ITU Publications

International Telecommunication Union
Development Sector

Global Cybersecurity Index

2020

Global Cybersecurity Index 2020

Measuring commitment to cybersecurity

Acknowledgements

The Global Cybersecurity Index (GCI) is an initiative of the International Telecommunication Union (ITU), the UN specialized agency for ICTs, shaped, and improved by the work of a diverse range of experts and contributors within countries and other international organizations. ITU would like to acknowledge and thank all partners and contributors for their hard work and commitment in providing support to the GCI, and more importantly, helping to advance our collective understanding of cybersecurity commitments.

ITU would like to especially highlight the contributions received through ITU-D Study Group 2, and the Telecommunication Development Bureau (BDT) Management Consultation Group, and their work on changes to the GCI questionnaire. The BDT Cybersecurity team would like to thank ITU membership for their nominations of experts to advise in the weightage process. More information about the weightage process and expert participation can be found in the methodology. The inputs of the following experts from ITU membership provided invaluable support in assigning weighting determinations:

Prof. Dr. Marco Gercke (Cybercrime Research Institute GmbH, Germany), Ms Melissa Hathaway (The Potomac Institute for Policy Studies, United States of America), Mr Scott James Shackelford (Indiana University, Program on Cybersecurity and Internet Governance, United States of America), Mr Gueric Goncalves (ANNSI, Benin), Pr. Eng Emmanuel Thekiso (BOCRA, Botswana), Mr Dlamini (Ministry of ICT, Eswatini), Mr Fillemon Johannes (Ministry of Information and Communication Technology, Namibia), Mr Palakiyem ASSIH (Cyber Defense Africa S.A.S., Togo), Mr Nawa J. Samatebele (Zambia Information & Communication Technology Authority, Zambia), Mr Gonzalo Díaz de Valdés Olavarrieta (Chile), Ms Jessica Machado Álvarez (Administration of Cuba, Cuba), Eng. Raquel Piña (Venezuela), Mtro. Jacobo Bello Joya (The National Guard of the Secretariat of Security and Citizen Protection, Mexico), Ms Gladys Ocampos (Statistics, Surveys and Censuses (DGEEC) of Paraguay, Paraguay), Ms María Teresa Chica (Statistics, Surveys and Censuses (DGEEC) of Paraguay, Paraguay), Mr Renzo Zegarra (Ministerio de Transportes y Comunicaciones, Peru), Mr Junior McIntyre (The Caribbean Telecommunications Union (CTU), Trinidad and Tobago), Mr Fernando Hernadez (The Uruguayan Communications Regulator, Uruguay), Ms Anne-Rachel Inné (American Registry for Internet Numbers (ARIN), United States of America), Mr Mohammad Odeh Alsalamin (Jordan), Ms Nada Khater (Ministry of Digital Economy and Entrepreneurship, Jordan), Mr Yusuf Ahmed Buhijji (Ministry of Transport and Communication, Kingdom of Bahrain), Mrs Aziza Al Rashdi (Ministry of Transport, Communication and information Technology, Oman), Mr Abdulrahman AlHassan (Communications and Information Technology Commission (CITC, Saudi Arabia), Eng. Mohammad Alawi (Ministry of Telecomm. & Information Technology, State of Palestine), Mr Khalili Urahman Kabirzoy (Afghanistan Root Certification Authority(ARCA), Afghanistan), Mr Nasratullah Ghafoory (Afghanistan Root Certification Authority(ARCA), Afghanistan), Ms Xu Ming (Ministry of information and Technology, National Computer Network Emergency Response Team, China), Ms Wan Xinxin (Ministry of Information and Technology, National Computer Network Emergency Response Team, China), Ms Catherine M. Subhyadas(Department of Communications, Fiji), Puan Lyana Shohaimay (Ministry of Communications and Multimedia, Malaysia), Puan Nurul Adiah Hani Husin (Ministry of Communications and Multimedia, Malaysia), Mr Yan Naung Soe (National Cyber Security Center, Information Technology and Cyber Security Department, Myanmar), Mr Jakkrapong Chavong (Ministry of Digital Economy and Society, Thailand), Mr Alan Olegovich Khubaev (Department of Information Security, Russia), Mr Andrey Sergeevich Zhivov (Department for International Cooperation, Russia), Mr Ilgyz Turganbaev (State Committee of Information Technologies and Communications of the Kyrgyz Republic, Kyrgyz Republic), Mr Muhamedjan Alymkulov (State Committee of Information Technologies and Communications of the Kyrgyz Republic, Kyrgyz Republic), Mr Vladimir Yuryevich Shurin (Department of Information Security

of the Security Service of the Republican Unitary Enterprise, Belarus), Mr Nestoras Chouliaras (General Secretariat of Telecommunications & Post Ministry of Digital Governance, Greece), Ms Eglė Vasiliauskaitė (Ministry of National Defence of the Republic of Lithuania, Lithuania), Mr Tadas Šakūnas (Ministry of National Defence of the Republic of Lithuania, Lithuania), Mrs Radoja (Serbia), Mr Matej Šalmík (National Cyber Security Centre SK-CERT, Slovakia), Mr Rastislav Janota (National Cyber Security Centre SK-CERT, Slovakia), Mr Aidan Murchland (United Kingdom), Mr Miguel Pinto (BitSight, United States of America), Mrs Nunil Pantjawati (Indonesia), Mrs Intan Rahayu (Indonesia), Mr Makaireh JONGA (Gambia Computer Security & Incident Response Team (gmCSIRT), Gambia), Ms Banchale Gufu (Kenya), Ms Sonam Choki(Department of Information Technology and Telecom, Bhutan), Aqeel Taha Saadoon (ICT SECRETARIAT, Iraq), and Thar Kadhim Ali (CERTIraq, Iraq).

The ITU Cybersecurity team would like to thank the GCI focal points, who collected data from across their respective countries regarding cybersecurity commitments. This report would not have been possible without the GCI country focal points.

The team is grateful to the many ITU colleagues and interns that provided support to this report.

The team apologizes to any individuals or organizations inadvertently omitted from this list and expresses its gratitude to all who contributed to the GCI.

Please contact the ITU Cybersecurity team at gci@itu.int with any comments or inquiries in respect to this publication.

Disclaimer

ISBN:

978-92-61-33921-0 (Electronic version)
978-92-61-33931-9 (EPUB version)
978-92-61-33941-8 (Mobi version)

Foreword

The need for a safe and secure cyberspace has become more important than ever, especially as we all grow increasingly dependent on "digital lifelines". One of the greatest challenges of the COVID-19 pandemic has been finding ways to meaningfully connect with each other, despite uncertainty, anxiety, and change. Even prior to the pandemic, cybersecurity was essential to keeping us safe online so that we could carry out critical day-to-day functions.

I am inspired by people's ability to adapt to this uncertain environment, and their use of technology to find creative solutions. Many organizations, including the International Telecommunication Union, have grappled with new challenges stemming from remote work. Cybersecurity is fundamentally intertwined with remote work, from managing video call participants, to making sure that documents are shared safely. ITU has therefore continued to work together with countries to be more efficient, more active, and deliver impact in the areas where we are needed the most.

When the Global Cybersecurity Index was first launched in 2015, few people could have imagined the situation that we currently find ourselves in. This latest iteration of the Global Cybersecurity Index will help promote further action towards secure digital ecosystems needed for recovery and growth, by measuring the types of cybersecurity commitments countries have made and their prevalence.

This iteration reveals that many countries are making progress in their commitments to responding to cybersecurity challenges, despite opportunistic actors that have taken advantage of our desire for information, our fears about the pandemic, shift to working from home and remote learning, dependence on healthcare systems, and more.

The Global Cybersecurity Index report shows that many countries enacted new cybersecurity legislation and regulations to address areas such as privacy, unauthorized access, and online safety. It also emphasizes the need to establish strategies and mechanisms to build capacity and help governments and businesses better prepare for and mitigate growing cyber risks. More than half of the world's countries now have a computer incident response team (CIRT) and almost two-thirds have some form of a national cybersecurity strategy guiding their overall cybersecurity posture.

The Global Cybersecurity Index reveals that cybersecurity is truly a developmental issue, and that there is an urgent need to address the growing cybercapacity gap between developed and developing countries by fostering knowledge, upskilling, and building competencies. We need to close this gap by going to the roots and building capacity in terms of digital infrastructure, digital skills, and resources in the developing world.

I hope the Global Cybersecurity Index will continue to be a useful capacity development tool to governments, policy makers, cybersecurity experts and academia in identifying areas for improvement and highlighting best practices for strengthening national cybersecurity.

I would like to thank countries for their valuable engagement and contribution to this effort, especially for their involvement during the development, data collection, and validation of this iteration of the Index. I would also like to thank all of those involved in the study group process for their support and direction. I invite all ITU Member States to continue updating us on their progress on cybersecurity related commitments, so that we can effectively share experiences, research, and solutions to create a trusted cyberspace for all.

Doreen Bogdan-Martin
Director, ITU Telecommunication Development Bureau

Executive summary

The Global Cybersecurity Index (GCI) was first launched in 2015 by the International Telecommunication Union (ITU) to measure the commitment of 193 ITU Member States and the State of Palestine[1] to cybersecurity to help them identify areas of improvement and encourage countries to take action, through raising awareness on the state of cybersecurity worldwide. As cybersecurity risks, priorities, and resources evolve, the GCI has also adapted to give a more accurate snapshot of cybersecurity measures taken by countries.

This report aims to better understand countries' commitments to cybersecurity, identify gaps, encourage the incorporation of good practices, and provide useful insights for countries to improve their cybersecurity postures.

Countries have reported using the GCI to facilitate:

- discussions through formally established forums that enable self-assessments and better coordination;
- gathering insights about overall national initiatives and resources used to manage cybersecurity at the national level;
- benchmarking against good practices, partners, and regional neighbours;
- awareness raising among various stakeholders on coordination needs at a national level.

The GCI results show overall improvement and strengthening of all five pillars of the cybersecurity agenda, but that regional gaps in cybercapacity persist. Illustrative practices by countries have been highlighted in the report.

Countries Measured	Collection Year	Focal Points from Countries	Submitted Questionnaires	Median Overall Score Growth since 2018
194	**2020**	**169**	**150**	**9.5%**

The Index maps 82 questions on Member State cybersecurity commitments across five pillars:

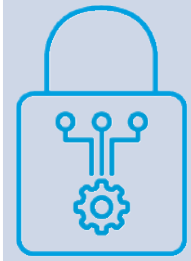
- legal measures;
- technical measures;
- organizational measures;
- capacity development measures;
- cooperation measures.

[1] The State of Palestine participates in ITU work under Resolution 99 (Rev. Dubai, 2018) of the Plenipotentiary Conference.

The table below shows global commitments of specific indicators per pillar.

