Global Cybersecurity Index

Frequently Asked Questions

Last updated: 25 June 2021

Contact: gci@itu.int

Contents

General Questions

Question	Answer
What is the goal of the Global Cybersecurity Index?	The Global Cybersecurity Index aims to raise awareness of country-level commitments on cybersecurity, to identify strengths and areas for improvement, and share current cybersecurity practices. The Global Cybersecurity Index measures countries' cybersecurity commitments across five (5) pillars: • Legal Measures • Technical Measures • Organizational Measures • Capacity Development Measures • Cooperation Measures
What does the Global Cybersecurity Index measure?	The Global Cybersecurity Index measures actions taken by countries in terms of cybersecurity to tackle cyber risks challenges through assessing commitment in the five pillars of Legal, Technical, Cooperative, Organizational, and Capacity Building Measures.
What is the link between Global Cybersecurity Agenda and Global Cybersecurity Index?	The Global Cybersecurity Index was first released in 2015, based on the five strategic pillars of the 2007 Global Cybersecurity Agenda as a framework for measuring cybersecurity. The Global Cybersecurity Agenda was designed "for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating effort." More information about the GCA can be found on its website.
Why is the Global Cybersecurity Index important?	The Global Cybersecurity Index provides a complement to other measures related to cybersecurity by enabling countries to identify where action has been taken, what action may be insufficient, and understand the landscape of successes. Cybersecurity is a multidimensional and cross-border challenge, for which measures on the number of cyberattacks/vulnerabilities does not necessarily reflect the efforts taken by countries, organizations, or individuals to protect their cybersecurity. The Global Cybersecurity

<table>
<tr><td></td><td>Index helps determines the global effort taken by countries to ensure a secure cyber space for all.</td></tr>
<tr><td><b>Is this the fourth iteration or edition?</b></td><td>Both terms are acceptable. Early in the process, we referred to it as the fourth iteration of the Global Cybersecurity Index, or GCI version 4. Going forward, we are referring to it as the fourth edition of the Global Cybersecurity Index, or Global Cybersecurity Index 2020.</td></tr>
<tr><td><b>What does GCI, GCIv4, GCIe4 and other similar abbreviations mean?</b></td><td>
<table>
<tr><th>Abbreviation</th><th>Description</th></tr>
<tr><td>GCI</td><td>Global Cybersecurity Index</td></tr>
<tr><td>GCIv4, GCIe4, GCI2020</td><td>The fourth edition of the Global Cybersecurity Index</td></tr>
<tr><td>GCIv3, GCI2018</td><td>The third iteration of the Global Cybersecurity Index</td></tr>
<tr><td>GCIv2</td><td>The second iteration of the Global Cybersecurity Index</td></tr>
<tr><td>GCIv1</td><td>The first iteration of the Global Cybersecurity Index</td></tr>
</table>
</td></tr>
</table>

Country Participation

<table>
<tr><th>Question</th><th colspan="5">Answer</th></tr>
<tr><td><b>Who can participate in the GCI survey/Questionnaire?</b></td><td colspan="5">ITU Member States and the State of Palestine, are invited to nominate focal points, who can respond to the GCI questionnaire.</td></tr>
<tr><td><b>Who can participate in the methodological processes of the GCI?</b></td><td colspan="5">The Global Cybersecurity Index takes a multistakeholder approach and engages governments, private industry, civil society, and academia.

Governments, private industry, civil society, and academia contribute to methodological discussions, such as weightage recommendations and questions to be included.</td></tr>
<tr><td rowspan="5"><b>How many countries have nominated focal points and submitted questionnaire in this and previous GCI iterations?</b></td><td></td><td><b>GCIv1</b></td><td><b>GCIv2</b></td><td><b>GCIv3</b></td><td><b>GCIe4</b></td></tr>
<tr><td><b>Countries nominating focal point</b></td><td>105</td><td>136</td><td>155</td><td>169</td></tr>
<tr><td><b>Questionnaires submitted</b></td><td>99</td><td>136</td><td>120</td><td>150</td></tr>
<tr><td><b>Data collection years</b></td><td>2013-2014</td><td>2016</td><td>2017-2018</td><td>2020</td></tr>
<tr><td><b>Publishing year</b></td><td>2015</td><td>2017</td><td>2019</td><td>2021</td></tr>
<tr><td><b>How many countries participated in GCIe4?</b></td><td colspan="5">169 countries provided a focal point for the fourth edition of the Global Cybersecurity Index, and 150 countries submitted questionnaires. For countries that did not submit responses to the questionnaire, desk research was carried out by the Global Cybersecurity Index team, and submitted to the respective country to input. If no input was given, the desk research was used to calculate scores.</td></tr>
<tr><td><b>How were country focal points appointed?</b>

<b>How did countries participate?</b></td><td colspan="5">Through their ITU point of contact, countries were invited to designate a focal point to respond to the Global Cybersecurity Index questionnaire beginning in January 2020. Countries, facilitated by their focal points, were also able to respond to the verified questionnaires and validate the final Global Cybersecurity Index assessment.</td></tr>
</table>

