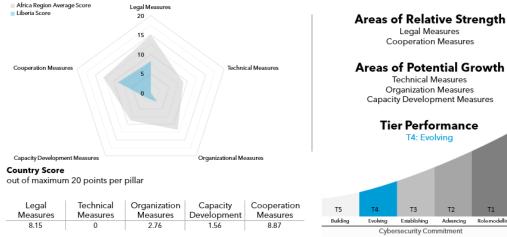
Liberia

GCI 5th Edition CountryPerformance

T2

Advancing

Role-modelling



^{*}Countries are classified according to www.itu.int



Madagascar

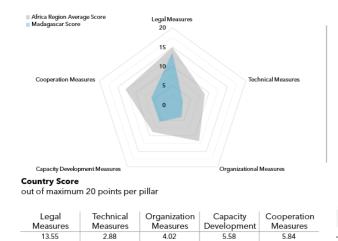
Madagascar

GCI 5th Edition CountryPerformance

Area of Relative Strength Legal Measures

Areas of Potential Growth

Technical Measures Organization Measures
Capacity Development Measures
Cooperation Measures





Malawi

Malawi





*Countries are classified according to www.itu.int

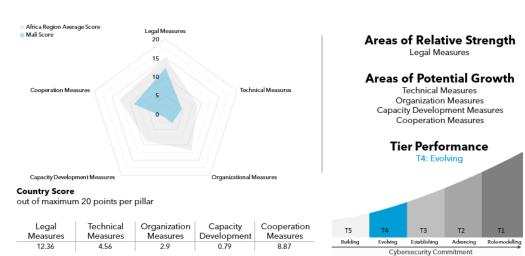
GCI 5th Edition CountryPerformance



Mali

Mali

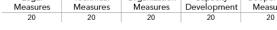
GCI 5th Edition CountryPerformance



Mauritius

Mauritius

Mauritius Score
Africa Region Average Score 15 10 Technical Measures Capacity Developm Measures Organizational Measures Country Score out of maximum 20 points per pillar Legal Organization Capacity Cooperation Development Measures Measures Measures



*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Cybersecurity Commitment

Cooperation

16,58

Mozambique

Mozambique

 Mozambique Score
 Africa Region Average Score Legal Measures 15 10 Technical Measures Capacity Development Measures Organizational Measures **Country Score** out of maximum 20 points per pillar Capacity Development

Organization

Measures

7.93

15.79

Technical

11.83

GCI 5th Edition CountryPerformance



Namibia

Namibia

Legal

13.92

 Africa Region Average Score
 Namibia Score Legal Mea 20 15 Cooperation Measures Technical Measures Capacity Development Measures **Country Score** out of maximum 20 points per pillar Legal Technical Capacity Organization Cooperation Development Measures Measures Measures Measures 3.54 5.66 16.35 4.57 6.81

*Countries are classified according to www.itu.int

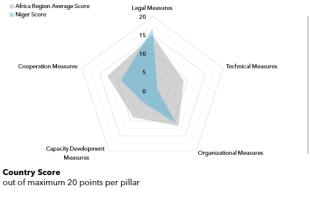
GCI 5th Edition CountryPerformance



Niger

Niger

GCI 5th Edition CountryPerformance



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
16.78	1.39	10.72	3.98	

Area of Relative Strength Legal Measures **Areas of Potential Growth** Technical Measures Organizational Measures Capacity Development Measures Cooperation Measures **Tier Performance** T4: Evolving T5 T3 T2 Role-modelling lving Establishing Advancing Cybersecurity Commitment Building Advancing

Nigeria

Nigeria

Nigeria Score
Africa Region Average Score 10 Technical Measures Cooperation Measures

Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
19.52	18.88	16.57	13.15	14.28

*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance

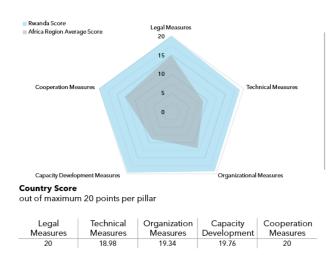


lving Establishing Advancing
Cybersecurity Commitment

Rolemodelling

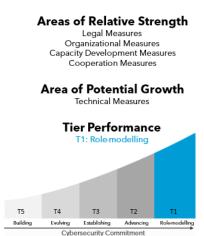
Rwanda

Rwanda



*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Sao Tome and Principe

Sao Tome and Principe

 Africa Region Average Score
 Sao Tome and Principe Score Legal Measures Cooperation Measures Technical Measures Capacity Development Measures **Country Score** out of maximum 20 points per pillar Legal Technical Organization Capacity Cooperation Development Measures Measures Measures Measures 9.83 1.39 3.17 0.96 5.09

*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Senegal

Senegal

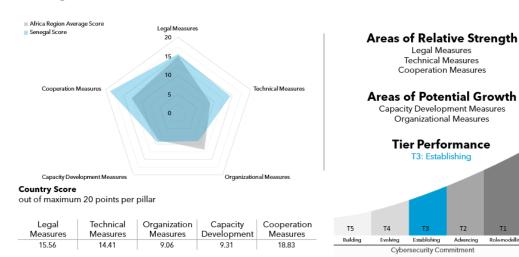
GCI 5th Edition CountryPerformance

T3: Establishing

T2

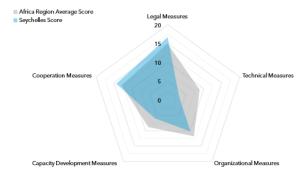
Advancing

Role-modelling



Seychelles

Seychelles



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
16.75	3.17	10.18	5.88	14.28

*Countries are classified according to www.itu.int

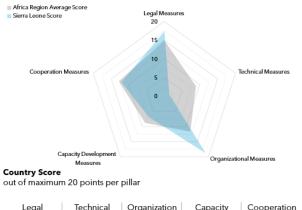
GCI 5th Edition CountryPerformance



Sierra Leone

Sierra Leone

GCI 5th Edition CountryPerformance



Legal
MeasuresTechnical
MeasuresOrganization
MeasuresCapacity
DevelopmentCooperation
Measures17.291.3918.816.9512.02

*Countries are classified according to www.itu.int



South Africa

South Africa



*Countries are classified according to www.itu.int

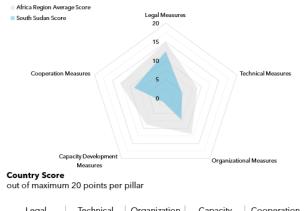
GCI 5th Edition CountryPerformance



South Sudan

South Sudan

GCI 5th Edition CountryPerformance



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
12.47	4.56	7.21	1.27	8.87

Area of Relative Strength Legal Measures **Areas of Potential Growth** Technical Measures Capacity Development Measures Cooperation Measures Organizational Measures **Tier Performance**

T3 T2 Building Establishing Advancing Cybersecurity Commitment

T5

Tanzania

Tanzania

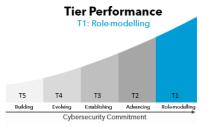
Tanzania Score
Africa Region Average Score Legal Measures 20 15 10 Technical Measures **Country Score** out of maximum 20 points per pillar

Legal Organization Capacity Cooperation Development Measures Measures Measures Measures 20 19.69 20 19.57 20

GCI 5th Edition CountryPerformance

Areas of Relative Strength Legal Measures Cooperation Measures Organizational Measures

Areas of Potential Growth Technical Measures Capacity Development Measures



^{*}Countries are classified according to www.itu.int

Togo

Togo

GCI 5th Edition CountryPerformance



Legal MeasuresTechnical MeasuresOrganization MeasuresCapacity DevelopmentCooperation Measures2015.317.8817.2918.33

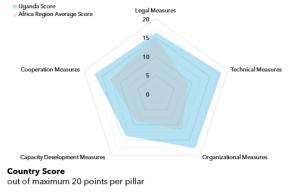
*Countries are classified according to www.itu.ini



Uganda

Uganda

GCI 5th Edition CountryPerformance



 Legal Measures
 Technical Measures
 Organization Measures
 Capacity Development
 Cooperation Measures

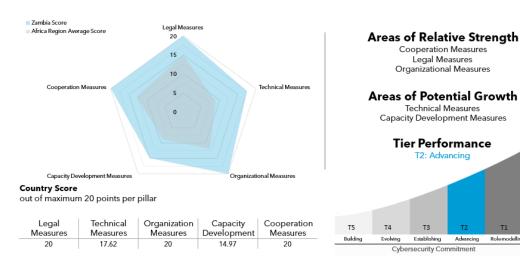
 16.41
 18.21
 17.61
 13.59
 17.12



Zambia

Zambia

GCI 5th Edition CountryPerformance



Zimbabwe

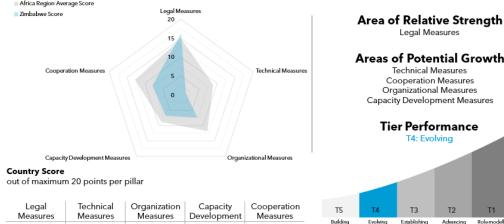
Zimbabwe

GCI 5th Edition CountryPerformance

Legal Measures

Advancing

Role-modelling



6.81

7.97

7.38

*Countries are classified according to www.itu.int

1.39

16.3



Americas

Antigua and Barbuda

Antigua and Barbuda

GCI 5th Edition Country Performance



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
11.84	0	0	2.36	

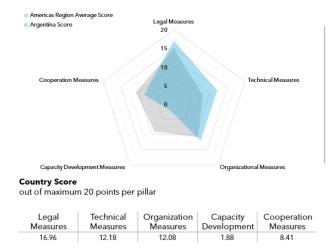
^{*}Countries are classified according to www.itu.int



Argentina

Argentina

GCI 5^{th} Edition Country Performance



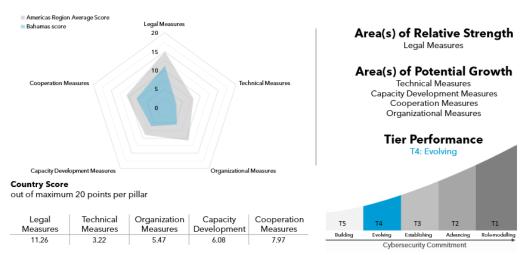
*Countries are classified according to $\underline{www.itu.int}$



Bahamas

Bahamas

GCI 5th Edition Country Performance

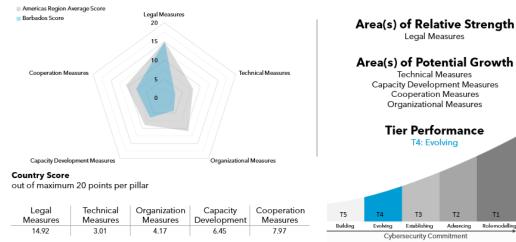


^{*}Countries are classified according to www.itu.in

Barbados

Barbados

GCI 5th Edition Country Performance

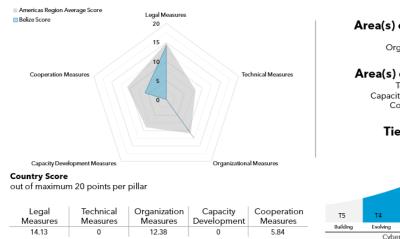


^{*}Countries are classified according to www.itu.int

Belize

Belize

GCI 5th Edition Country Performance





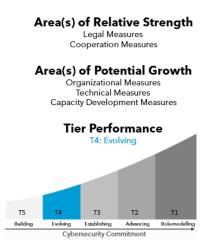
Bolivia (Plurinational State of)