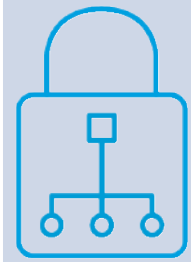
Legal

Measuring the laws and regulations on cybercrime and cybersecurity	167	Countries with some form of cybersecurity legislation
	133	Data Protection Regulations
	97	Critical Infrastructure regulations



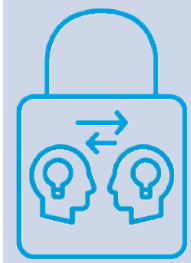
Technical

Measuring the implementation of technical capabilities through national and sector-specific agencies	131	Active CIRTs
	104	Engaged in a regional CIRT
	101	Child Online Protection Reporting mechanisms



Organizational

Measuring the national strategies and organizations implementing cybersecurity	127	National Cybersecurity Strategies
	136	Cybersecurity Agencies
	86	Child Online Protection strategies and initiatives reported



Capacity development

Measuring awareness campaigns, training, education, and incentives for cybersecurity capacity development	142	Countries conduct cyber-awareness initiatives
	94	Countries with cybersecurity R&D programs
	98	Countries reported having national cybersecurity industries

Cooperation

Measuring partnerships between agencies, firms, and countries	166	Countries engaged in cybersecurity Public-Private Partnerships
	90	Countries with cybersecurity bilateral agreements
	112	Countries with cybersecurity multilateral agreements

Changes to the Global Cybersecurity Index impacting scores

- This edition of the Global Cybersecurity Index is based on data reported by a record level of Member State participation, from 105 responses in the 2013-2014 iteration, to 150 questionnaires returned in 2020.
- The GCI questionnaire has been updated. Questions have been re-defined, added, or removed in each of the five pillars (legal, technical, organizational, capacity development and cooperative measures) to reflect changes in cybersecurity security concerns and efforts. Changes to the questionnaire have an impact results, with these changes being one factor in country scores and rankings.
- Weightages differ from the previous iterations, reflecting, in part, changes in structure of questions as well as the addition and removal of questions.
- Weightages for indicators were based on expert recommendations. ITU membership nominated experts to advise in the weightage process to allocate weights to indicators based on relative importance to cybersecurity. Variations in weightage allocation can impact country scores and rankings.
- A section has been prepared to give more information about the construction, composition, and recent changes to the GCI questionnaire (Annex A).
- Many countries, especially top performing countries, are increasingly close in terms of score, which is why individual ranks should be carefully interpreted.
- Some countries declined to verify collected data or participate in this edition of the Global Cybersecurity Index. Data regarding these countries (marked with an *) should not be taken as officially endorsed by any representative on behalf of that country. As those data were collected through online research, missing elements needed to be interpreted as not found instead of as non-existent.

In addition, country participation may have positively impacted scores in some cases, as the more a country contributes to the questionnaire, the more likely affirmative responses will be found.

There are many areas in which countries excel, and areas where there is scope to strengthen efforts, and countries should be discouraged from focusing on rankings.

For countries that did not submit responses to the questionnaire, desk research was conducted through publicly available information on official websites and other resources. For countries for which desk research was undertaken, collected data may not accurately reflect the cybersecurity posture of the country. The GCI does not contain estimated data.

Table of contents

List of tables and figures

Tables

Figures

1. Global Cybersecurity Index: Background and context

The fourth iteration of the Global Cybersecurity Index (GCI) comes at a very different time than its predecessors. When the Global Cybersecurity Agenda was first launched in 2007, the first iPhone was still a month away from release and Facebook had only been open to users outside universities in the United States for a year. A billion people were online, and there were concerns that the amount of data created, 255 exabytes, would exceed available storage.[1] Today, smartphones have reshaped daily life, and social media has become embedded across a larger sphere of society. Currently, 3.5 billion people are online and the digital world is estimated to be 44 zettabytes, with no risk of unavailable storage thanks to cloud computing.[2] In addition, ICT proliferation has affected the broader national ecosystem giving life to new organizational possibilities, such as e-government services, and new economic and productive paradigms such as Industry 4.0 and the broader digital economy.

All countries are affected to some extent by the digital divide, and as a key enabler of the economy, society, and government, which rely on digital systems, cybersecurity should be a high priority.

The COVID-19 pandemic has dramatically affected how societies operate. As the pandemic began to take hold in April 2020, Akamai noted Internet traffic increased by 30 per cent.[3] From telecommuting to remote learning, technology has played a key role in keeping people connected. For the digital age to realize its potential, a trusted and safe cyberspace must be key. A year after COVID-19 was declared a pandemic by the World Health Organization, and the development of new management systems and vaccinations, our reliance on digital technologies continues to grow. And as the world connects the unconnected, a safe and trustworthy cyberspace must be ensured.

There is an increased recognition of cybersecurity risk.[4] The ongoing pandemic has created distrust, especially online. The data collected in the GCI is the start of a broader conversation about cybersecurity, around which local context and observations are critical in shaping a way forward.

To help create a trusted and safe cyberspace in the aftermath of the pandemic, the GCI can be a jumping point to understand how the pandemic has impacted cybersecurity efforts, and how countries are working to address cybersecurity and trust. For example, some countries reported delays with the approval and entry into force of laws, the implementation or improvement of CIRTs, the development or the revision of the national cybersecurity strategies, and the delivery of capacity development efforts. Even cooperative agreements no longer benefitted from in-person interaction and collaboration.

---

1 http://core.xsomo.com.jm/images/web/File/white%20papaers/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf
2 https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/
3 https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html
4 http://reports.weforum.org/global-risks-report-2020/executive-summary/

It is important for governments to take stock of what policies and practices are in place regarding cybersecurity as the world continues to change. As cybersecurity has evolved and adapted, so has the way it is measured. The GCI has updated questions on the role of CIRTs, cooperative agreements, organizational frameworks, and public awareness. While these changes make the GCI less comparable over time, this iteration more accurately reflects the current commitments by countries.

2. Key themes

2.1 Legal measures: Planning for future interventions

Many challenges today erode online trust and prevent the digital society from operating at its full potential. For example, global losses due to cybercrime are estimated from as low as USD 1 trillion in 2020,[5] to as high as USD 6 trillion in 2021.[6] The development of a legal and regulatory framework to protect society and promote a safe and secure digital environment is key and should be at the outset of any national efforts in cybersecurity.

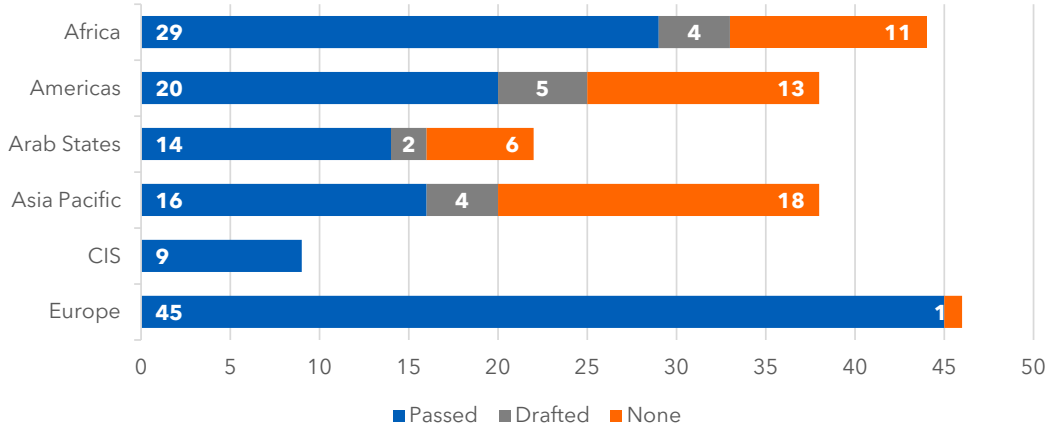
Legal and regulatory frameworks include the establishment of legislation identifying what constitutes illicit activities in cyberspace, together with the definition of the necessary procedural tools to investigate, prosecute and enforce such legislation; the establishment of cybersecurity baselines and compliance mechanisms for a set of national stakeholders; and procedures to ensure consistency with international obligations.

The fourth edition of the Global Cybersecurity Index takes stock of cybersecurity interventions within a country's legal framework through measuring the presence of:

- basic requirements that public and private stakeholders must uphold;
- legal instruments prohibiting harmful actions.

Data protection

Figure 1: Countries with data protection legislation



Source: ITU

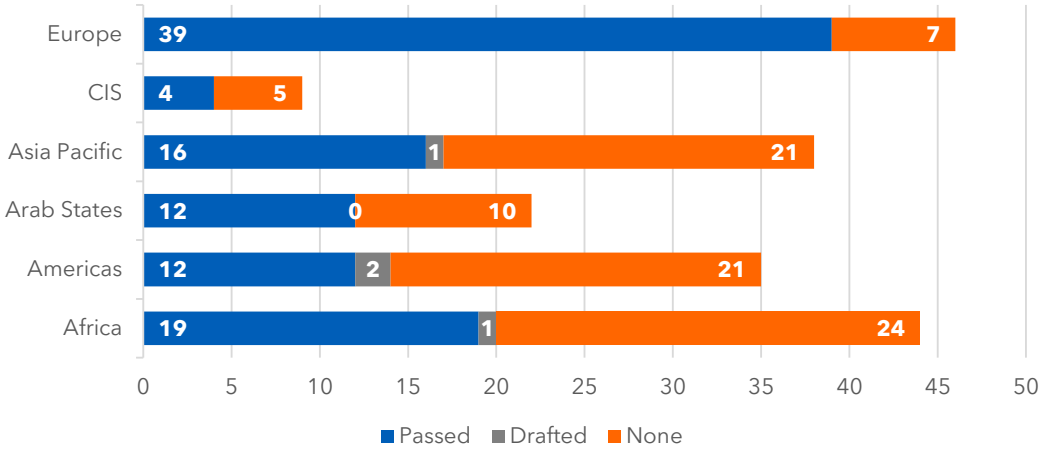
Data protection legislation may take the form of regulation that could, for example, compel an organization to disclose a cybersecurity breach or establish yearly audit requirements.

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[6] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

On the surface, privacy advocates may note that a significant number of countries that already have data protection and privacy regulations in place have worked to update them. In addition, 133 countries have signed protection and privacy regulations into law, 15 are in the drafting process, and 46 have no regulation in place. Many countries with existing regulation have made updates to their legislation to reflect new agreements and norms.

Since the last iteration, more countries have implemented measures requiring breach notifications. In this edition, 102 countries have introduced data breach and incident notification requirements in legislation and policies.