Questions about country scores and ranks

Question	Answer
What does a high Global Cybersecurity Index score indicate?	A higher score in the Global Cybersecurity Index indicates that a country has put in place more measures as measured by the GCI to strengthen its cybersecurity posture across the five pillars: Legal, Technical, Cooperative, Organizational, and Capacity Building Measures. It does not indicate that a country has fewer cybersecurity attacks. For example, a correct statement would be: "A country that scores high in the GCI has more measures as measured by the GCI to addressing cybersecurity." **Incorrect**: "A country that scores high in the GCI is more cybersecure." **Correct**: Countries may have other indicators not measured in the GCI. Thus, a country may not perform well in the GCI, but perform quite well in other indices that measure other actions. **Scores and ranking do not indicate how cybersecure a country is or how effective measures are.**
How do we score and weigh countries? **How were weights assigned?**	The Global Cybersecurity Index is a composite index based on weighted answers. To each question, countries are scored with a full (1), partial (0.5), or no (0) point based on the evidence submitted to support their responses to the questionnaire. These scores are combined using a weighted average. Each micro-indicator, sub-indicator, and indicator are aggregated based on a weighted average. **Weights are based on the average of expert weightage submissions.** **More information about the expert group process can be found on the GCI webpage.**
Who was eligible to participate in the weightage process? **What was the demographic makeup of weightage experts?**	All ITU-D Members were invited to nominate weightage experts (English, عربي, 中文, Español , Français, Русский) . Previous weightage experts who had contributed to the GCI were invited to participate again. The total size of the weightage group was expanded from 40 to 88 people.

	The weightage group included approximately: • 9% Academia • 7% Civil Society • 79% Government (including regulatory agencies) • 3% International Organizations • 2% Private Sector NB: Some individuals had multiple affiliations. Only primary affiliation was used in this calculation. By region: • 9% Africa • 13.6% Americas • 13.6% Arab Countries • 28% Asia Pacific • 4.5% CIS • 18% Europe • 12.5% Academia/International Organizations NB: Some individuals operated across regions. Only primary region was used in this calculation, and academia/international organizations were excluded
How are rankings assigned?	Ranks are assigned using dense ranking distribution, where countries with the same score receive the same rank, and the country with the next, lower score receiving the next numerical value as their rank. (For example. 1, 1, 2, 3, 4, 4, 5)
What if two or more countries have the same score, how are they placed in ranking list?	It is not uncommon for two or more countries to score the same. Countries that score the same receive the same rank and are listed alphabetically.
Do you have country/regional rankings by pillar?	Pillar rankings can be derived from the data from the ITU Global Cybersecurity Index website or are available upon request.
What factors can explain why a country ranks higher or lower in this	Country ranks are highly sensitive to small changes in scores. This sensitivity should be taken into consideration in any rank-based analysis.

edition compared to previous editions?	Country scores are influenced by: • Changes in countries' cybersecurity measures • Changes to questions that include deletion and addition of new questions in the Global Cybersecurity Index • Changes to weightages within the Global Cybersecurity Index • Country's participation: Data collected without the country support may affect a country's ranking. Depending on country scores and the relative changes of an individual countries versus others, a country may have risen or declined in ranks. It is possible for a country to improve their score but decline in rankings due to the relative greater increase in scores by other countries.
A country provided more than one supporting documents to a question in the GCIe4 questionnaire, does that improve their score?	For GCIe4, a minimum of one supporting document, such as a text (e.g. MS Word, pdf etc.), website link, video, or photo/image, was required to achieve the maximum full marks/score for an indicator. Additional documentation does not change this. We always appreciate additional documentation and context and refer to it for best practices in reports or other documents.
Where can I find information on a specific country?	Country profiles, including pillar scores, are available through the ITU Global Cybersecurity Index website.

Questionnaire specific questions

Question	Answer
How were the 5 pillars of the GCI chosen? Aren't there any more pillars that might offer a wider perspective?	Cybersecurity is a multidimensional field. The Global Cybersecurity Index pillars were derived from the Global Cybersecurity Agenda, a framework for international cooperation aimed at enhancing confidence and security in the information society. There are a number of additional cybersecurity measures produced by other organizations that can complement the Global Cybersecurity Index and provide a broader perspective. Complementing the Global Cybersecurity Index with other indices should always be done with careful consideration of compatibility of methodologies and data limitations.
Why have questions changed from the previous edition? **Will the same questions asked in the next edition of the GCI?**	Questions change between editions of the Global Cybersecurity Index to reflect changes in cybersecurity practices and priorities. While this makes the Index not as easily compared from one edition to the next, it enables a more accurate snapshot of cybersecurity measures taken by countries. The next edition of the GCI may feature new or different questions. All changes will be approved by the Study Group 2, Question 3 before countries are invited to respond.
What are the processes in validating supporting evidence provided by countries? **Can other countries give input on a country's scoring or documentation?**	The GCI team verifies evidence provided by the country through reviewing links and documents to ensure that the proof is relevant to the corresponding questions asked. A country's response is checked by two different validators then the validated responses are returned to the country's focal point for final review and approval of the validated answers. In the absence of supporting documentation, the question does not receive any points.