Bolivia (Plurinational State of)

GCI 5th Edition Country Performance



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
13.7	6.18	4.65	8.23	



Brazil

Brazil

GCI 5th Edition Country Performance



 Legal Measures
 Technical Measures
 Organization Measures
 Capacity Development
 Cooperation Measures

 20
 20
 17.29
 19.09
 20

*Countries are classified according to www.itu.int

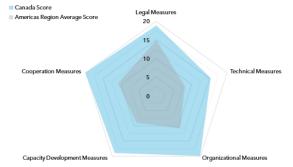
Area(s) of Relative Strength Legal Measures Cooperation Measures Technical Measures Capacity Development Measures Area(s) of Potential Growth Organizational Measures Tier Performance T1: Role-modelling

Cybersecurity Commitment

Canada

Canada

GCI 5th Edition Country Performance



Country Score

out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures	
18.9	15.3	20	18.98	20	



Chile

Chile

GCI 5th Edition Country Performance



 Measures
 Measures
 Measures
 Development
 Measures

 14.69
 13.81
 13.41
 11.52
 16.8

*Countries are classified according to www.itu.int



Colombia

Colombia

GCI 5th Edition Country Performance



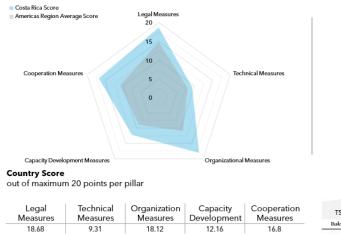
*Countries are classified according to www.itu.int



Costa Rica

Costa Rica

GCI 5th Edition Country Performance



*Countries are classified according to www.ltu.int

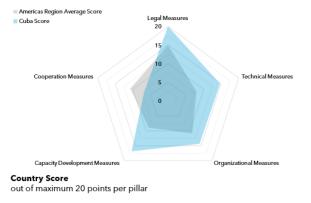
Area(s) of Relative Strength Legal Measures Organizational Measures Cooperation Measures Area(s) of Potential Growth Technical Measures Capacity Development Measures Tier Performance T3: Establishing

Cybersecurity Commitment

Cuba

Cuba

GCI 5th Edition Country Performance







Dominica

Dominica

GCI 5th Edition Country Performance



*Countries are classified according to $\underline{www.itu.int}$

Area(s) of Relative Strength Capacity Development Measures Area(s) of Potential Growth Technical Measures Organizational Measures Cooperation Measures Legal Measures Tier Performance T4: Evolving

Cybersecurity Commitment

Dominican Republic

Dominican Republic

Dominican Republic Score

Americas Region Average Score

Legal Measures
20

15

Cooperation Measures
5

Technical Measures

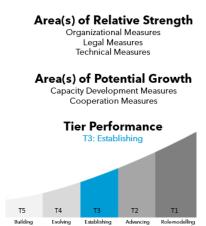
Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
18.48	15.74	18.37	10.64	

*Countries are classified according to www.itu.int

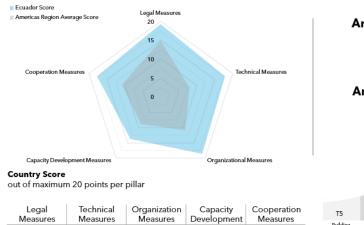
GCI 5th Edition Country Performance



Ecuador

Ecuador

GCI 5th Edition Country Performance



19.21 17.89 18.6 13.78 17.7

*Countries are classified according to wow its int

Area(s) of Relative Strength Organizational Measures Legal Measures Cooperation Measures Technical Measures Area(s) of Potential Growth Capacity Development Measures Tier Performance T2: Advancing T5 T4 T3 T2 T1 Building Evolving Establishing Advancing Role modelling Cybersecurity Commitment

El Salvador

Sierra Leone

Africa Region Average Score
Sierra Leone Score

Legal Measures

20

15

10

Cooperation Measures

5

0

Capacity Development Measures

Capacity Development Measures

Country Score

out of maximum 20 points per pillar

 Legal Measures
 Technical Measures
 Organization Measures
 Capacity Development
 Cooperation Measures

 17.29
 1.39
 18.81
 6.95
 12.02

*Countries are classified according to www.itu.int

GCI 5th Edition CountryPerformance



Establishing

Advancing

Rolemodelling

Grenada

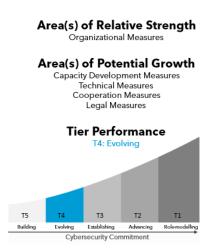
Grenada

GCI 5th Edition Country Performance



Measures 13.8 2.36 3.99

*Countries are classified according to www.itu.int



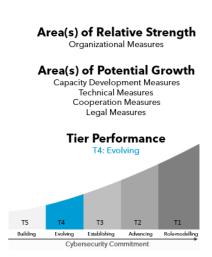
Guatemala

Guatemala

GCI 5th Edition Country Performance



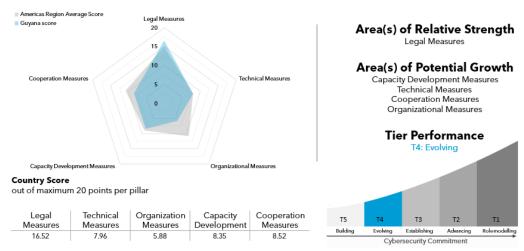
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
6.99	3.77	12.58	8.68	7.97



Guyana

Guyana

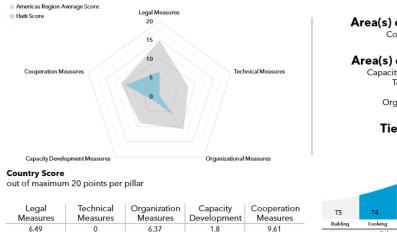
GCI 5th Edition Country Performance



*Countries are classified according to www.itu.int

Haiti

Haiti GCI 5th Edition Country Performance

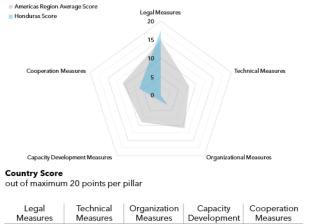




Honduras

Honduras

GCI 5th Edition Country Performance



17.44 0 3.16 1.38 6.09

*Countries are classified according to www.itu.int



Jamaica

Jamaica

GCI 5th Edition Country Performance

Area(s) of Relative Strength
Legal Measures
Organizational Measures



16.41 6.58 15.82

Area(s) of Potential Growth
Capacity Development Measures
Cooperation Measures
Technical Measures

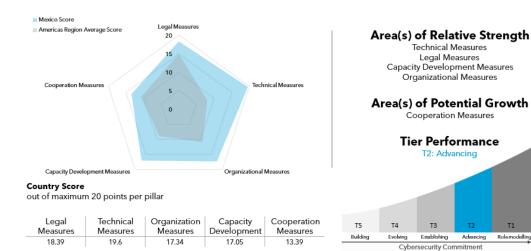
Tier Performance
T3: Establishing

T5
T4
T4
T5
T4
T6
Evolving
Establishing
T7
Role modelling
Cybersecurity Commitment

Mexico

Mexico

GCI 5th Edition Country Performance



Nicaragua

Nicaragua

GCI 5th Edition Country Performance

Advancing

Role-modelling



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
12.33	0	5.97	0	



Panama

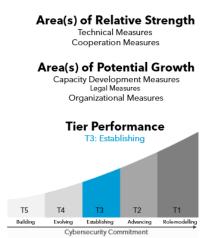
Panama

GCI 5th Edition Country Performance



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
14.02	14.49	13.15	7.14	17.74

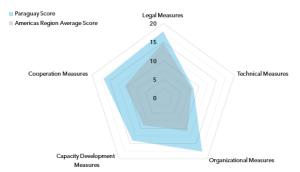
*Countries are classified according to www.itu.int



Paraguay

Paraguay

GCI 5th Edition Country Performance



Country Score

out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures	
17.81	8.47	17.66	14.03	16.8	



Peru

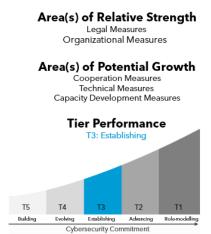
Peru

GCI 5th Edition Country Performance



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	13.51	18.27	15.16	16.8

*Countries are classified according to www.itu.int



Saint Kitts and Nevis

Saint Kitts and Nevis

GCI 5th Edition Country Performance



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
13.35	1.78	2.67	7.34	6.46



Saint Lucia

Saint Lucia

GCI 5th Edition Country Performance



*Countries are classified according to www.itu.int

Area(s) of Relative Strength Legal Measures Area(s) of Potential Growth Cooperation Measures Technical Measures Organizational Measures Capacity Development Measures Tier Performance T4: Evolving T5 T4 T3 T2 T1 Rolemodolling Cybersecurity Commitment

Saint Vincent and the Grenadines

Saint Vincent and the Grenadines

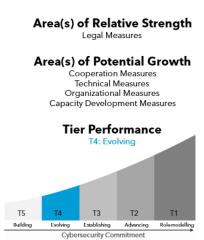
GCI 5th Edition Country Performance



Country Score

out of maximum 20 points per pillar

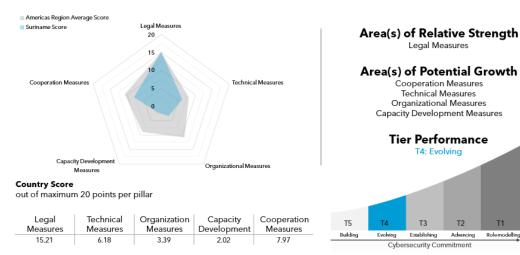
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
11.58	0	4.72	3.78	6.46



Suriname

Suriname

GCI 5th Edition Country Performance



Trinidad and Tobago

Trinidad and Tobago

 Americas Region Average Score
 Trinidad and Tobago Score 15 Cooperation Measures Technical Measures

Country Score out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
8.88	6.98	16.21	13.03	

*Countries are classified according to www.itu.int

GCI 5th Edition Country Performance



Rolemodelling

United States

United States

GCI 5th Edition Country Performance



Capacity Development Measures 20 20 19.86 20

*Countries are classified according to www.itu.int



Uruguay

Uruguay

GCI 5th Edition Country Performance



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
19.15	20	19.51	19.45	16.58



Venezuela

Venezuela

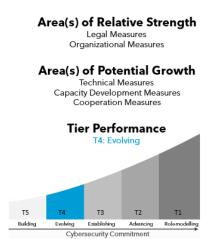
GCI 5th Edition Country Performance



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
15.01	4.56	12.23	4.69	



Arab States

Algeria

Algeria

GCI 5th Edition Country Profile



Measures Measures Measures Measures 19.18 8.57 11.02 13.19 13.91

Area(s) of Relative Strength Legal Measures Area(s) of Potential Growth Technical Measures Organizational Measures Capacity Development Measures Cooperation Measures **Tier Performance** T3: Establishing T5