Figure 2: Countries with breach notification measures

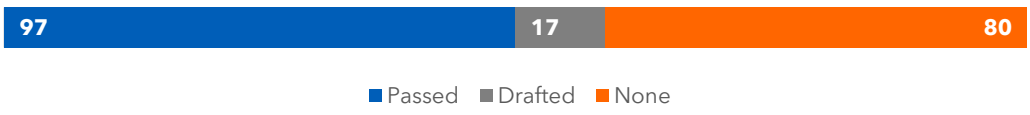


Source: ITU

Online identity and data theft

While countries have acted on illegal access, online identity and data theft legislation still lacks attention, yet online identity protection is significantly important especially with the current shift to the digital environment. The world's population has shifted online through social media and work practices, which needs considerable security as a stolen identity can compromise everyday life both privately and professionally.

Figure 3: Countries with legislation on the theft of personal information

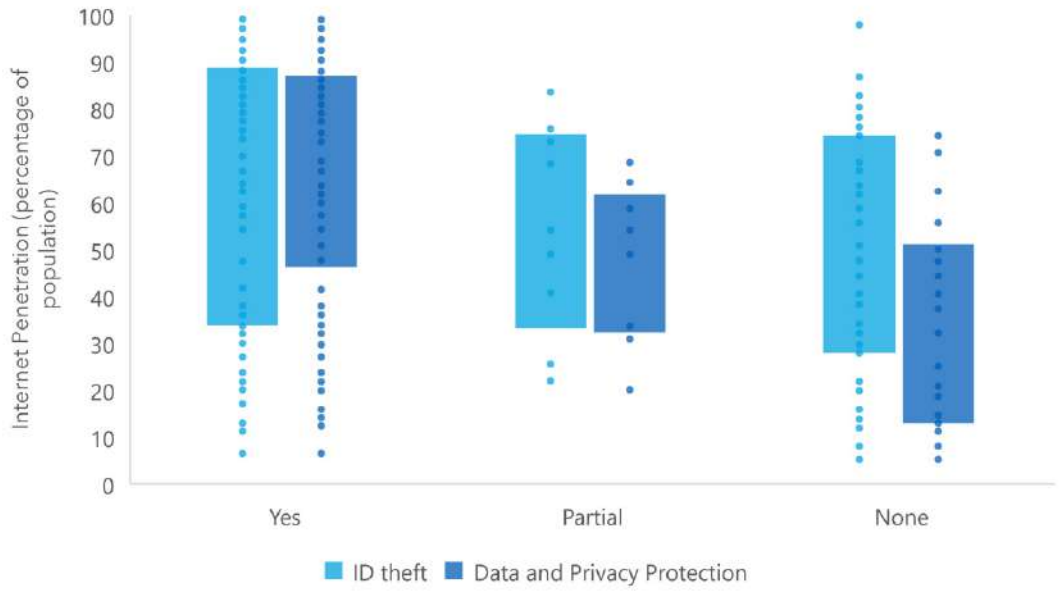


Source: ITU

As seen in Figure 4, when looking at median and average Internet penetration, countries with high Internet penetration are slightly more likely to have online data protection law or regulation than countries with low Internet penetration. By contrast, data and privacy protection regulation is more likely to be found in countries with high Internet penetration. These trends reflect, in part, economic conditions, overall development, and government digitalization strategies. It is

noteworthy that some countries have prepared for greater Internet penetration by proactively instituting legislation related to identity theft and data and privacy protection.

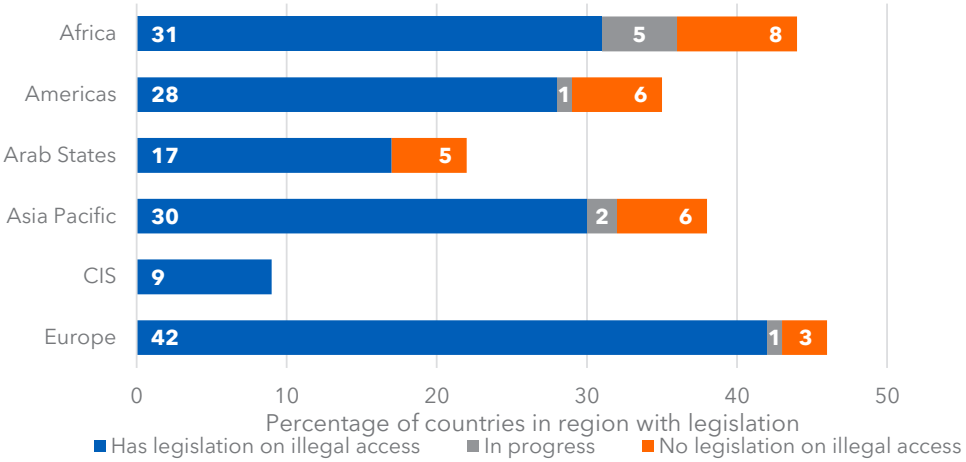
Figure 4: Legislation on identity theft and data and privacy protection, plotted over Internet Access (% of population)



Source: ITU World Telecommunication/ICT Indicators Database

As shown in Figure 5, most countries have legislation on illegal access, with few significant differences across regions.

Figure 5: Legislation on illegal access



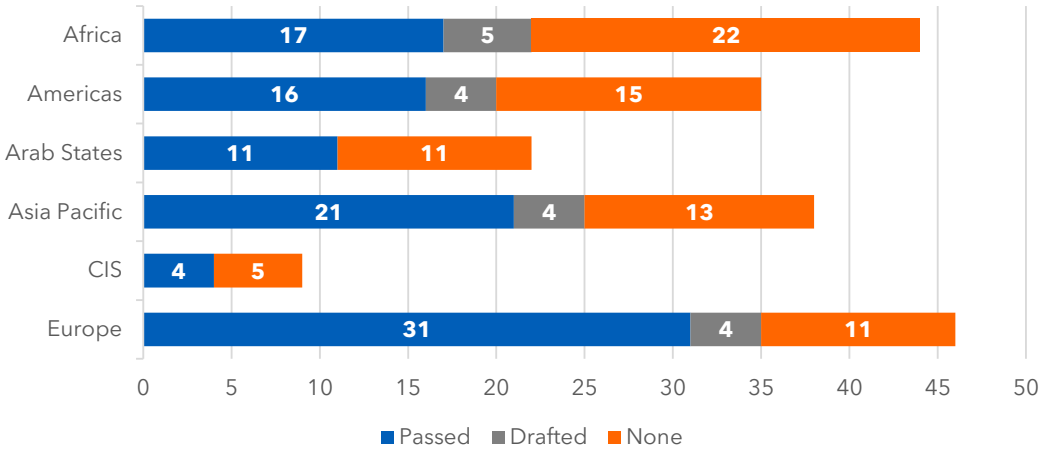
Source: ITU World Telecommunication/ICT Indicators Database

Online antisocial behaviour

Online antisocial behaviour is an ongoing challenge for which countries are increasing legislative support. The GCI measures two aspects: online harassment, and online racism and xenophobia.

Online harassment remains a persistent problem: in the United States of America in 2020, "41% of Americans have personally experienced some form of online harassment"[7] and at least 1 in 10 women in the European Union have faced online harassment.[8] In a survey of adults in 32 countries, one in five adults reported experiencing online hate speech.[9]

Figure 6: Countries with online harassment legislation



Source: ITU World Telecommunication/ICT Indicators Database

Globally, 100 countries have adopted legislation criminalizing instances of online harassment and abuse, 17 are in the process of drafting and implementing these measures and 77 have no legislation on the subject. However, what constitutes abuse is often ill defined.

Efforts to address online racism and xenophobia face barriers around clarity, but a significant number of countries are in the process of drafting some form of legislation in this direction. Several countries are extending or adapting offline laws on racism and xenophobia to online context. The threshold for what constitutes an offence varies greatly, for what may be legal in one country may constitute a punishable offense in another. However, some countries have decided to write provisions singling out online racist behaviour.

2.2 Technical measures: Increased deployment of CIRTs/CERTs

Effective mechanisms and institutional structures at the national level are necessary to deal with cyber risks and incidents reliably. Computer incident response teams (CIRTs) or Computer Emergency Response Teams (CERTs), enable countries to respond to incidents at the national level using a centralized contact point and promote quick and systematic action, empowering countries to learn from experience and build cybersecurity resilience.

National CIRTs are often developed and implemented following legislation or national policy. CIRTs can be part of a governmental institution or under the umbrella of a specific ministry or another entity. Where countries lack time, knowledge, or resources to set up a national CIRT, some outsource CIRT responsibilities to a third-party.

---

7 https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

8 https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/factsheet_lets_put_an_end_to_violence_against_women_en.pdf

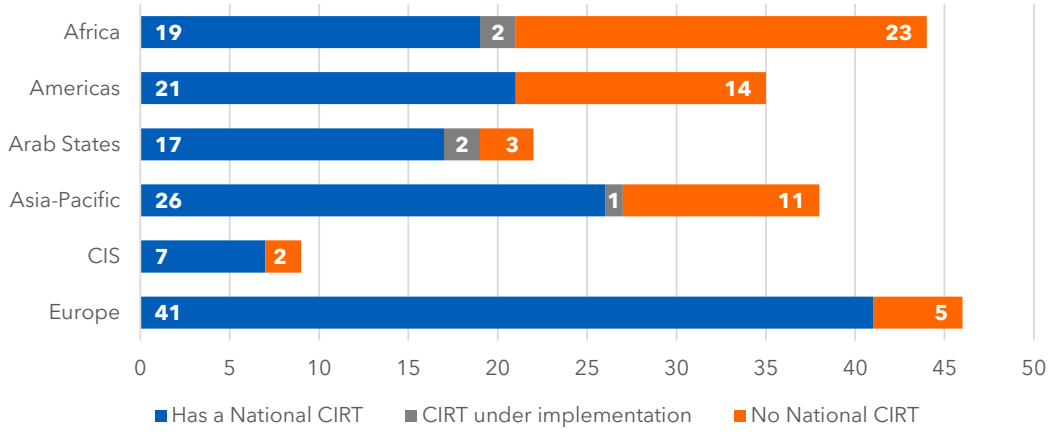
9 https://blogs.microsoft.com/on-the-issues/2020/11/13/microsoft-study-online-risks-world-kindness-day/#_edn1

New CIRTs are being established

At the end of 2020, 131 countries had established national CIRTs, including 10 new CIRTs established since the 2018 Global Cybersecurity Index. An additional four national CIRTs are currently under development.

While many countries have made progress in implementing CIRTs, many, especially least developed countries (LDCs) face significant barriers in establishing CIRTs. A lack of resources, technological knowledge, cybersecurity ecosystem, research and development, prioritization, and political will can hamper efforts in technical measures to address cybersecurity challenges.

Figure 7: Number of countries with a national CIRT



Source: ITU

Despite the Africa region not leading in the technical field, six additional CIRTs have been developed since the 2018 Global Cybersecurity Index, the region has improved from 13 to 19 countries having a national CIRT. The Americas region has 21 CIRTs, and the Arab States region has 17 countries with a national CIRT. However, only two countries in the CIS region and six in Europe lack national CIRTs.