	Documentation and revisions are only accepted by the relevant country: no country can submit or dispute the documentation or scoring of another country as country's documents are confidential
How are indicators, sub-indicators, and micro-indicators determined?	Indicators, sub-indicators, and micro-indicators are developed based on: • Expert recommendations • Study Group amendments
Are the Global Cybersecurity Index questions mutually exclusive?	No, GCI measures are not MECE (Mutually Exclusive, Completely Exhaustive), but instead can be thought of as ICE (Independently Completely Exhaustive)
Legal Measures: Is the efficacy of cybersecurity legislation measured in this questionnaire?	Legal Measures gauge the presence of legislation, regulations, and other rules relevant to cybersecurity. It does not assess the impact of the legislation, regulations, and other rules, or their direct impact on cybersecurity. How the law or regulation is applied is not measured in the GCI.
Technical Measures: What is the difference between a sectorial CERT/CIRT/CSIRT and a national CERT/CIRT/CSIRT? (Technical questions 2.1, 2.2, 2.2.1, 2.2.2 and 2.2.3)	A sectorial CIRT are CERTs/CSIRTs designed by the government for digital security monitoring specific sectors, such as the health, finance, education sectors, and any other national critical infrastructure. We can consider the CERT that belongs to private business and provides its services to the government. A Computer Incident Response Team, also known as CSIRT / CERT, is a specific agency/organizational entity responsible for coordinating and supporting responses to computer security incidents or incidents at the national level.
Capacity Development Measures: What kind of awareness campaigns have been accepted for the purpose of this questionnaire?	Any type of awareness campaign that seeks to improve cybersecurity related behaviors in specific target groups, conducted through social media, television, radio, print media, or other, were accepted as part of this edition of the Global Cybersecurity Index.
Cooperation Measures: Is ITU Membership sufficient to get full point for "International Cooperation" section?	No, international cooperation activities other than ITU Membership are used to evaluate the "International Cooperation" section.

Cooperative Measures: What is the difference between an International mechanism and a Multilateral agreement?	Multilateral Agreements – For GCI purposes, Multilateral Agreements refers to any officially recognized national or sector-specific program for cross-border sharing of cybersecurity information or assets by governments with multiple foreign governments such as an agreement with more than two countries that excludes them from being part of an organizational cooperation such as the African Union or the Budapest Convention. Participation in International Mechanisms (forums) - May include ratification of international agreements regarding cybersecurity, such as African Union Convention on Cyber Security and Personal Data Protection, Budapest Convention on Cybercrime and others.
Where is the original Questionnaire available?	The Questionnaire is available in the six UN languages at https://www.itu.int/gci, and as an appendix in the GCI report.

Confidentiality of Responses

Question	Answer
How does the ITU treat confidential/internal drafts/documents shared by countries?	All supporting documentation provided by countries are treated as confidential, and are not shared by the ITU with third parties.
Can other countries get access to scores and ranking of my country?	Scores and associated rankings are publicly accessible via the ITU website.
Can I have access to documentations ' submitted by other countries to support their questionnaire responses?	Countries' documentation submitted to the ITU to support their questionnaire responses cannot be shared outside of the ITU Global Cybersecurity team and their consultants.

Taking action

Question	Answer
How can a country improve their ranking?	Countries can improve their positions in future editions of the Global Cybersecurity Index through enacting measures and practices that fulfil the various indicators within the index and working with the ITU to ensure that data collected for the GCI is complete and accurate. Countries cannot improve their position in current or previous GCI editions.
How can countries improve their Global Cybersecurity Index scores?	Countries can improve the Cybersecurity Index scores through addressing current areas in which they underperform in the Index.
Does the ITU provide support to help countries improve their GCI scores?	The ITU supports countries who wish to improve their cybersecurity performance in the Global Cybersecurity Index (GCI) through: • Support of drafting new or updated National Cybersecurity Strategies

	• CyberDrills • Establishments and improvement of national CIRTs
How can I give input in the next edition of the Global Cybersecurity Index?	ITU Members are encouraged to provide input through their focal points. Each country respective focal point coordinates with the GCI Team to ensure all necessary checks are conducted. Other queries on providing input can be sent to the GCI Team at gci@itu.int .

Other questions

Question	Answer
I have a question that has not been answered in this FAQ.	Contact us at gci@itu.int with additional questions.
We provided all information and supporting documents, can we get scores and ranks prior the Report launch?	Scores and ranks will be released concurrently at the point of report launch.
What is your privacy policy on reproducing this document elsewhere or using some of the data presented?	Media outlets can use the Global Cybersecurity Index with no specific authorization from ITU provided that ITU is acknowledged as the source. Researchers can use content of the GCI report that is publicly available as long as ITU is referenced in the section cited.
How should the Global Cybersecurity Index be cited?	APA style: *Global Cybersecurity Index, 4th edition*. (2021) International Telecommunication Union (ITU). https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI/GCIv4-Report-Launch.aspx Chicago: International Telecommunication Union (ITU). *Global Cybersecurity Index, 4th edition*. Geneva: International Telecommunications Union. June, 2021. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.