Establishing

Bahrain

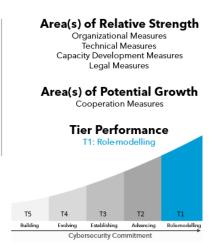
Bahrain

GCI 5th Edition Country Profile

Advancing



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	20	20	17.94

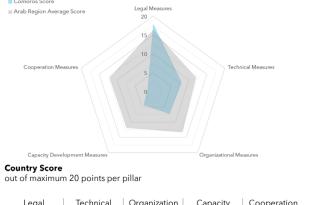


^{*}Countries are classified according to www.itu.int

Comoros

Comoros

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
18.03	7.92	7.29	4.39	1.52

^{*}Countries are classified according to www.itu.int

Area(s) of Relative Strength Legal Measures Area(s) of Potential Growth Technical Measures Organizational Measures Capacity Development Measures Cooperation Measures Tier Performance T4: Evolving

Cybersecurity Commitment

Djibouti

Djibouti

GCI 5th Edition Country Profile



Out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
11.84	3.54	5.57	1.67	8.87



Egypt

Egypt

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	20	20	20

*Countries are classified according to www.itu.int



Iraq

Iraq GCI 5th Edition Country Profile



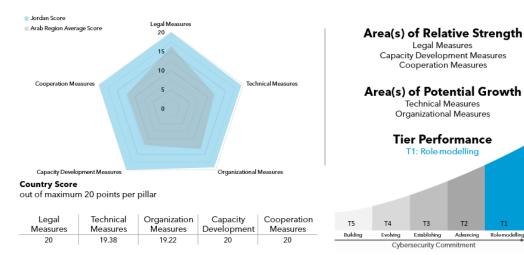
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
11.21	9.6	15.77	8.38	8.11



Jordan

Jordan

GCI 5th Edition Country Profile



Kuwait

Kuwait GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
16.9	5.8	11.88	12.16	

*Countries are classified according to www.itu.int



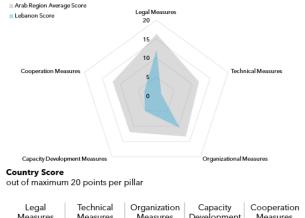
T3

T2

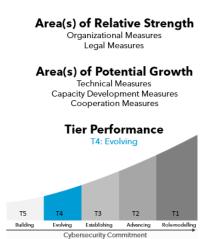
Lebanon

Lebanon

GCI 5th Edition Country Profile







Libya

Libya

GCI 5th Edition Country Profile



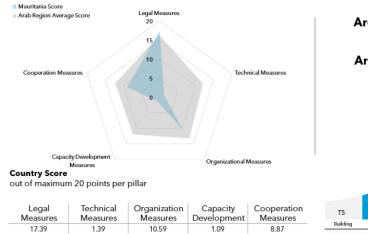
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
16.75	11.2	14	15.75	10.39



Mauritania

Mauritania

GCI 5th Edition Country Profile



*Countries are classified according to www.itu.int

Area(s) of Relative Strength Legal Measures Area(s) of Potential Growth Organizational Measures Technical Measures Capacity Development Measures Cooperation Measures Tier Performance T4: Evolving T5 T4 T3 T2 T1 Building Evolving Establishing Advancing Rolo-modelling Cybersecurity Commitment

Morocco

Morocco

GCI 5th Edition Country Profile





Oman

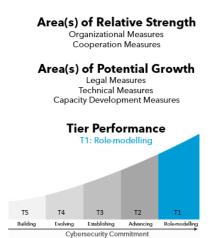
Oman

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
19.59	18.39	20	19.03	20

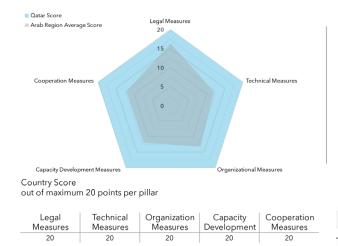
*Countries are classified according to www.itu.int

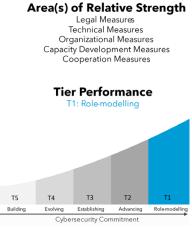


Qatar

Qatar

GCI 5th Edition Country Profile

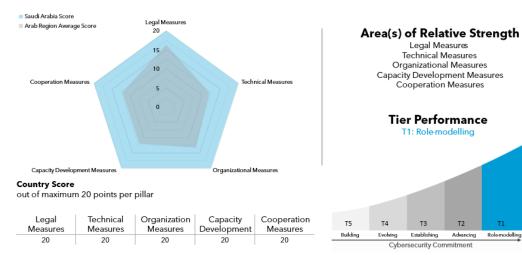




Saudi Arabia

Saudi Arabia

GCI 5th Edition Country Profile



^{*}Countries are classified according to www.itu.int

Somalia

Somalia GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
6.49	4.79	10.64	4.29	11.17



State of Palestine

State of Palestine

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
14.24	9.6	2.38	9.04	2.46

*Countries are classified according to www.itu.int

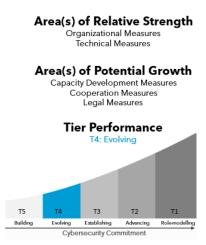


Sudan

Sudan GCI 5th Edition Country Profile



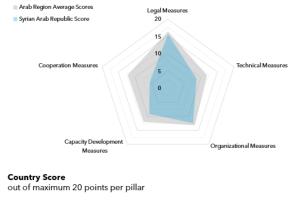
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
15.57	14.47	6.41	4.37	7.35



Syrian Arab Republic

Syrian Arab Republic

GCI 5th Edition Country Profile



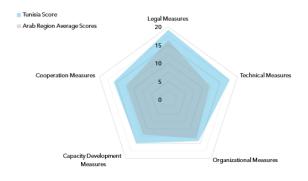
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
15.6	8.74	12.4	9.17	5.48

^{*}Countries are classified according to www.itu.int



Tunisia

Tunisia GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
19.18	17.8	14.23	14.97	15.82

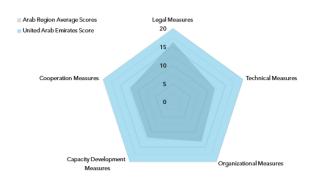
^{*}Countries are classified according to www.ltu.int



United Arab Emirates

United Arab Emirates

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures	
20	20	20	20	20	

*Countries are classified according to $\underline{www.itu.int}$



Yemen

Yemen

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
5.29	1.9	0	0	

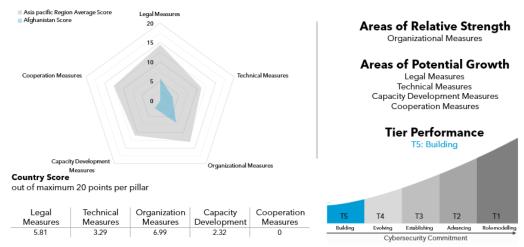


Asia and the Pacific

Afghanistan

Afghanistan

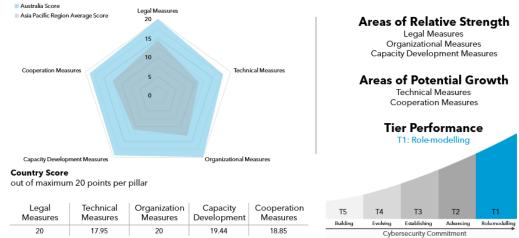
GCI 5^{th} Edition Country Profile



^{*}Countries are classified according to www.itu.int

Australia

Australia GCI 5th Edition Country Profile

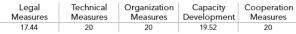


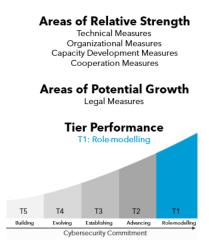
Bangladesh

Bangladesh

GCI 5th Edition Country Profile







Bhutan

Bhutan GCI 5th Edition Country Profile



Development Measures Measures Measures Measures 14.18 16,43 13,14 9.71 7.15



Brunei Darussalam

Brunei Darussalam

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
17.2	14.89	11.35	10.76	16.18

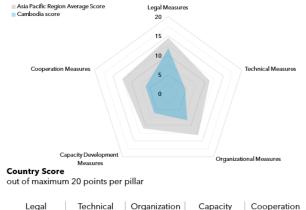
*Countries are classified according to www.itu.ini

Areas of Relative Strength Legal Measures Cooperation Measures Areas of Potential Growth Technical Measures Organizational Measures Capacity Development Measures Tier Performance T3: Establishing T5 T4 T3 T2 T1 Building Evolving Establiching Advancing Cybersecurity Commitment

Cambodia

Cambodia

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
11.82	4.56	8.3	6.12	6.22



China

China GCI 5th Edition Country Profile

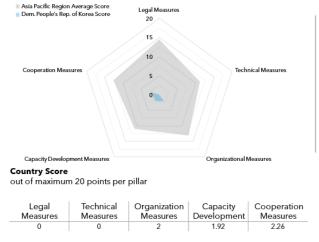




Democratic People's Republic of Korea

Democratic People's Republic of Korea

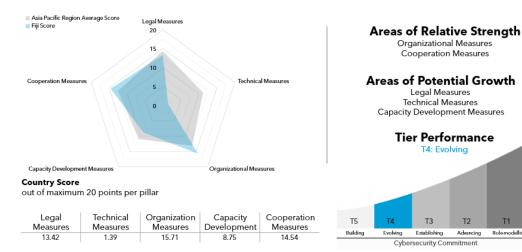
GCI 5th Edition Country Profile





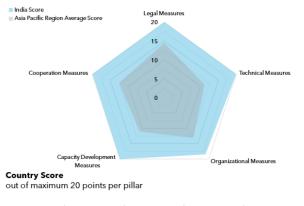
Fiji

Fiji GCI 5th Edition Country Profile



India

India GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	18.49	20	20

*Countries are classified according to www.itu.int



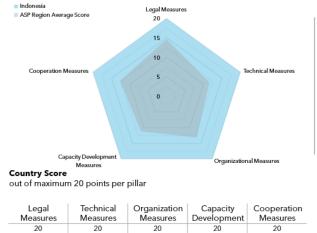
T2

Advancing

Indonesia

Indonesia

GCI 5th Edition Country Profile



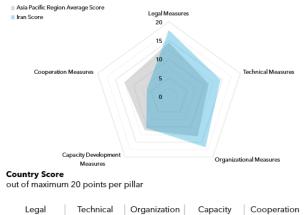


Areas of Relative Strength Legal Measures Technical Measures Organizational Measures Capacity Development Measures Cooperation Measures **Tier Performance** T5 T4 T3 T2 Advancing Establishing Cybersecurity Commitment

Iran (Islamic Republic of)

Iran (Islamic Republic of)

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
17.79	14.49	16.72	10.27	6.25



Japan

Japan

GCI 5th Edition Country Profile



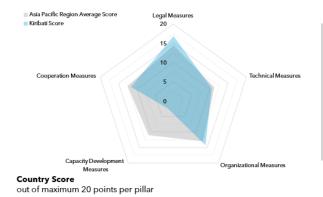
20 19.6 20 19.07 18,91

Areas of Relative Strength Legal Measures Technical Measures Organizational Measures Capacity Development Measures **Area of Potential Growth** Cooperation Measures **Tier Performance** T1: Role-modelling T4 Т3 T2 lving Establishing Advancing Cybersecurity Commitment Advancing

Kiribati

Kiribati

GCI 5th Edition Country Profile



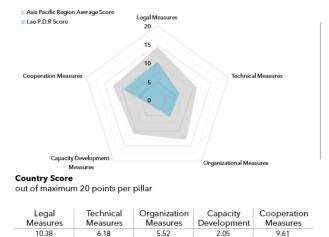
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
16.8	10.49	14.34	2.41	11.6



Lao P.D.R.