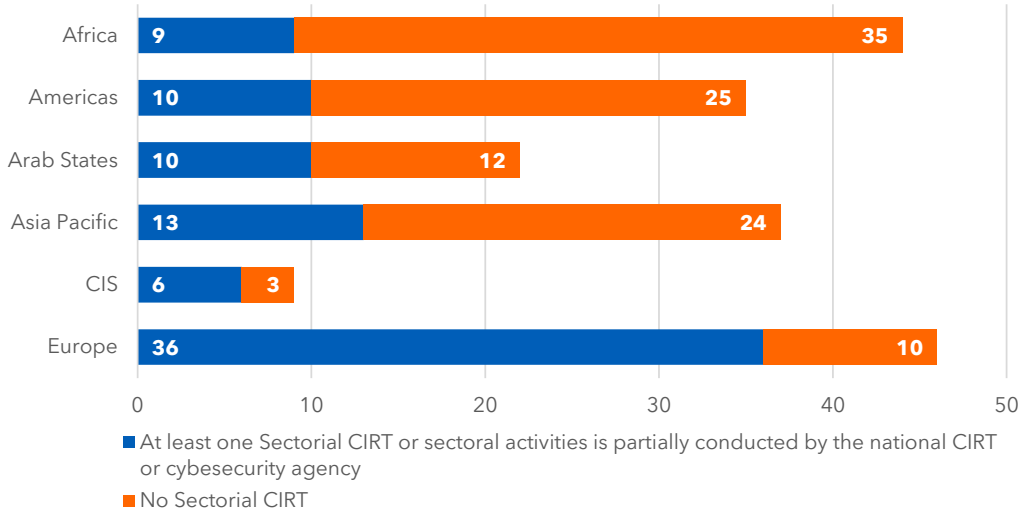
The GCI also tracks CIRT activities. Out of the 131 implemented CIRTs, 11 were engaged in all of the following activities:

- promoting cybersecurity awareness and child online protection by providing tips, guides, manuals, training, and videos;
- delivering cybersecurity advisories to IT specialists;
- conducting cyber drills during the past two years;
- engaging with regional CIRTs and FIRST[10];
- certified by Trusted Introducer[11] or other recognized certification.

While national CIRTs address issues on the national level, sector-specific CIRTs address the cybersecurity needs of a specific sector such as health, transport, telecommunication, utilities. Other types of CIRTs serve multi-national companies or large companies, private universities, among others, and these other types of CIRTs where not tracked in this GCI report.

[10] www.first.org
[11] www.trusted-introducer.org/

Figure 8: Number of sector-specific CIRTs



Source: ITU

As shown in Figure 8, two-thirds of countries do not have sector-specific CIRTs. Out of 76 countries having a sector-specific CIRT, 37 conduct awareness campaigns, cyber drills, and share information related to incidents and threats publicly or confidentially with their community.

2.3 Organizational measures: Aligning strategy

Organizational measures examine the governance and coordination mechanisms within countries that address cybersecurity. Organizational measures include ensuring that cybersecurity is sustained at the highest level of the executive and assigning relevant roles and responsibilities to various national entities, and making them accountable for the national cybersecurity posture.

The presence of organizational measures is not always found in countries with strong telecommunication infrastructure. Comparing the UN E-Government Survey 2020 Digital Government in the Decade of Action for Sustainable Development Telecommunications Infrastructure Index, part of the e-Government Readiness Index,[12] against overall scores in organizational measures, shows that while there is a weak trend, there are many countries that currently do well in telecommunications infrastructure measures, but do not have the organizational measures in place to address cybersecurity issues.

The lack of adequate organizational measures can contribute to a lack of clear responsibilities and accountability in the national cybersecurity governance, and it can prevent effective intra-government and inter-sector coordination.

Importance of up-to-date national cybersecurity strategies

A national cybersecurity strategy (NCS) is often the key cornerstone of organizational measures at national cybersecurity level. According to the ITU Guide to developing a national cybersecurity strategy, an NCS is a comprehensive framework or strategy which has to be developed, implemented and executed in a multi-stakeholder approach, that tackles coordinated action for

[12] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

prevention, preparation, response, and incident recovery on the part of government authorities, the private sector and civil society.[13]

More and more countries are developing national cybersecurity strategies (NCS) to manage cybersecurity in a more structured way. An NCS can confer several benefits, including countries convening relevant stakeholders, clarifying national priorities, and planning cybersecurity capacity development.

As the Global Cybersecurity Index has matured, more focus is being placed on countries that engage in regular updates to their NCS, to ensure that they are adapting to evolving realities. Indeed, having an NCS is a positive first step for countries' cybersecurity posture, but revisions in a regular basis according to the changes in cybersecurity threats and priorities are needed. Countries, when updating an NCS, usually adopt a 4–5-year timeframe. Some countries have opted for longer timeframes, spanning for a decade or more.

With 127 countries having a national cybersecurity strategy, whether current, older than five years, or in progress of being drafted, 60 countries have demonstrated progress in establishing clearer goals through revision and development of new cybersecurity strategies or by updating their action plan.

Protection of critical infrastructure/national resiliency

An important aspect in the developmental process of a national cybersecurity strategy is having a clear set of objectives on the protection of critical infrastructure. Ensuring continuity of operations at the national level is an ongoing challenge for countries. Critical infrastructure, such as electrical grids, water purification plants, and transportation systems, continue to face cybersecurity risks. The potential consequences of an incident impacting critical infrastructure are high, and the strategy should result in greater attention to risk management efforts intended to reduce the likelihood and escalation of a high-consequence event.

Cybersecurity spending for critical infrastructure is expected to increase to USD 9 billion over the next year to reach USD 105.99 billion in 2021.[14] As critical infrastructure, much like the rest of the workforce, has shifted to socially distanced working conditions, they have needed to balance an increased attack surface. ABI Research noted that investment in cybersecurity varied greatly based on region, sector, and connectivity, with spending highest in defense, financial services, and ICTs, but lagging in industrial sectors. [15]

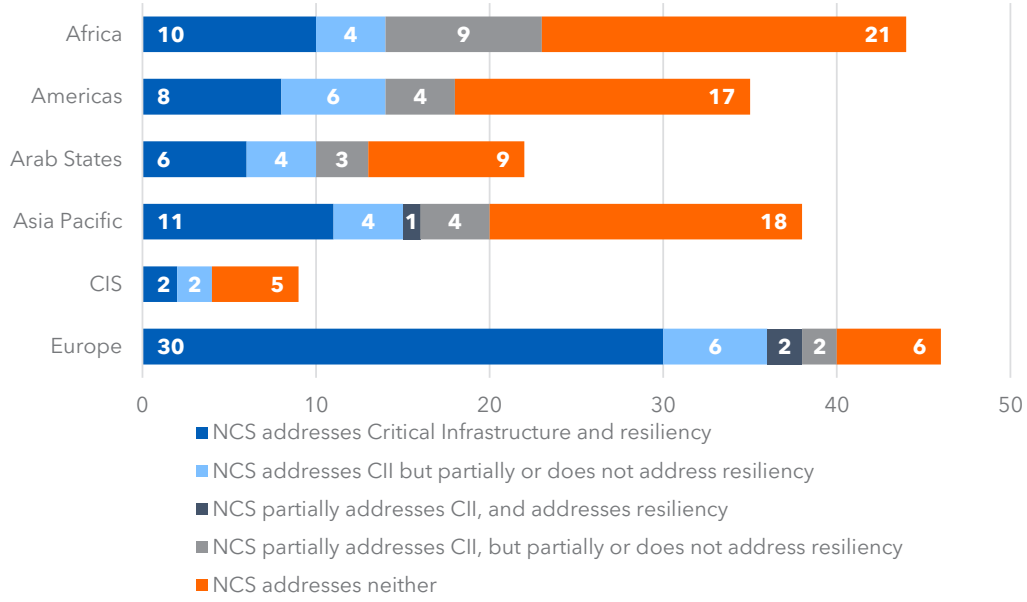
---

13 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

14 https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/

15 https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/

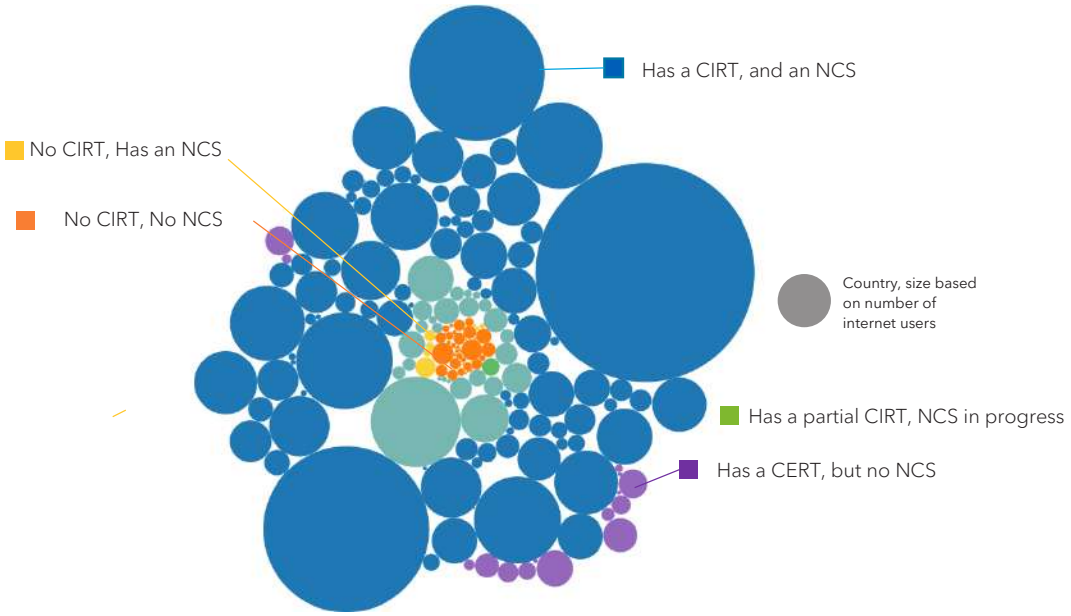
Figure 9: Countries that address critical infrastructure and resiliency



Source: ITU

The prioritization of cybersecurity as part critical infrastructure and resilience is not only reflected in budgetary commitments, but also in national cybersecurity strategies. National cybersecurity strategies more often address critical infrastructure, and/or cybersecurity resiliency. However, many countries do not address either.