Lao P.D.R.

GCI 5th Edition Country Profile





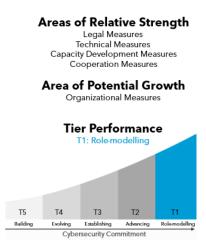
Malaysia

Malaysia

GCI 5th Edition Country Profile



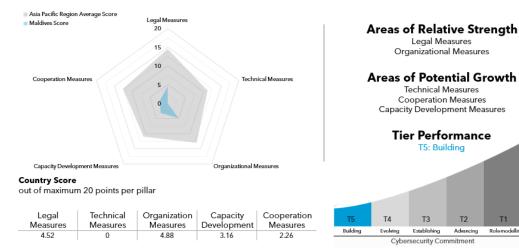
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	18.82	20	20



Maldives

Maldives

GCI 5th Edition Country Profile

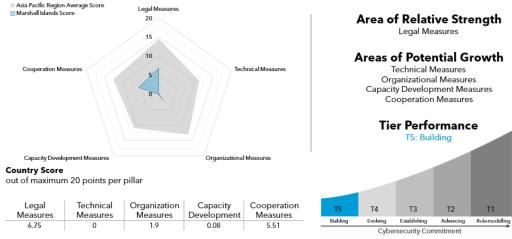


^{*}Countries are classified according to www.itu.int

Marshall Islands

Marshall Islands

GCI 5th Edition Country Profile



^{*}Countries are classified according to www.itu.int

Micronesia

Micronesia

GCI 5th Edition Country Profile



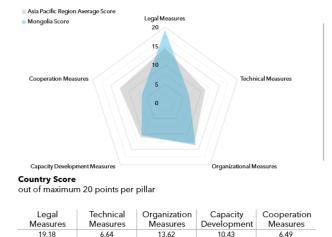
Capacity Development Measures 2.81 1.9 0.08 3.99



Mongolia

Mongolia

GCI 5th Edition Country Profile

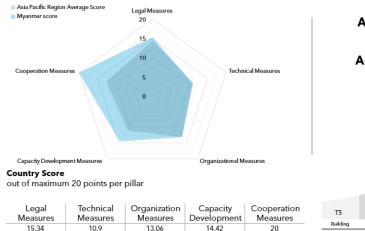




Myanmar

Myanmar

GCI 5th Edition Country Profile

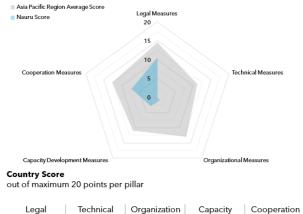


*Countries are classified according to www.itu.int

Area of Relative Strength Cooperation Measures Areas of Potential Growth Legal Measures Technical Measures Organizational Measures Capacity Development Measures Tier Performance T3: Establishing T5 T4 T3 T2 T1 Bulding Evolving Establishing Advancing Role modelling Cybersecurity Commitment

Nauru

Nauru GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
10.47	0	1.04	2.93	7.15



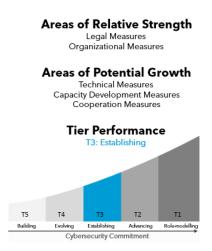
Nepal (Republic of)

Nepal (Republic of)

GCI 5th Edition Country Profile



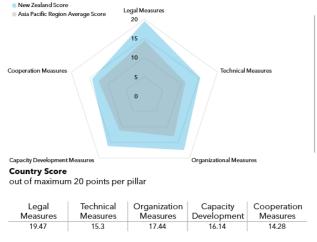
Measures Development 19.21 11.09 16.92 13.09 9.45



New Zealand

New Zealand

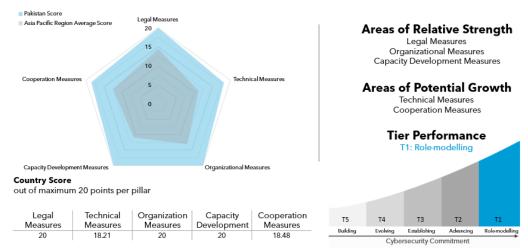
GCI 5th Edition Country Profile





Pakistan

Pakistan GCI 5th Edition Country Profile

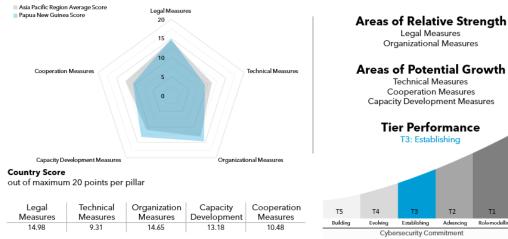


^{*}Countries are classified according to www.itu.in

Papua New Guinea

Papua New Guinea

GCI 5th Edition Country Profile

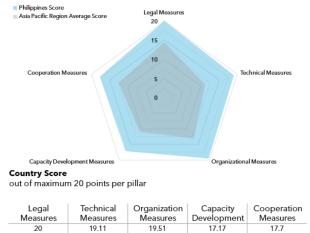


^{*}Countries are classified according to www.itu.int

Philippines

Philippines

GCI 5th Edition Country Profile





Republic of Korea

Republic of Korea

GCI 5th Edition Country Profile

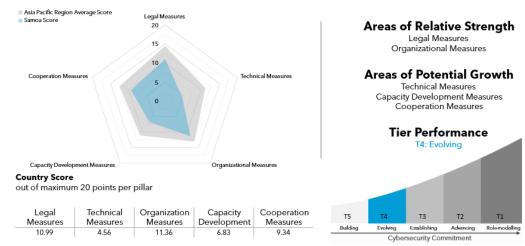






Samoa

Samoa GCI 5th Edition Country Profile

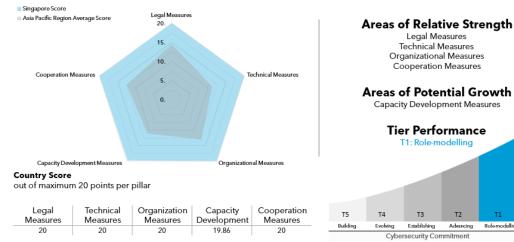


Singapore

Singapore

GCI 5th Edition Country Profile

Role-modelling



^{*}Countries are classified according to www.itu.int

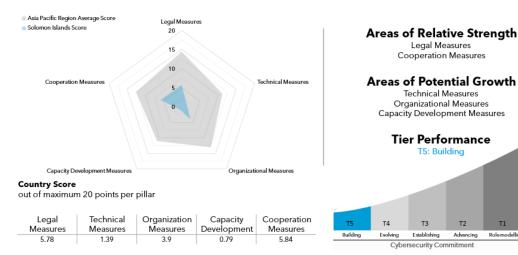
Solomon Islands

Solomon Islands

GCI 5th Edition Country Profile

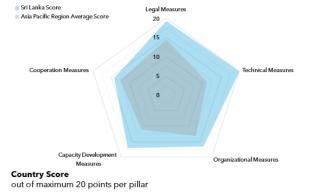
T2

Advancing



Sri Lanka

Sri Lanka GCI 5th Edition Country Profile



Legal Technical Organization Capacity Cooperation Development Measures Measures Measures Measures 19.21 20 16.42 17.11 14.28



Thailand

Thailand

GCI 5th Edition Country Profile



20 20 19.22 20

Areas of Relative Strength Legal Measures Technical Measures Capacity Development Measures Cooperation Measures **Area of Potential Growth** Organizational Measures **Tier Performance** T1: Role-modelling T5 T4 T3 T2 Establishing

Cybersecurity Commitment

Timor-Leste

Timor-Leste

GCI 5th Edition Country Profile

Advancing



Country Score

out of maximum 20 points per pillar

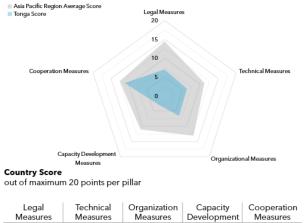
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
6.22	0	2.9	1.01	6.69

^{*}Countries are classified according to $\underline{www.itu.int}$



Tonga

Tonga GCI 5th Edition Country Profile



7.01 6.18 6.59 2.87 11.13

Area of Relative Strength Cooperation Measures **Areas of Potential Growth** Legal Measures Technical Measures Organizational Measures Capacity Development Measures **Tier Performance** T4: Evolving T5 T2 olving Establishing Advancing Cybersecurity Commitment

Tuvalu

Tuvalu GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
7.28	0	3.57	2.34	7.15



Vanuatu

Vanuatu

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
15.63	14.49	17.37	5.62	16.18

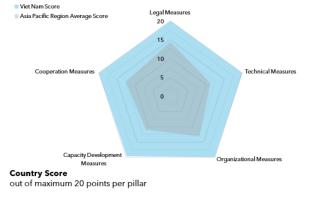
Areas of Relative Strength Cooperation Measures Organizational Measures **Areas of Potential Growth** Legal Measures Technical Measures Capacity Development Measures **Tier Performance** T3: Establishing T5 T4 T2 lving Establishing Advancing Cybersecurity Commitment Rolemodelling

Building

Viet Nam

Viet Nam

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	20	19.74	20



Commonwealth of Independent States

Armenia

Armenia

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
17.22	8.69	2.81	10.35	

*Countries are classified according to www.itu.int



Azerbaijan

Azerbaijan

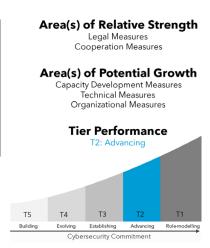
GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	18.02	18.05	17.69	20



Belarus

Belarus

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
18.61	2.78	11.97	8.98	19.11

^{*}Countries are classified according to www.itu.int

Area(s) of Relative Strength Legal Measures Cooperation Measures Area(s) of Potential Growth Technical Measures Organizational Measures Capacity Development Measures Tier Performance T3: Establishing T5 T4 T3 T2 T1 Bullding Evolving Establishing Cybersecurity Commitment

Kazakhstan

Kazakhstan

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	19.38	18.3	16.36	20



Kyrgyzstan

Kyrgyzstan

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
16.71	14.87	16.32	5.53	12.16

*Countries are classified according to www.itu.int



Russian Federation

Russian Federation

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

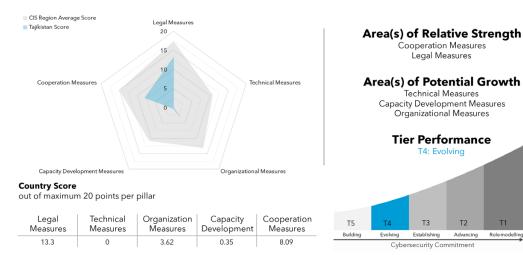
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	16.59	20	18.77	



Tajikistan

Tajikistan

GCI 5th Edition Country Profile

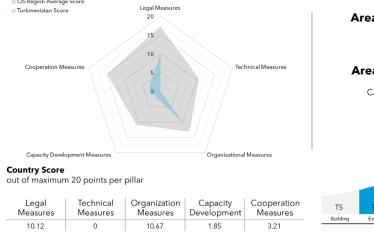


Turkmenistan

Turkmenistan

GCI 5th Edition Country Profile

Role-modelling



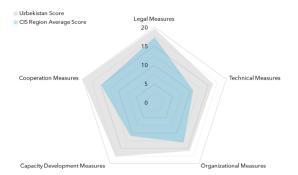




Uzbekistan

Uzbekistan

GCI 5th Edition Country Profile



Country Score out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
19.59	16.22	15.75	17.64	20

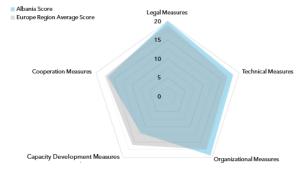


Europe

Albania

Albania

GCI 5th Edition Country Profile



Country Score out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	18.38	19.47	12.08	16.58

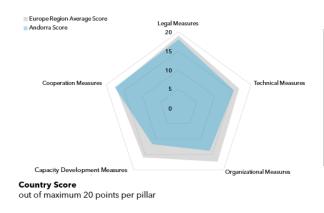
^{*}Countries are classified according to www.itu.int



Andorra

Andorra

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
18.04	15.3	13.88	11.74	17.7



Austria

Austria

GCI 5th Edition Country Profile



Legal
MeasuresTechnical
MeasuresOrganization
MeasuresCapacity
DevelopmentCooperation
Measures18.4218.2317.5618.3616.59

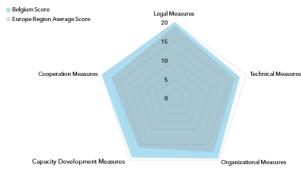
*Countries are classified according to www.itu.ini



Belgium

Belgium

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

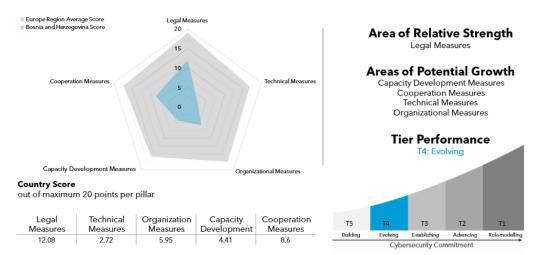
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	18.11	19.51	19.19	20



Bosnia and Herzegovina

Bosnia and Herzegovina

GCI 5th Edition Country Profile

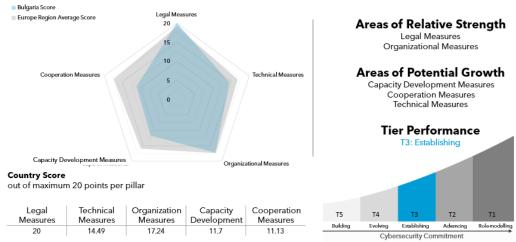


^{*}Countries are classified according to www.itu.ini

Bulgaria

Bulgaria

GCI 5th Edition Country Profile

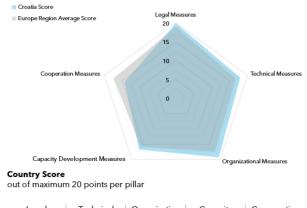


^{*}Countries are classified according to www.itu.int

Croatia

Croatia

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	17.39	19.34	16.74	14.28

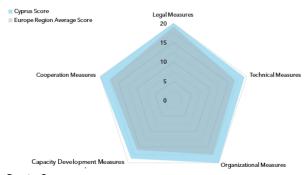
*Countries are classified according to www.itu.in



Cyprus

Cyprus

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	19.38	20	18.64	



Czech Republic

Czech Republic

GCI 5th Edition Country Profile



Legal
MeasuresTechnical
MeasuresOrganization
MeasuresCapacity
DevelopmentCooperation
Measures2015.32018.3614.28

*Countries are classified according to www.itu.in



Denmark

Denmark

GCI 5th Edition Country Profile



Country Score

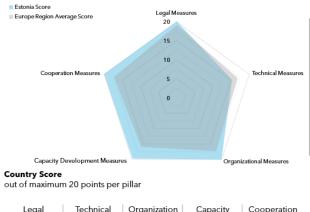
out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures	
20	20	20	20	20	



Estonia

Estonia GCI 5th Edition Country Profile



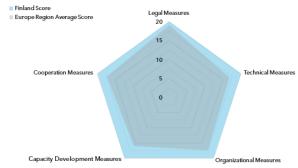
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	15.3	20	19.74	20

*Countries are classified according to www.itu.int



Finland

Finland GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

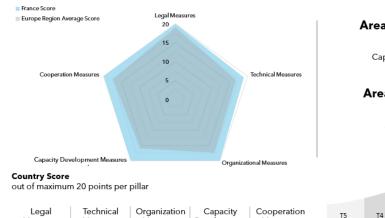
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	20	20	



France

France

GCI 5th Edition Country Profile



Capacity Development Measures 20 18.98 20

Areas of Relative Strength Legal Measures Organizational Measures Capacity Development Measures Cooperation Measures **Area of Potential Growth** Technical Measures **Tier Performance** T1: Role-modelling T5 T3 T2

Establishing

CybersecurityCommitment

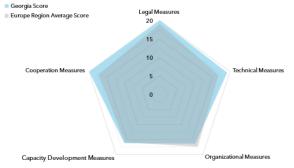
Building

Georgia

Georgia

GCI 5th Edition Country Profile

Advancing



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	19.25	16.35	16.32	20



Germany

Germany

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	17.93	20	19.92	15.99

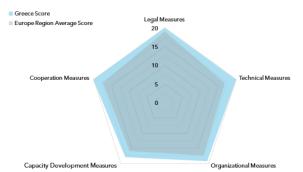
*Countries are classified according to www.itu.int



Greece

Greece

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

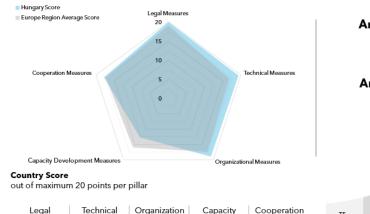
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	19.22	17.89	



Hungary

Hungary

GCI 5th Edition Country Profile



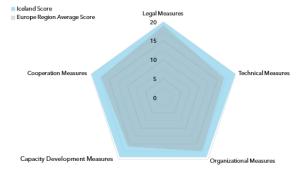
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	19.4	18.96	12.63	17.74

^{*}Countries are classified according to www.itu.int

Areas of Relative Strength Legal Measures Technical Measures Organizational Measures Organizational Measures Areas of Potential Growth Capacity Development Measures Cooperation Measures Tier Performance T2: Advancing T5 T4 T3 T2 Building Evolving Establishing Advancing Rolemodelling Cybersecurity Commitment

Iceland

Iceland GCI 5th Edition Country Profile

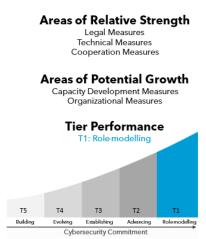


Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	19.4	19.7	20

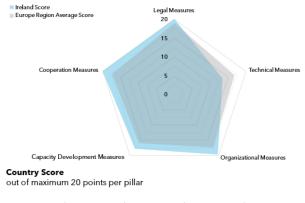
^{*}Countries are classified according to $\underline{www.ltu.int}$



Ireland

Ireland

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	13.52	19.67	17.71	20

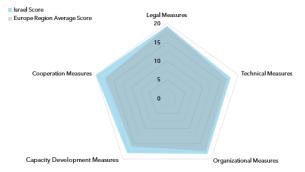
^{*}Countries are classified according to www.itu.int



Israel

Israel

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

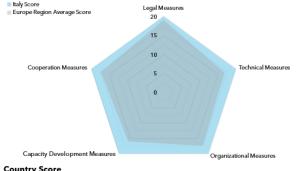
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
19.27	17.87	18.34	18.12	



Italy

Italy

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures	
20	20	20	20	20	

^{*}Countries are classified according to www.itu.int

Areas of Relative Strength Legal Measures Technical Measures Organizational Measures Capacity Development Measures Cooperation Measures **Tier Performance** T5 T4 T3 T2 lving Establishing Advancing Cybersecurity Commitment

Latvia

Latvia

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

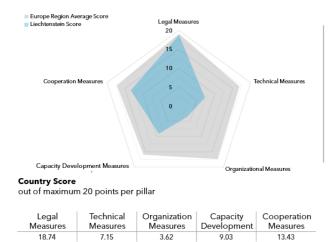
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	14.89	19.34	14.12	14.28



Liechtenstein

Liechtenstein

GCI 5th Edition Country Profile



^{*}Countries are classified according to www.lhu.int

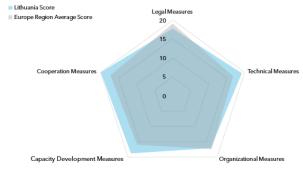
Areas of Relative Strength Legal Measures Cooperation Measures Areas of Potential Growth Technical Measures Organizational Measures Capacity Development Measures Tier Performance T4: Evolving T5 T4 T3 T2 T1 Evolving Cybersecurity Commitment

*Countries are classified according to <u>www.ltu.int</u>

Lithuania

Lithuania

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

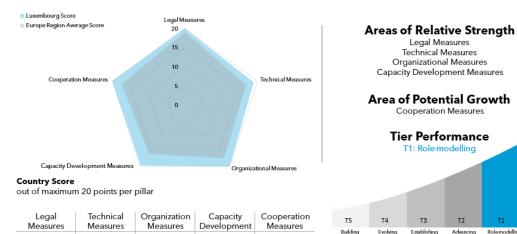
Legal	Technical	Organization	Capacity	Cooperation	
Measures	Measures	Measures	Development	Measures	
17.79	19.25	17.05	18.79	20	