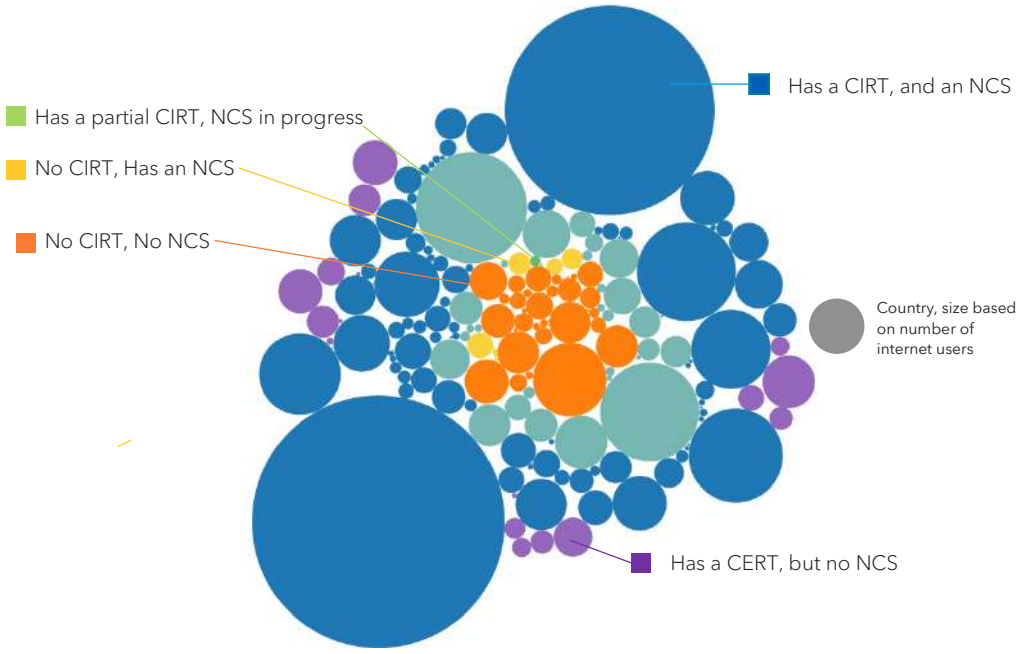
Figure 10: Internet users (by CIRT and national cybersecurity strategy coverage)



Source: Global Cybersecurity Index, ITU World Telecommunication /ICT Indicators

When looking at countries around the world by the number of Internet users, over 95 per cent of Internet users are in countries with both a national cybersecurity strategy and a national CIRT.

Figure 11: Size of unconnected population (by CIRT and national cybersecurity strategy coverage)



Source: Global Cybersecurity Index, ITU World Telecommunication /ICT Indicators

However, the less connected countries often lack an NCS and/or a national CIRT. Nine per cent of the unconnected population live in countries without a national CIRT or national cybersecurity strategy, while an additional 15 per cent are in countries without a strategy, but with a national CIRT in place. Over half of least developed countries are without a CIRT, and 60 per cent lack or have not yet started the process of developing a national cybersecurity strategy.

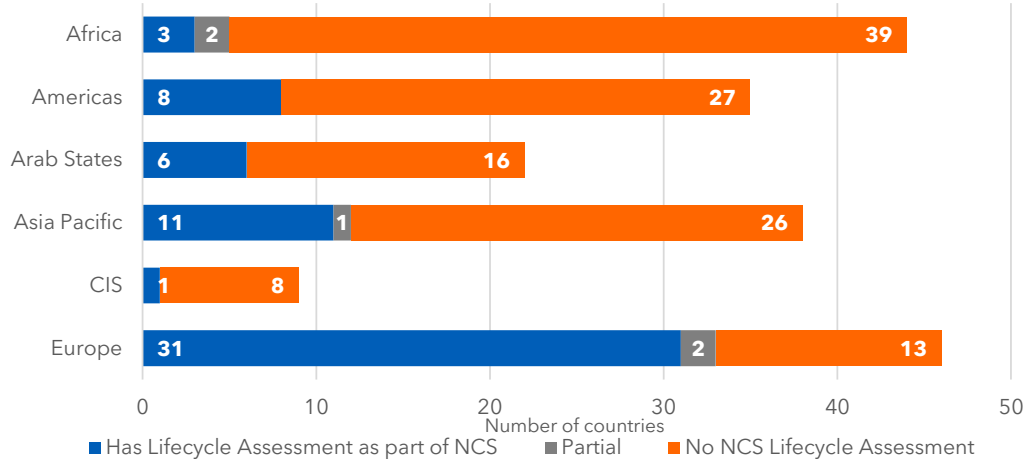
Table 1: Number of countries with an NCS and CIRT

	Has NCS	NCS in progress or >5 years old	No NCS
National CIRT	90 countries	29	18
No national CIRT	7	1	49

Source: ITU

Countries without a national strategy are less likely to have a CIRT. Not surprisingly, between the 63 countries without CIRT, and 67 countries without an NCS, 49 countries have neither a CIRT nor NCS.

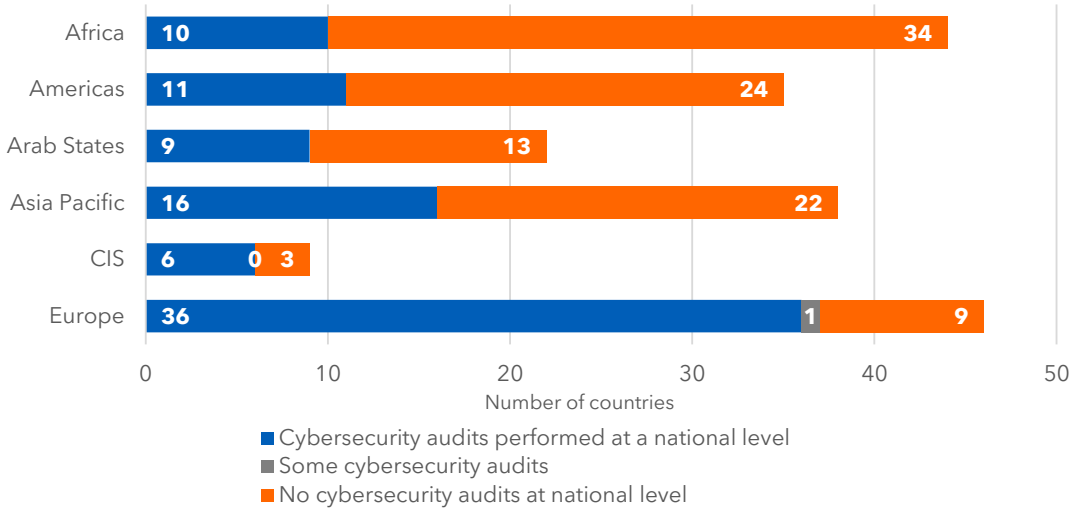
Figure 12: Lifecycle assessment as part of NCS



Source: ITU

Having a national cybersecurity strategy is a positive first step for a cybersecurity posture, but regular updates and revisions are needed. Many countries that have an NCS do not revise and readjust on a regular basis according to the changes in cybersecurity threats and priorities. Of the 98 countries that have an up-to-date NCS, only 60 incorporate lifecycle assessments as part of their strategy.

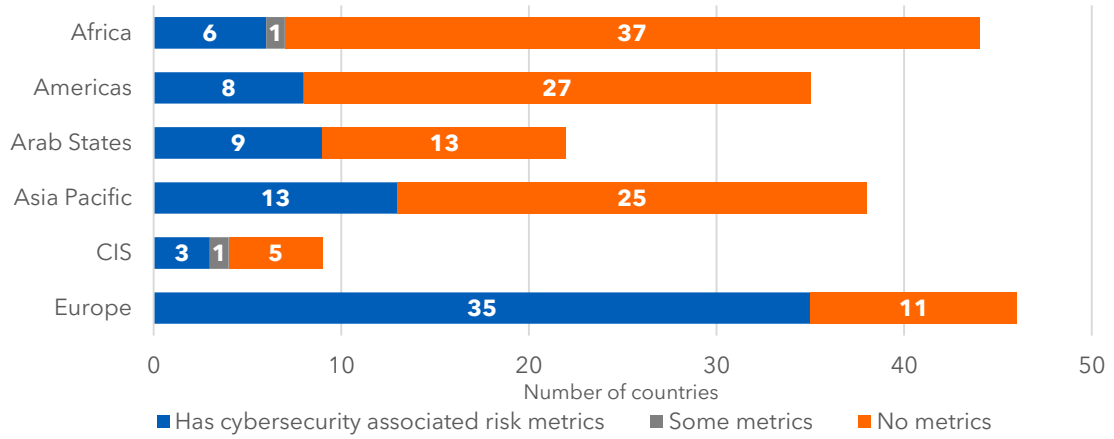
Figure 13: National cybersecurity audits performed at the national level



Source: ITU

National cybersecurity audits (Figure 13) are more common than lifecycle assessments. The frequency of these audits was not assessed as part of this iteration of the GCI.

Figure 14: Metrics for assessing cyberspace associated risk at the national level



Source: ITU

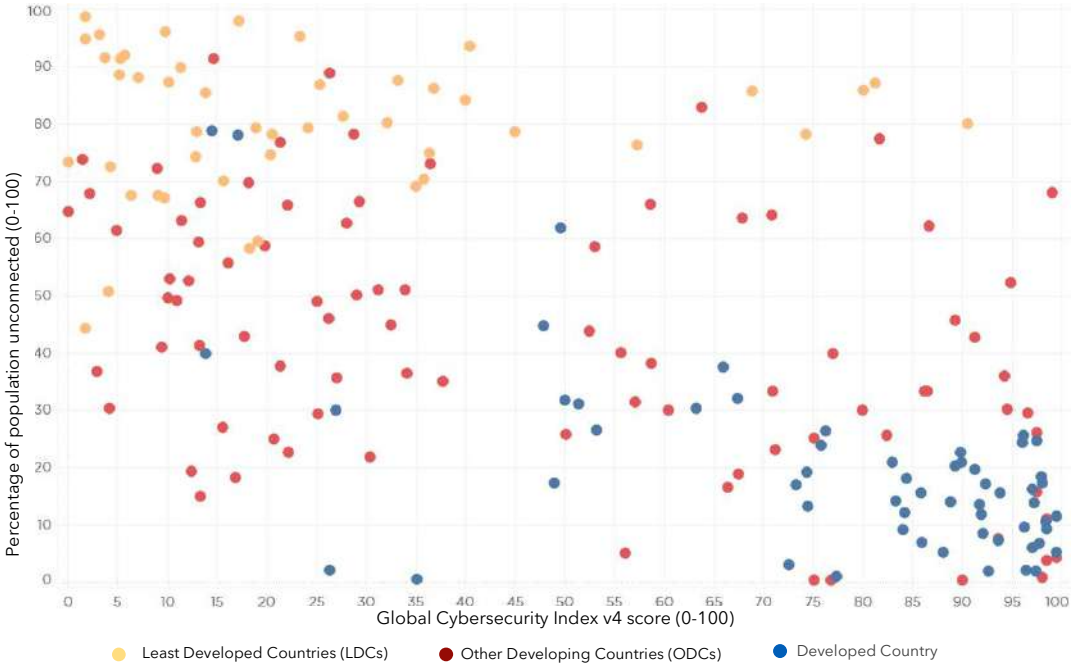
Similarly, most countries do not have metrics for assessing cyberspace associated risk at the national level. The lack of these metrics can make it more difficult for countries to assess current risks, prioritize cybersecurity interventions, and track progress.