Luxembourg

Luxembourg

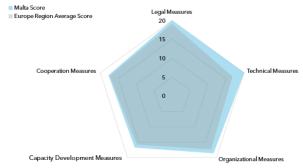
GCI 5th Edition Country Profile



20 18.98 19.74 20

Malta

Malta GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation	
Measures	Measures	Measures	Development	Measures	
20	20	18.68	16.84	17.44	

*Countries are classified according to www.itu.int



T3

Establishing

Cybersecurity Commitment

T2

Advancing

Moldova

Moldova

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
18.28	6.68	15.51	8.04	16.58



Monaco

Monaco

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

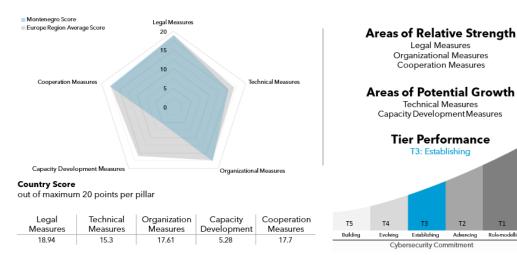
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
18.6	13.68	15.16	13.7	



Montenegro

Montenegro

GCI 5th Edition Country Profile



Netherlands (Kingdom of the)

Netherlands (Kingdom of the)

GCI 5th Edition Country Profile



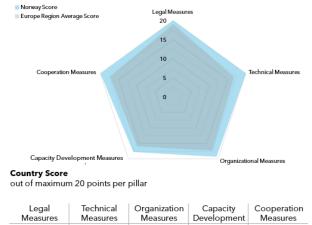




Norway

Norway

GCI 5th Edition Country Profile



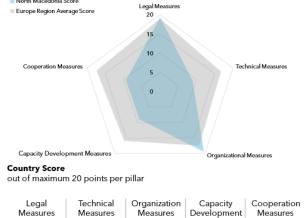
20 20 19.31 17.7



North Macedonia

North Macedonia

GCI 5th Edition Country Profile



Development Measures Measures 19.21 8.89 19.47 9.04 9.28



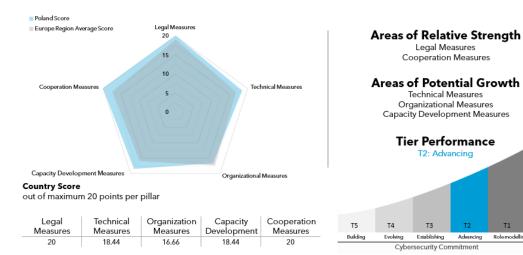
Poland

Poland

GCI 5th Edition Country Profile

T2: Advancing

T3



Portugal

Portugal

GCI 5th Edition Country Profile

Role-modelling



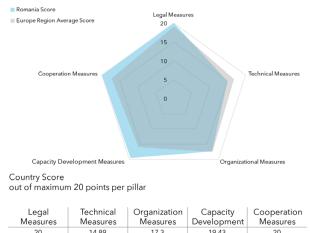
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	20	19.86	20



Romania

Romania

GCI 5th Edition Country Profile



20 14.89 17.3 19.43 20

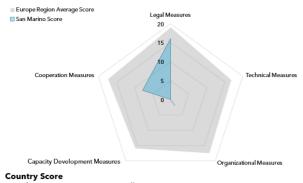
*Countries are classified according to www.itu.int



San Marino

San Marino

GCI 5th Edition Country Profile



out of maximum 20 points per pillar

Legal Measures	5		Capacity Development	Cooperation Measures
16.11	0	2	0	7.77



Serbia

Serbia

GCI 5th Edition Country Profile



Legal			Capacity	Cooperation
Measures			Development	Measures
20	18.38	19.22	19.22	20

^{*}Countries are classified according to www.itu.ini

Areas of Relative Strength Legal Measures Organizational Measures Capacity DevelopmentMeasures Cooperation Measures Area of Potential Growth Technical Measures Tier Performance T1: Role-modelling

Slovakia

Slovakia

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation	
Measures	Measures	Measures	Development	Measures	
20	20	20	18.45	15.99	



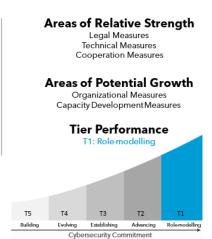
Slovenia

Slovenia

GCI 5th Edition Country Profile



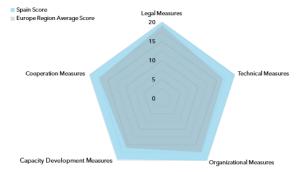




Spain

Spain

GCI 5th Edition Country Profile



Country Score

out of maximum 20 points per pillar

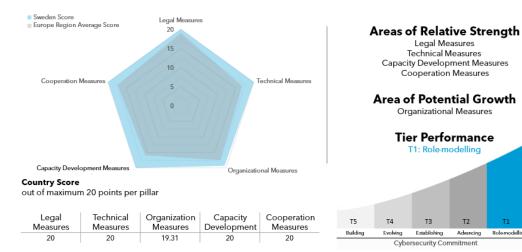
Legal	Technical	Organization	Capacity	Cooperation
Measures	Measures	Measures	Development	Measures
20	20	20	19.74	



Sweden

Sweden

GCI 5th Edition Country Profile

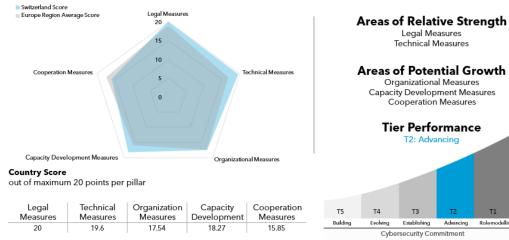


^{*}Countries are classified according to www.itu.int

Switzerland

Switzerland

GCI 5th Edition Country Profile



^{*}Countries are classified according to www.ltu.int

Türkiye

Türkiye

GCI 5th Edition Country Profile





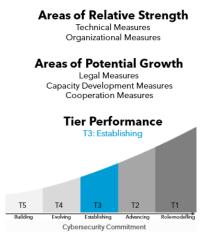


Ukraine

Ukraine

GCI 5th Edition Country Profile





United Kingdom

United Kingdom

GCI 5th Edition Country Profile



Legal	Technical	Organization	Capacity	Cooperation	
Measures	Measures	Measures	Development	Measures	
20	20	20	20	20	



Vatican

Vatican GCI 5th Edition Country Profile



out of maximum 20 points per pillar

Legal	Technical	Organization	Capacity	Cooperation	
Measures	Measures	Measures	Development	Measures	
1.41	0	3.62	2.91	1.13	

^{*}Countries are classified according to www.itu.int



Methodology

Scope and objectives

The Global Cybersecurity Index (GCI) is formulated based on data provided by the ITU membership, including interested individuals, experts and industry stakeholders as contributing partners. The mandate for the GCI is derived from Resolution 130 (Rev. Bucharest, 2022) of the ITU Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of information and communication technologies (ICTs), which, in particular, invites Member States to support ITU initiatives on cybersecurity, including the GCI, in order to promote government strategies and the sharing of information on efforts across industries and sectors.

The fifth edition of the GCI continues this tradition and builds on earlier iterations. This is manifested in areas such as a refined methodology, increased participation and collaboration throughout the process, greater availability and accessibility of relevant inputs, developments in questionnaire designs, and the strengthening of evidence-based data collection and analysis.

The GCI is a composite index of indicators that monitors the cybersecurity measures across the five work areas of the Global Cybersecurity Agenda (GCA). The GCI measures:

- the type, level and extent of progress of cybersecurity activities within countries and relative to other countries;
- the progress in cybersecurity commitment of countries from a global perspective;
- the progress in cybersecurity activities from a regional perspective;
- the cybersecurity divide (i.e. the difference between countries and regions in terms of their level of engagement in cybersecurity initiatives).

Collectively, these measures represent a country's level of cybersecurity commitments.

The GCI seeks to foster a global culture of cybersecurity, so that ICTs incorporate cybersecurity in their development and adoption. Further, the GCI aims to assist countries in identifying areas of relative strength in managing cybersecurity and cybercrime, in addition to identifying areas of improvement, and to encourage them to take proactive measures towards further development and innovations in those areas. It is anticipated that this perspective will provide an opportunity to help raise the overall level of cybersecurity commitment worldwide, harmonize good practices and foster a culture of cybersecurity at the national, regional and global levels. To this end, the GCI shares practical insights that might serve as good practices, lessons and guidelines for countries with similar national environments.

Structure

Cybersecurity framework

Cybersecurity is a multidisciplinary field, and its application involves all sectors, industries and stakeholders, both vertically and horizontally. To increase the development of national capabilities, efforts must be made by political, economic and social forces. This can be achieved through the efforts of good actors within the ecosystem, such as law enforcement, justice departments, educational institutions, ministries, private sector operators, ICT developers, public-private partnerships and intra-State cooperation.

Figure 21: GCI evolution over time through a basic comparison of its different editions

	GClv1	GClv2	GClv3	GClv4	GCIv5
Publishing year	2015	2017	2019	2021	2024
Data collection years	2013-2014	2016	2017-2018	2020	2023-2024
Countries providing a focal point	105	136	155	169	172
Question type	Open-ended	Closed- ended, binary	Closed- ended, binary	Closed- ended, ternary	Closed- ended, ternary
Scoring method	Benchmark scores	Rank-based weighted scores	Rank-based weighted scores	Aggregate weighted average score	Aggregate weighted average score
Total indicators	17	25	25	20	20
Total questions	17	153 + 4 optional questions on child online protection	50	82	82 + 1 optional question on training for MSMEs

The ITU framework for international multistakeholder cooperation in cybersecurity aims to build synergies between current and future initiatives. It focuses on the following five pillars, which shape the inherent building blocks of a national cybersecurity culture:

- Legal measures
- Technical measures
- Organizational measures
- Capacity-development measures
- Cooperation measures

Cybercrime Laws

Cybercrime Laws

Cybercrime Laws

Cybersecurity
Regulations

Responsible agency
Cybersecurity grown implementation of cybersecurity standards
Child Online Protection strategies and initiatives

Cybersecurity Research
Autional Cybersecurity agreements with other countries

Cybersecurity Research
Autional framework for implementation of cybersecurity standards
Child Online Protection
Cybersecurity Research
Autional Cybersecurit

Figure 22: Structure of the fifth edition of the GCI

The five pillars are described in detail below and presented in a flowchart in Figure 22: Structure of the fifth edition of the GCI.

Legal measures



Measures based on the existence of legal frameworks dealing with cybersecurity and cybercrime.

Legal measures authorize a State to set up basic response mechanisms through the criminalization of certain acts, the investigation and prosecution of crimes, the imposition of sanctions for offences, non-compliance or breaches, and the establishment of institutional frameworks for managing or governing cybersecurity.

A legislative framework sets the minimum foundation of behaviour on which further cybersecurity capabilities can be built. Fundamentally, the objective is to have sufficient legislation in place to harmonize practices at the regional/international level, strengthen cybersecurity systems, and simplify international frameworks to combat cybercrime.

Technical measures



Measures based on the existence of technical institutions, standards and frameworks dealing with cybersecurity and cybercrime.

Efficient ICT development and use can only prosper in an environment of trust and security. Countries therefore need to have the technical capabilities and capacity to be able to effectively identify, detect, protect and respond to cyber-risks and cyberthreats, and to recover from attacks, as well as to promote information-sharing and evaluate and implement standards, good cybersecurity practices, and schemes for secure ICTs.

Organizational measures



Measures based on the existence of coordination institutions, policies and strategies for cybercrime management and cybersecurity development at the national level.

Organizational measures include the identification of cybersecurity objectives and strategic plans, as well as the formal definition of institutional roles, responsibilities and accountabilities to ensure implementation and achievement of objectives. These measures are indispensable for endorsing the elaboration and implementation of an effective cybersecurity posture. Broad strategic targets and goals need to be set by the State, along with a comprehensive plan for implementation, delivery and measurement. National agencies must be present to implement the strategy and evaluate outcomes. Without a national strategy, governance model or supervisory body, efforts in different sectors become conflicted, undermining efforts to obtain an effective harmonization in cybersecurity development.

Capacity-development measures



Measures based on the existence of research and development, awareness raising, education and training programmes, certified professionals and public sector agencies fostering capacity development.

Capacity development includes public awareness-raising campaigns, frameworks for certification and accreditation of cybersecurity professionals, professional training courses in cybersecurity, educational programmes or academic curricula, etc. This pillar is intrinsic to the first three pillars (legal, technical and organizational). Cybersecurity is most often tackled from a technological perspective even though there are numerous socio-economic and political implications. Human and institutional capacity development is essential to increasing awareness, knowledge and know-how across sectors for systematic and appropriate solutions and to promoting the development of qualified professionals.

Cooperation measures



Measures based on the existence of partnerships, cooperation frameworks and information sharing networks at the national, regional and global levels.

Due to the unprecedented level of interconnection between states, cybersecurity is a shared responsibility and a transnational challenge. Greater cooperation can enable the development of much stronger cybersecurity capabilities, helping to mitigate cyber-risks and enable better investigation, apprehension and prosecution of malicious agents.

Computational methodology

The GCI is based on cybersecurity measures that a country can undertake as part of strengthening their cybersecurity commitment. The GCI questionnaire provides a value for the 20 indicators constructed through 83 questions, where one question is not scored. Countries can submit ternary responses (yes; partial/in progress; no) to all questions.

To ensure accuracy, countries were required to support their answer through evidence, such as an active URL, pdf, photo or other document which can reasonably substantiate their response. Countries can also comment on their submission to contextualize their evidence.

Weighting

This fifth iteration of the GCI is on a scale of 0 to 100, with each pillar weighted at 20 points.

As a composite weighted index, each indicator, sub-indicator and micro-indicator is assigned a weight given the relative importance to the indicator group. Weighting can have a significant impact on final scores, and different techniques will produce different overall scores.

Weighting recommendations were done using a budget allocation method.²³ Experts were asked to contribute weighting recommendations for pillars in which they had expertise. Experts were given a "budget" that they could distribute within an indicator group, thereby allocating a greater amount towards indicators that were assessed as more important within their relative group. The average weighting recommendations were adopted.

These weightings were not shared with countries during the GCI data collection period so as not to influence country responses. The weighting does not account for the accuracy of the data.

Aggregation

Indicator groups were aggregated using weighted arithmetic averages. As a result, a country scoring poorly in one area could compensate by performing well elsewhere. However, for the purposes of clarity and comprehension, a linear approach was deemed more understandable.

A country's score aggregation for each pillar is expressed as follows:

$$GCI_p = \left(\frac{\sum_{i=1}^{n} (q_i \times w_i)}{\sum_{i=1}^{n} w_i}\right) \times 20$$

Where:

 GCI_p = each pillar of the GCI

 q_i = the score associated with a ternary response to a question within a pillar

 w_i = weight assigned to a question within that pillar

n = total number of questions in each pillar

20 is the value of each pillar weighting

A country's overall score is the summation of its scores in each pillar, GCl₂.

https://www.oecd-ilibrary.org/docserver/533411815016.pdf?expires=1722358078&id=id&accname=ocid195767&checksum=D06A2D569CE2B1DC75AAF3967AEBEFE3

Tiers

As noted in in the methodology section on the move to a tier-based model, this edition presents country performance in tiers, rather than ranks. Tiers represent several benefits over ranks, as differences between country scores can be very narrow and include an error range based on the accuracy of questionnaire responses, clarifications provided or country engagement. Each tier groups similarly scoring countries together, thereby presenting a group of similarly performing peers.

The tier-based model has been set for overall scores. As the overall score is a weighted average of a country's cybersecurity activities across all five pillars in the questionnaire, countries with similar scores may still have significant differences on a pillar, indicator, sub-indicator or microindicator level. Countries' activities across pillars and indicators will vary in terms of quality and impact, factors not measured by the GCI.

Countries may choose to develop their own rankings or tiers for the GCI; it must be noted, however, that alternative ways of comparing countries are not endorsed by ITU.

The absolute-score method for tiers was applied based on the following, as described above in Table 1:

- T1 $95 \le x \le 100$
- T2 $85 \le x < 95$
- T3 $55 \le x < 85$
- T4 20 ≤ x < 55
- T5 $0 \le x < 20$

The tiers may be interpreted as follows:

- **Tier 1 (T1) Role-modelling** represents countries that obtained an overall GCI score of at least 95/100 by demonstrating a strong cybersecurity commitment to coordinated and government-driven actions that encompass evaluating, establishing and implementing certain generally accepted cybersecurity measures across all five pillars or up to all indicators.
- **Tier 2 (T2) Advancing** represents countries that have obtained an overall score of at least 85/100 by demonstrating a strong cybersecurity commitment to coordinated and government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures in up to four pillars or a substantial number of indicators.
- **Tier 3 (T3) Establishing** represents countries that obtained an overall score of at least 55/100 by demonstrating a basic cybersecurity commitment to government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures across a moderate number of pillars or indicators.
- **Tier 4 (T4) Evolving** represents countries that obtained an overall score of at least 20/100 by demonstrating a basic cybersecurity commitment to government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures in at least one pillar, or several indicators and/or sub-indicators.
- **Tier 5 (T5) Building** represents countries that obtained an overall score below 20/100 by demonstrating a basic cybersecurity commitment to government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures in at least one indicator and/or sub-indicator.

The tier-based model underscores that a cybersecurity commitment requires an adaptive stance in evaluating, establishing or implementing appropriate actions to effectively meet the demands

of the rapidly evolving cybersecurity landscape. Under these circumstances, opportunities will exist for further coordinated actions, improvements and expansions of the breadth and depth of cybersecurity measures, irrespective of a country's overall score.

Key changes and limitations in the fifth edition of the GCI

The GCI has been updated to ensure greater methodological consistency, clarify questions, reflect current weighting recommendations and better represent country performance, including in the following areas:

- Questionnaire: based on a series of meetings of the GCI Expert Group, questions were clarified and refined. This included expanding on the rationales for each question. A final version of the questionnaire was approved by the ITU Telecommunication Development Bureau (BDT) management.
- **Weightings**: as country scores are calculated using a weighted average, the GCI Expert Group was invited to update their weighting recommendations. Some 140 experts were tasked with providing weighting recommendations in pillars related to their areas of expertise. Based on their recommendations, an arithmetic average is taken and used in computation.
- **Tier model**: the GCI Expert Group met and put forward several possible models for a tier-based GCI scoring model to replace the existing model, which ranked country performance. For the final selection of the model, BDT management relied on the preferred choice of the Expert Group.

As cybersecurity continues to be an area of change and countries have innovated to find ways forward, the aim is for GCI questions not to be overly prescriptive and instead to capture the wide variety of tools, programmes, initiatives and other methods countries may use to accomplish various objectives; the trade-off with this less prescriptive approach, however, is that questions might contain ambiguities.

The GCI verification team worked to ensure consistency through regular meetings and communications to ensure that verification decisions were coherent across countries. While feedback from countries was solicited where necessary, the risk of inconsistencies in the verifications remains, particularly in edge cases.

Changes and limitations by pillar

The changes made across the pillars include:

Legal measures

The legal pillar has been updated to better reflect:

• legislation that is in force versus partial/in progress.

Notable limitations that arose during verification include:

- comparability of laws, regulations and decrees what can be considered a law in one country may have lower enforceability or implementation in another country; and
- applicability of laws and regulations while some countries used targeted laws that directly addressed issues at hand, other countries reported using general laws and regulations and applying them to cybersecurity; for the latter, verification was challenging as it was not always clear whether the law or regulation could be applied in a cyber-context.

Technical measures

The technical pillar has been restructured to better reflect how computer incident response teams (CIRTs) operate, including by:

- clarifying that CIRTs do not need to develop and deliver cyber awareness activities, but their involvement is desirable; and
- better reflecting that national CIRTs often develop and deliver cyber drills, while sectoral CIRTs may only participate in them.

Notable limitations that arose included:

- the relevance of certain types of cybersecurity standards and certification;
- the definition of a "framework" for implementation of standards;
- roles and functions of information-sharing and analysis centres (ISACs);
- key activities by CIRTs, particularly around cyber-awareness campaigns and threat notifications.

Organizational measures

The organizational pillar has been updated to better reflect:

- the second edition of the Guide to Developing a National Cybersecurity Strategy;
- regional CIRT membership;
- the need for national CIRTs to assist in conducting cyber drills, while sectoral CIRTs need only to participate.

Notable limitations that arose included:

- the comparability of draft status of national cybersecurity strategies (NCSs);
- perspectives on the life of NCSs;
- depth and specificity of NCS action plans;
- assessment of outcomes of the adoption of cybersecurity metrics; and
- many countries' national CIRTs participated in regional cyber drills but did not organize their own.

Capacity-development measures

The capacity-development pillar has been updated to better reflect:

- diversity in the types of targeted cyber-awareness campaigns;
- promotion and development of the cybersecurity private sector; and
- cybersecurity certification schemes.

Notable limitations that arose included:

- evaluation of whether cybersecurity was substantially present in academic curricula in primary and secondary education;
- lack of data about reach and impact of cyber-awareness campaigns;
- measurement of the cybersecurity industry; and
- evaluation of the presence of research and development in academia and the private and public sectors.

Cooperation measures

The cooperation pillar has been updated to better reflect:

- types of bilateral and multilateral agreements that are to be considered; and
- cooperation agreements that have been signed or ratified the Budapest Convention had been previously counted under international mechanisms, which is no longer a question, and is now counted under multilateral agreements.

Notable limitations that arose included:

- definition of what an "agreement" should be (e.g. joint statement or signed treaty); and
- assessment of the outcomes of cooperation agreements.

The verification team has noted areas of ambiguity and has striven to apply any decisions as evenly as possible to country verifications. The GCI team will present their observations to the GCI Expert Group for feedback and input ahead of the next edition.