2.4 Capacity development measures: Developing cybersecurity capacity

The World Economic Forum estimates that "approximately one million people go online for their first time each day, and two-thirds of the global population own a mobile device."[16] While the advantage of digital technology brings immense economic and societal benefits, cyber risks can offset the benefits of digitalization. Securing the cyber domain through cybersecurity capacity building activities is key as it contributes to reducing issues such as digital divide and cyber risks.

[16] https://reports.weforum.org/global-risks-report-2020/executive-summary/

Figure 15: Global Cybersecurity Index and the unconnected



Source: Global Cybersecurity Index, ITU World Telecommunication /ICT Indicators

As seen in Figure 15, countries that tend do less well in the Global Cybersecurity Index are more likely to be least developed countries and to have a high percentage of their populations unconnected. As these people begin to become more connected, they need support to develop cybersecurity capacity to better respond to threats. However, many countries particularly LDCs are more likely to face resource challenges in bridging their cybercapacity gap, including a lack of institutional knowledge, policy limitations, skills shortages, among others to protect their ICT systems, both physically and virtually.

Several countries are outliers among least developed countries, such as Bangladesh, Benin, Rwanda, and Tanzania, which have demonstrated strong cybersecurity commitments. Notably, these countries all reported having national cybersecurity industries, a key feature of capacity development measures.

Figure 16: Sustainable Development Goals (8, 9, 10)

Source: UN (https://sdgs.un.org/goals)

To promote decent work and economic growth, build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation, and reduce inequality within and among countries, cybersecurity capacity development is necessary to reinforce processes, skills, resources and research and developments aimed at strengthening national capabilities.

Cybersecurity capacity also reinforces developing collective capabilities and at facilitating international cooperation and partnerships to respond effectively to cyber-related challenges of the digital security.

Capacity development tools and measures can contribute to managing cyber-related risks, protecting citizens, infrastructure, businesses, and build stronger cyber communities.

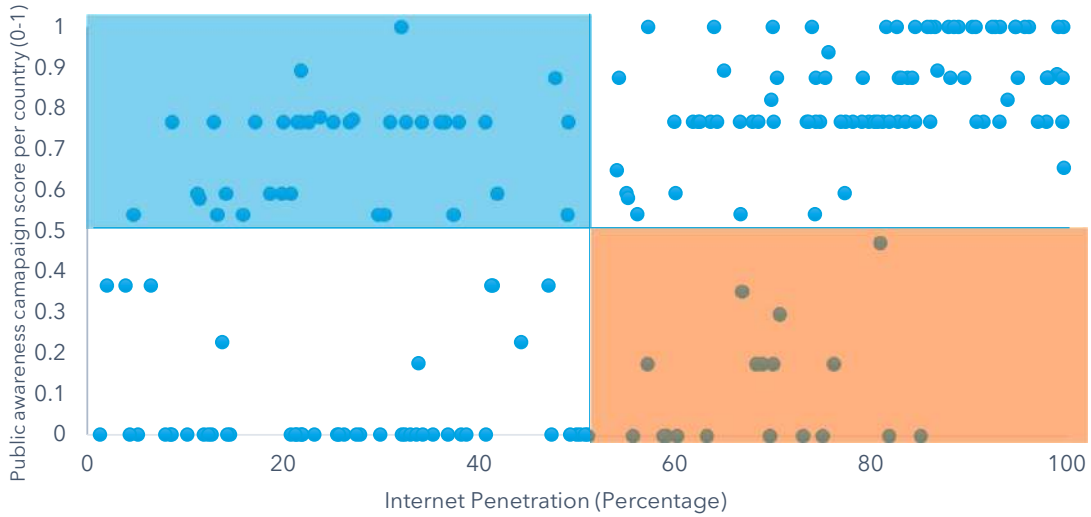
Public cybersecurity awareness raising

Effective cybersecurity awareness raising is essential in keeping citizens, businesses, governments, youth, and organizations alert. With the current shift to digital services, governments need to ensure that all users are aware of the risks they face while carrying out digital activities.

When cybersecurity public awareness campaigns are contrasted against Internet penetration, countries fall into four main groups:

1 Low Internet penetration/promoting cybersecurity awareness (blue box in Figure 17): these countries are better poised to connect the unconnected and equip people with awareness needed online.
2 Low Internet penetration/not promoting cybersecurity awareness: these countries have not yet connected the unconnected, and people are not being offered awareness resources in cybersecurity.
3 High Internet penetration/Promoting cybersecurity awareness: these countries are digitally connected and are engaged in cybersecurity awareness activities to help promote safe behaviour online.
4 High Internet penetration/not promoting cybersecurity awareness (orange box in Figure 17): these countries are digitally connected but their populations may not be aware of cyber risks.

Figure 17: Public cybersecurity awareness campaigns score (per country compared to Internet penetration)



Source: ITU

Public awareness campaign for persons with disabilities and older people

As much as the Internet and the digital world brings unprecedented opportunities, most often persons with disabilities and older people are not considered when operationalizing decisions and technology options are taken. There are an estimated 752 million persons aged 65 or over in 2021.[17] By comparing this figure to the numbers of countries with awareness campaigns focused on persons with disabilities and older people, the result is significantly low. Out of 194 countries, only 18 per cent were raising awareness for persons with disabilities and 25 per cent conducted campaigns for older people. The small number of countries engaged in raising awareness for these two specific populations is alarming as it creates a significant digital divide and gap since persons with disabilities and older people are being urged to use digital services, such as COVID-19 contact tracing apps.

Increased focus on small and medium-sized enterprises (SMEs), private sector, and government cyber awareness

Business operations have shifted further online during the COVID-19 pandemic, placing increased demands on private sector cybersecurity practices. SMEs are often the most common size of business within a country, as 90 per cent of businesses are SMEs, 50 per cent of employment stems from SMEs, and formal SMEs contribute up to 40 per cent to GDP in emerging economies.[18] SMEs are also often least able to tackle cybersecurity. This puts SMEs in need of cybersecurity awareness activities.

Figure 18: Number of countries with cybersecurity awareness campaigns aimed at SMEs, the private sector, and government agencies

Source: ITU

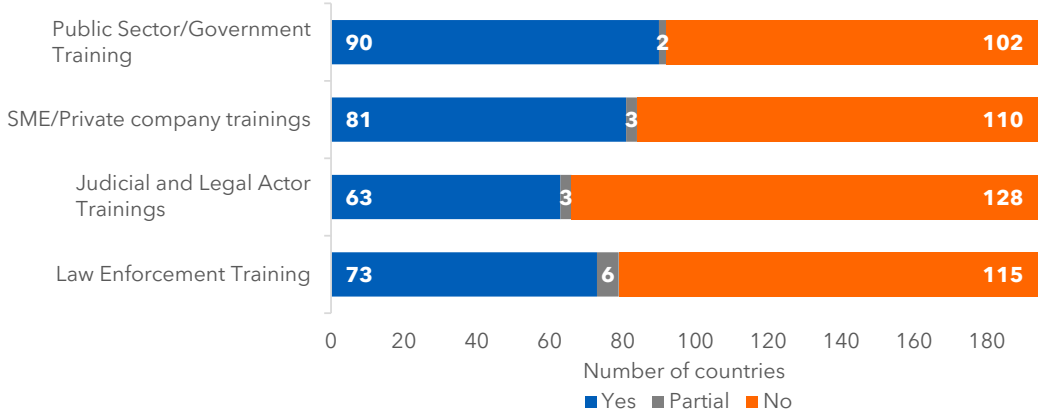
Results from the GCI show that about 60 per cent of countries are, or have been during the past two years, engaged in improving cyber awareness among SMEs, private sector companies, or government agencies, against 38 per cent that did not report any cybersecurity campaigns. They engaged by informing the targeted group on online safety and cybersecurity baselines, providing resources such as through the national CIRT, or offering tools to secure the networks. Two per cent of countries are at an early stage of developing campaigns targeting SMEs, private sector companies, and government agencies.

[17] https://population.un.org/wpp/DataQuery/
[18] https://www.worldbank.org/en/topic/smefinance

Governments are recognizing the need for sector-specific educational programmes and training for cybersecurity professionals

It is increasingly important to provide training programmes to address the various sector needs. Cybersecurity analysts predict that there will be from 3.5 million[19] to as high as 4 million[20] cybersecurity jobs left unfilled globally by 2021. Despite this projected gap, a significant number of countries are yet to develop sector-specific training, and over 50 per cent of countries lack programmes tailored towards specific sectors or professions such as law enforcement, legal actors, SMEs, private companies, and government officials.

Figure 19: Number of countries with specific cybersecurity educational programmes/training for professionals



Source: ITU

As shown in Figure 19, 46 per cent (90) of countries reported providing national sector specific cybersecurity training to public sector and government officials, 41 per cent (81) are providing capacity building exercises on cybersecurity issues for IT professionals including SMEs and the private sector, 37 per cent (73) for law enforcement agents, and 32 per cent (63) of countries are ensuring that judicial and other legal actors are not left behind in ensuring resilience and security.

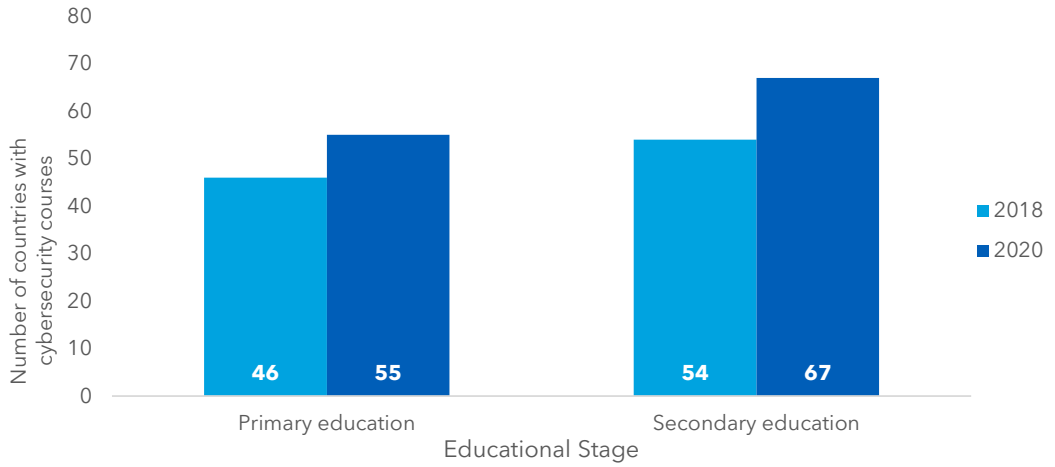
Countries reported providing these cybersecurity training through their national CIRTs, national cybersecurity centres, and government approved or endorsed trainings provided by other regional and international institutions. Some countries seeking to increase the number of cybersecurity professionals, but not able to provide national based training, endorsed international training provided by cybersecurity certification bodies such as SANS[21], ISC[2], ICSPA[22], ISACA[23] and others.