Changes to the weighted average scoring

As with the previous edition of the GCI, weightings have been updated as the relative importance and influence of questions and measures may have changed. These changes reflect the dynamism of the cybersecurity landscape and access to an enlarged and more diverse GCI Expert Group. In the future, it is reasonable to expect central tendency effects should there be a sufficiently large expert group.

As always, individual countries may judge that their ideal weighting mix is different, based on their own priorities and dependencies.

Move to a tier-based model

Through Resolution 45 (Rev. Kigali, 2022) of the World Telecommunication Development Conference and Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, BDT was instructed by Member States to move from a rank-based presentation of GCI scoring to a tier-based model.

The GCI Expert Group developed and presented recommendations on how these tiers could be set. After six meetings, the group arrived at two proposals for BDT management. The final proposals are reflected in Table 1.

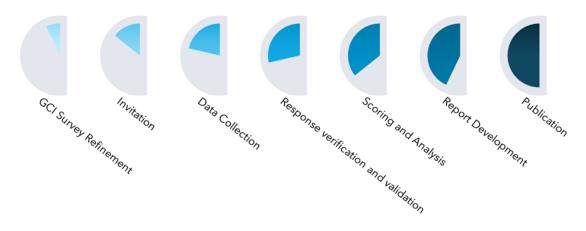
Based on the recommendations of the GCI Expert Group, ITU management approved the use of the "absolute score" method.

Table 1: Tier-based model

	Absolute score	Quantiles	
Proposed Tiers	T1 $95 \le x \le 100$	T1 Top 10% of countries	
	T2 85 ≤ x < 95	T2 Next 20%	
	T3 55 ≤ x < 85	T3 Next 25%	
	T4 20 ≤ x < 55	T4 Next 25%	
	T5 $0 \le x < 20$	T5 Next 20%	
Benefits	 Country performance is primarily gauged against the country itself. Tier score boundaries remain constant over time 	 Distribution of countries across tiers will remain constant over time. Easier for countries to assess their progress against the rest of the world. 	
Limitations	As time goes on, more countries may end up in the top tier, limiting differentiation among them.	Country absolute scores can improve, but their relative position can decrease, potentially demotivating further cybersecurity efforts.	

GCI report development process

Figure 23: GCI report development process



The GCI report is produced according to the following steps, as shown in Figure 23.

- 1) GCI survey refinement: a multistakeholder approach is undertaken in the review and refinement of the GCI indicators and questions. This includes considering the lessons and opportunities for refinements and improvements from previous iterations, feedback from the GCI Expert Group and an assessment of the evolving state of the cybersecurity field. The GCI questionnaire is thereafter reviewed, refined, finalized and approved for dissemination.
- 2) **Invitation**: a letter of invitation is sent to all ITU Member States and the State of Palestine, informing them of the initiative and requesting a focal point responsible for collecting all relevant data and for completing the online GCI questionnaire. During the online survey, the approved focal point is officially invited by BDT to answer the questionnaire.

- 3) **Data collection**: primary and secondary data collection techniques are used to reflect the current state of cybersecurity commitment.
 - Primary data collection: the online questionnaire is used to collect responses from countries;
 - **Secondary data collection**: desk research, using publicly available data sources, is relied on in instances where a country did not respond to the questionnaire.

Note: Should a country not provide a focal point for the GCI questionnaire, BDT shall attempt to establish contact with the institutional focal point in the ITU Global Directory.

1) Verification and validation

A comprehensive iterative process of reviews, analyses, revisions and approvals is established throughout this phase and applied to both data collection methods. Once completed, consistency checks are conducted to help to ensure reliability.

A. Online questionnaire:

- ITU identifies any missing responses, supporting documents, links, etc.
- The focal point improves the accuracy of responses where necessary, including by offering relevant evidence.
- Validated questionnaires are used for analysis and scoring.

B. Desk research questionnaire:

- A draft questionnaire is sent to focal points for review.
- Focal points improve accuracy and return the draft questionnaire.
- BDT reviews responses against the evidence provided and identifies any missing responses, supporting documents, links, etc.
- The corrected draft questionnaire is sent to each focal point for final approval.
- The validated questionnaire is used for analysis and scoring.

2) Scoring and analysis

- Scores associated with ternary responses to the validated questionnaire for each country are collated for analysis.
- Scoring methodology is applied to assign each country to the established tiers.
- Identification of findings from the GCI that provide insights into regional and world trends

3) Report development and publication

- A GCI report is drafted, reviewed and approved for publication.
- The GCI report becomes available to countries, stakeholders and members of the public.

Areas for further research

As part of the intrinsic review and analysis, ITU has identified areas for development and improvements. This includes refinements of questions to improve clarity and reduce ambiguity, as well as to enhance validity and reliability of measures.

Several areas were identified for further research, including:

 What are effective approaches for managing and conducting national cybersecurity audits?

- What are the most effective strategies for conducting cybersecurity awareness activities? Do these strategies differ based on the target group?
- How can the effectiveness of cyber development activities be evaluated in the short term?
- How can countries improve utilization of bilateral and multilateral cybersecurity agreements?
- What are the barriers to establishing and adopting effective cooperation measures, such as bilateral and multilateral cybersecurity agreements?
- How effective are government incentives at developing the cybersecurity industry?
- How effective are government incentives at driving cybersecurity research and development?
- Based on a country's level of digitalization, what activities are needed from CIRTs?

The GCI team hopes that researchers continue to explore these and other cybersecurity-related areas.

Office of the Director International Telecommunication Union (ITU) Telecommunication Development Bureau (BDT)

Place des Nations CH-1211 Geneva 20 Switzerland

bdtdirector@itu.int Email: +41 22 730 5035/5435 Tel.: Fax: +41 22 730 5484

Digital Networks and Society (DNS)

Email: bdt-dns@itu.int +41 22 730 5421 Tel.: Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication Union (ITU) Regional Office Gambia Road

Leghar Ethio Telecom Bldg. 3rd floor P.Ö. Box 60 005 Addis Ababa Ethiopia

Email: itu-ro-africa@itu.int +251 11 551 4977 Tel.: +251 11 551 4855 Tel: Tel.: +251 11 551 8328 Fax: +251 11 551 7299

Americas

Brazil

União Internacional de Telecomunicações (UIT) Escritório Regional

SAUS Quadra 6 Ed. Luis Eduardo Magalhães,

Bloco "E", 10° andar, Ala Sul

(Anatel)

CEP 70070-940 Brasilia - DF

Brazil

Email: itubrasilia@itu.int +55 61 2312 2730-1 Tel· +55 61 2312 2733-5 Tel.: Fax: +55 61 2312 2738

Arab States

Egypt

International Telecommunication Union (ITU) Regional Office Smart Village, Building B 147,

3rd floor Km 28 Cairo

Alexandria Desert Road Giza Governorate

Cairo Egypt

Email: itu-ro-arabstates@itu.int

+202 3537 1777 Tel.: +202 3537 1888 Fax:

Europe

Fmail:

Tel.:

+41 22 730 5467 Fax: +41 22 730 5484 Office of Deputy Director and Regional Presence Field Operations Coordination Department (DDR)

Place des Nations CH-1211 Geneva 20 Switzerland

Email: bdtdeputydir@itu.int +41 22 730 5131 Tel: Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)

Email: bdt-pdd@itu.int +41 22 730 5447 Tel.: +41 22 730 5484 Fax:

Senegal

Union internationale des télécommunications (UIT) Bureau de zone

Immeuble CAMPOST, 3e étage Boulevard du 20 mai Boîte postale 11017 Yaoundé Cameroon

Digital Knowledge Hub Department

bdt-dkh@itu.int

+41 22 730 5900

+41 22 730 5484

(DKH)

Email:

Tel.:

Fax:

Cameroon

Barbados

Email: itu-yaounde@itu.int + 237 22 22 9292 Tel.: + 237 22 22 9291 Tel.: Fax: + 237 22 22 9297

International Telecommunication

Union (ITU) Area Office

United Nations House

Hastings, Christ Church

Marine Gardens

P.O. Box 1047

Bridgetown

Barbados

Email:

Tel:

Fax:

Union internationale des télécommunications (UIT) Bureau de zone

8, Route du Méridien Président Immeuble Rokhaya, 3º étage Boîte postale 29471 Dakar - Yoff Senegal

Email: itu-dakar@itu.int Tel.: +221 33 859 7021 Tel: +221 33 868 6386 Fax:

Zimbabwe

International Telecommunication Union (ITU) Area Office USAF POTRAZ Building 877 Endeavour Crescent Mount Pleasant Business Park

Harare Zimbabwe

Email: itu-harare@itu.int +221 33 859 7010 +263 242 369015 Tel.: Tel: +263 242 369016

Chile

Unión Internacional de Telecomunicaciones (UIT) Oficina de Representación de Área

itusantiago@itu.int

+56 2 632 6134/6147

+56 2 632 6154

+62 21 380 2322

Merced 753, Piso 4 Santiago de Chile

Chile

Email:

Tel:

Fax:

Honduras

Unión Internacional de Telecomunicaciones (UIT) Oficina de Representación de Área

Colonia Altos de Miramontes Calle principal, Edificio No. 1583 Frente a Santos y Cía Apartado Postal 976 Tegucigalpa

Honduras

Email: itutegucigalpa@itu.int +504 2235 5470 Tel: +504 2235 5471 Fax:

Asia-Pacific

Thailand

International Telecommunication Union (ITU) Regional Office 4th floor NBTC Region 1 Building 101 Chaengwattana Road

itubridgetown@itu.int

itu-ro-asiapacific@itu.int

+66 2 574 9326 - 8

+66 2 575 0055

+1 246 431 0343

+1 246 437 7403

Laksi, Bangkok 10210, Thailand

Indonesia

Fmail:

Tel.:

International Telecommunication Union (ITU) Area Office Gedung Sapta Pesona

13th floor Jl. Merdeka Barat No. 17 Jakarta 10110 Indonesia

India

International Telecommunication Union (ITU) Area Office and Innovation Centre

C-DOT Campus Mandi Road Chhatarpur, Mehrauli New Delhi 110030

India

bdt-ao-jakarta@itu.int Fmail:

Area Office: Innovation Centre:

itu-ao-southasia@itu.int itu-ic-southasia@itu.int

Website:

ITU Innovation Centre in New Delhi, India

CIS

Russian Federation

International Telecommunication Union (ITU) Regional Office 4, Building 1

Sergiy Radonezhsky Str. Moscow 105120 Russian Federation

itu-ro-cis@itu.int Fmail: +7 495 926 6070 Tel.:

Switzerland

International Telecommunication Union (ITU) Office for Europe

Place des Nations CH-1211 Geneva 20 Switzerland

eurregion@itu.int Fmail: Tel.:

International Telecommunication Union

Telecommunication Development Bureau Place des Nations CH-1211 Geneva 20 Switzerland

ISBN: 978-92-61-38751-8

9 789261 387518

Published in Switzerland Geneva, 2024

Photo credit: Adobe Stock