Cybersecurity courses for primary and secondary education are becoming more widespread

As nations have shifted to providing education online, online safety and cybersecurity courses are taught not only in higher education but also in primary and secondary school.

19 https://cybersecurityventures.com/jobs/
20 ESG Research Report: 2019 Digital Work Survey (esg-global.com)
21 https://www.sans.org/
22 https://icspa.org/about-us/
23 https://www.isaca.org/

Figure 20: Number of countries implementing cybersecurity courses into national academic curricula (by education stage)



Source: ITU

As shown in Figure 20, countries are integrating more cybersecurity courses into national educational curricula since the 2018 Global Cybersecurity Index. Five per cent more countries, from 46 to 55, provide introductory courses on keeping children safe from the Internet in primary education and 7 per cent more countries, from 54 to 67, provide resources in secondary academic curricular for students who are interested in pursuing cybersecurity as a career to start learning about it at an early age.

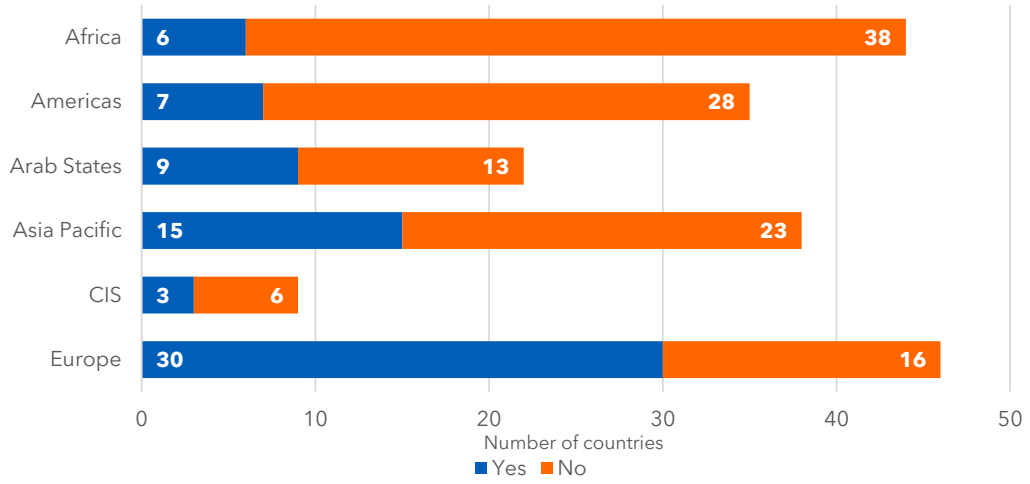
Government incentives for cybersecurity development lags behind

Fostering cybersecurity at a national level needs to be accompanied by the promotion of a cybersecurity culture, encouraging an attitude shift among business leaders, away from cybersecurity as an information technology-related problem, to a more holistic outlook that values the role of cybersecurity in improving overall business efficiency and performance. Cybersecurity precedence among organizations is a process that requires the availability of infrastructure and mechanisms to encourage cybersecurity adoption. Countries fostering cybersecurity development in the private sector and encouraging development of cybersecurity-related companies is reflected in the integration of incentives within their cybersecurity framework.

Countries can promote cybersecurity adoption in the private sector through incentive mechanisms, such as tax incentives based on cybersecurity parameters, tax holidays, or including cybersecurity standards as part contracts. These will encourage private sector actors to prioritize cybersecurity within operational structures and processes, in turn improving a country's cybersecurity posture in the short-, medium-, and long-term.

However, this edition of the GCI shows that 124 countries did not provide any cybersecurity incentives, reflecting the need for Member States to adopt such incentives to fast track cybersecurity measures.

Figure 21: Number of countries with a cybersecurity capacity development incentive mechanism



Source: ITU

2.5 Cooperative measures: Addressing collective cybersecurity action

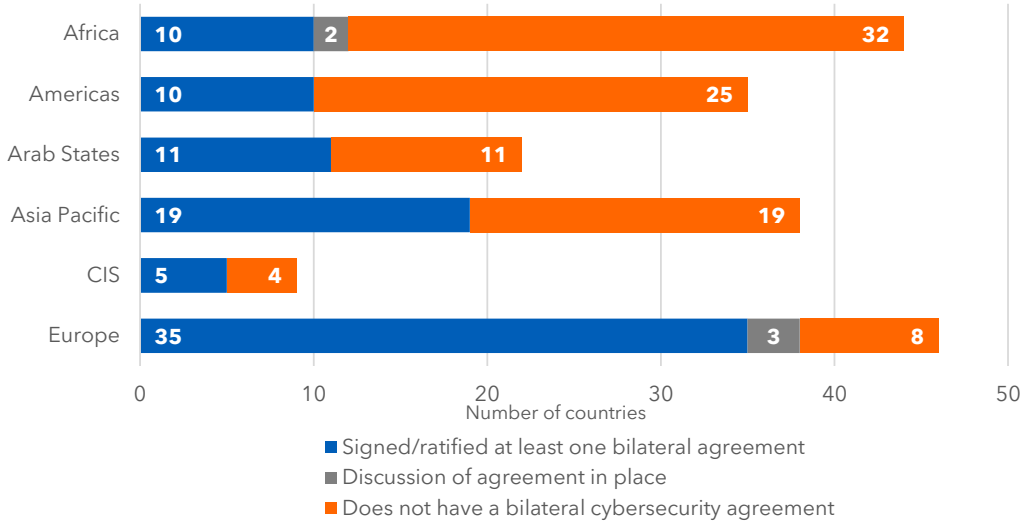
Cybersecurity risks are increasingly borderless,[24] and collaboration remains an essential tool to tackle cybersecurity challenges. Cybersecurity remains a transnational issue due to the increasing interconnection and correlated infrastructures. The security of the global cyber ecosystem cannot be guaranteed or managed by any single stakeholder, and it needs national, regional, and international cooperation to extend reach and impact. In this cooperation pillar, the questionnaire gathered the countries having a bilateral and multilateral agreement, and those engaged in interagency and public-private partnerships. Typical goals of cybersecurity cooperation include harmonization of minimum-security measures, information and good practice sharing, and codification of norms of behaviour.

Bilateral and multilateral agreements

Bilateral and multilateral agreements are crucial in codifying norms and behaviours and enhancing international cooperation on cybersecurity.

[24] https://risk.lexisnexis.com/global/en/insights-resources/infographic/cybercrime-report-infographic-july-december-2019

Figure 22: Countries participating in bilateral cybersecurity agreements



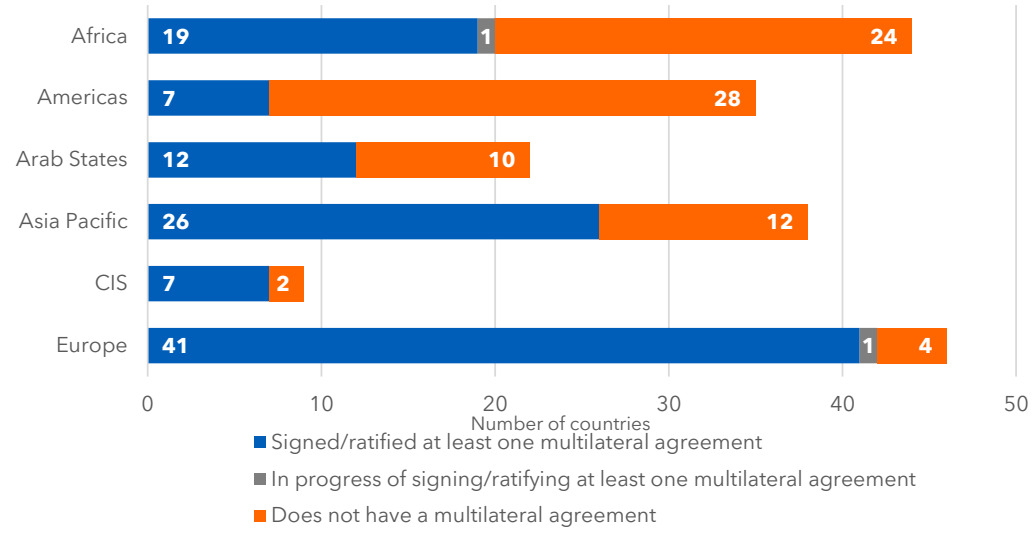
The data extracted shows that 90 countries have a bilateral agreement in cybersecurity. For agreements tracked in the GCI, some countries are concluding cybersecurity agreements in the field of capacity development. In some cases, the agreement is about sharing information only, with cybersecurity not always the central item of the agreement, and instead is included as part of other topics. For 37countries, their bilateral agreements include both information sharing and capacity development measures, but do not address mutual legal assistance.

Figure 23: Countries with a bilateral cybersecurity agreement (by topics covered)

Source: ITU

Given the collective action problem of cybersecurity, some countries have worked to ensure the signature not only to bilateral agreements, but also multilateral agreements. For this iteration of the Global Cybersecurity Index, multilateral agreements were those between three or more parties, including governments and regional organizations but excluding international conventions, such as the Budapest Convention on Cybercrime.

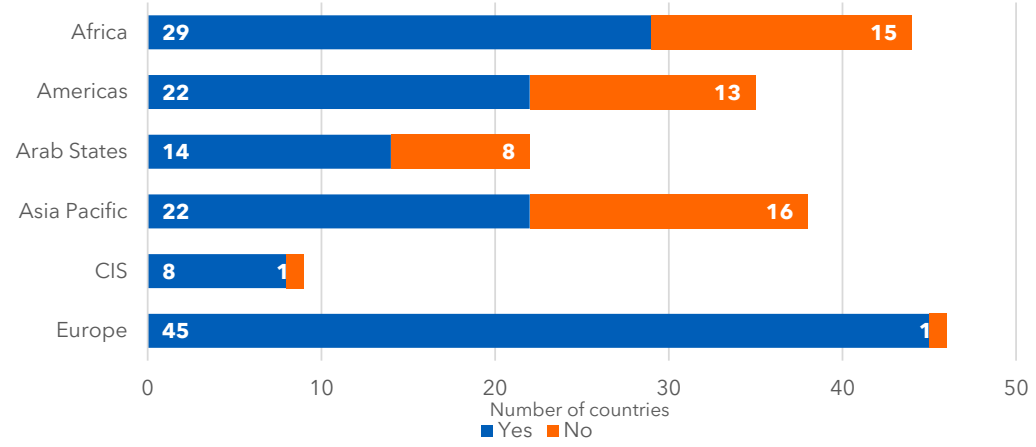
Figure 24: Number of countries participating in multilateral cybersecurity agreements (signed and ratified)



Source: ITU

Countries are more likely to have a multilateral agreement than a bilateral agreement, with almost 57 per cent of countries that signed a multilateral agreement, compared to 46 per cent of countries having signed a bilateral agreement. In addition, many countries (99) signed or ratified a multilateral agreement on information sharing and capacity development.

Figure 25: Engagement in international activities



Source: ITU

Beyond formal cooperation between two or more countries, participating in international activities provide countries opportunities to understand good practices and new approaches to tackle cybersecurity threats. Over the past two years, 140 countries participated in international activities such as cybersecurity conferences, workshops, partnerships, and conventions with other countries.

Public-private partnerships

Beyond collaborating with other countries, countries are collaborating with actors from the private sector. Public-private partnerships (PPP) are critical to cybersecurity efforts, from sharing actionable intelligence, exchanging good practice, and communicating R&D needs and priorities. Table 2 presents the number of countries participating in international and/or domestic PPPs.

Table 2: Countries participating in an international and/or domestic PPP

	International PPP	International PPP in progress	No international PPP
Domestic PPP	62	0	14
Domestic PPP in progress	1	0	0
No domestic PPP	12	1	104

Source: ITU

To engage with the wider cybersecurity ecosystem, some countries organized conferences and workshops, while others contracted private sector companies to develop trainings for the public sector. A growing number of countries reported developing science and technology parks to strengthen their cybersecurity ecosystems. Those platforms can serve as a location for the private and public sectors to meet, provide training, hold workshops, assist start-ups, and host competitions. This kind of cross-sector initiative aim to develop a cybersecurity ecosystem, sharing the knowledge and the competences from various stakeholders, from researchers, students, cybersecurity experts, start-ups, government institutions and foreign companies. The data gathered and collected shows that almost half the countries have at least one type of partnership, with 86 countries engaged, or soon to be engaged, in either an international or domestic PPP, 60 of them engaged both in domestic and international partnerships.

2.6 Child online protection

Figure 26: Reports from ITU child online protection series

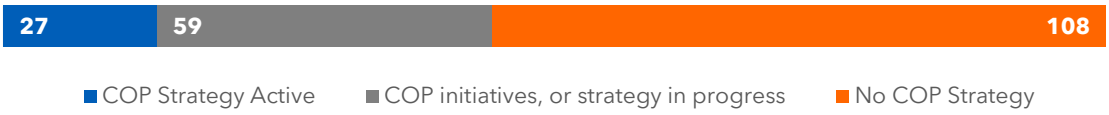
Source: ITU

As noted in the ITU child online protection guidelines, protecting children online is a global challenge, which requires a global approach[25]. The guidelines came at a time when remote learning has meant that children are online more than ever before, and children are more exposed to risks during the COVID-19 pandemic. Unlike previous generations who were driven to remote learning by radio due to pandemics,[26] digital technologies have enabled interactive, two-way educational experiences that not only promote connection among students to learning materials but also to each other.

The ITU child online protection guidelines were designed to help children, parents and educators manage online risks, while also benefiting from the potential of digital technology and strengthening their digital skills. In addition, the guidelines also provide recommendations to policymakers to accelerate the development and adoption of a sound national child online protection strategy and action plans, as well as promote the engagement of the private sector in the development of such policies.

In this regard, the questions related to child online protection measure the extent countries prepared for the digital generation through several items such as existing laws to protect children online, the reporting mechanism for online issues, the awareness campaigns and curricula for schools as well as the countries that created and follow a strategy to protect children online.

Figure 27: Countries with a child online protection strategy



Source: ITU

From the questionnaire, 86 countries out of 194 reported to having taken measures to protect children online. However, the data collected show that only 13 per cent of 194 countries have a standalone strategy dedicated to child online protection. On the other hand, 30 per cent have initiatives for protecting children online integrated in broader strategies, legislation, or initiatives on cybercrime.

The findings further shows that Europe region performs well in matters related to child online protection, with 89 per cent having fully implemented child online protection -related laws. In addition, 101 reporting mechanisms were recorded globally, including hotlines, websites, e-mail addresses, and social media, and 81 countries went further, sharing their child online protection strategies and broader initiatives.

2.7 Conclusion

Cybersecurity is continually evolving, behaviours and practices. Whether it is a global health emergency, climate change, aging populations, or other future challenge, digital technologies offer an enticing tool to help move the world forward. When the Sustainable Development Goals (SDGs) come to maturity in 2030, 90 per cent of the projected world population, or 7.5 billion

[25] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx
[26] https://www.washingtonpost.com/education/2020/04/03/chicago-schools-closed-during-1937-polio-epidemic-kids-learned-home-over-radio/

people, are projected to be online,[27] with an estimated 24.1 billion[28] to 125 billion[29] IoT (Internet of Things) devices connected. If the efforts put into the SDGs are to be sustained, cybersecurity will be needed to ensure that digital solutions are secure, reliable, and trustworthy.

One of the lessons from COVID-19 is that collective action problems like health or cybersecurity, need to be tackled with an interdisciplinary and holistic approach. Tackling all pillars of the GCI – legal, technical, organizational, capacity development and cooperative measures – will require connecting people to each other and building trust. Beyond working together within countries, countries may need to support other states less able to address cybersecurity challenges, such as least developed countries, small island developing states, and landlocked developing countries.

To move forward, countries need to address their strengths and weaknesses in cybersecurity and leverage their competitive advantages to promote general cybercapacity and health. The Global Cybersecurity Index can help countries begin this process. To continue it, countries may need to consider:

- regular assessments of their cybersecurity commitments, including meaningful metrics;
- the continued development of national CIRTs and further establishment of sector-specific CIRTs;
- monitoring and updating national cybersecurity strategies with clear implementation plans;
- inclusion and diversity, especially of underrepresented groups such as women and youth, within the cybersecurity workforce;
- regular participation in international activities to share good practices, case studies, and improve preparedness and response capability;
- improving the cybersecurity capacity of micro, small, and medium-sized enterprises (MSMEs); and,
- regular engagement of all relevant stakeholders in cybersecurity, including the private sector, academia, and civil society.

[27] https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/
[28] https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030--generating-1-5-trillion-annual-revenue-301061873.html
[29] https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

3. GCI results: Score and rankings

3.1 Global scores and ranking of countries

The following table sets out the score and rank for each country that took part in the questionnaire.

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15
Netherlands**	97.05	16
Norway**	96.89	17
Mauritius	96.89	17
Brazil	96.6	18
Belgium	96.25	19
Italy	96.13	20
Oman	96.04	21
Finland	95.78	22
Egypt	95.48	23
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43
Thailand	86.5	44
Tunisia	86.23	45
Ireland	85.86	46
Nigeria	84.76	47
New Zealand**	84.04	48
Malta	83.65	49
Morocco	82.41	50
Kenya	81.7	51
Mexico	81.68	52
Bangladesh	81.27	53

(continued)

Country Name	Score	Rank
Iran (Islamic Republic of)	81.07	54
Georgia	81.06	55
Benin	80.06	56
Rwanda	79.95	57
Iceland	79.81	58
South Africa**	78.46	59
Bahrain	77.86	60
Philippines	77	61
Romania	76.29	62
Moldova	75.78	63
Uruguay	75.15	64
Kuwait	75.07	65
Dominican Rep.	75.05	66
Slovenia	74.93	67
Czech Republic	74.37	68
Monaco	72.57	69
Uzbekistan	71.11	70
Jordan	70.96	71
Uganda	69.98	72
Zambia	68.88	73
Chile	68.83	74
Côte d'Ivoire	67.82	75
Costa Rica	67.45	76
Bulgaria	67.38	77
Ukraine	65.93	78
Pakistan	64.88	79
Albania	64.32	80
Colombia	63.72	81
Cuba	58.76	82
Sri Lanka	58.65	83
Paraguay	57.09	84
Brunei Darussalam	56.07	85
Peru	55.67	86
Montenegro	53.23	87
Botswana	53.06	88
Belarus	50.57	89
Armenia**	50.47	90
Argentina	50.12	91
Kyrgyzstan	49.64	92
Cameroon	45.63	93
Nepal (Republic of)	44.99	94
Chad	40.44	95
Burkina Faso**	39.98	96
Malawi	36.83	97
Zimbabwe	36.49	98
Myanmar	36.41	99
Senegal	35.85	100
Liechtenstein**	35.15	101
Sudan	35.03	102
Panama	34.11	103
Algeria	33.95	104
Togo	33.19	105
Jamaica**	32.53	106
Gambia	32.12	107
Suriname	31.2	108
Lebanon**	30.44	109
Bosnia and Herzegovina	29.44	110
Samoa	29.33	111
Fiji	29.08	112
Libya	28.78	113
Guyana	28.11	114
Ethiopia	27.74	115
Venezuela	27.06	116
Andorra**	26.38	117
Papua New Guinea**	26.33	118
Ecuador	26.3	119
Mongolia	26.2	120
Sierra Leone	25.31	121
State of Palestine	25.18	122
Mozambique	24.18	123
Madagascar**	23.33	124
Trinidad and Tobago	22.18	125
Syrian Arab Republic**	22.14	126
Nauru**	21.42	127
Tonga**	20.95	128
Iraq**	20.71	129
Guinea**	20.53	130

(continued)

Country Name	Score	Rank
Lao P.D.R.	20.34	131
Cambodia**	19.12	132
Mauritania	18.94	133
Bhutan	18.34	134
Eswatini	18.23	135
Cabo Verde	17.74	136
Somalia	17.25	137
Tajikistan**	17.1	138
Barbados	16.89	139
Bolivia (Plurinational State of)	16.14	140
Sao Tome and Principe	15.64	141
Antigua and Barbuda	15.62	142
Congo (Rep. of the)**	14.72	143
Turkmenistan**	14.48	144
Kiribati	13.84	145
San Marino	13.83	146
Bahamas	13.37	147
El Salvador**	13.3	148
Seychelles**	13.23	149
Guatemala	13.13	150
Angola	12.99	151
Vanuatu	12.88	152
Saint Kitts and Nevis**	12.44	153
Saint Vincent and the Grenadines**	12.18	154
Namibia	11.47	155
Niger	11.38	156
Gabon	11.36	157
Saint Lucia**	10.96	158
Belize	10.29	159
Mali**	10.14	160
Guinea-Bissau	9.85	161
Liberia	9.72	162
Grenada	9.41	163
Lesotho	9.08	164
Nicaragua**	9	165
Solomon Islands	7.08	166
Haiti	6.4	167
Tuvalu**	5.78	168
South Sudan**	5.75	169
Dem. Rep. of the Congo	5.3	170
Afghanistan	5.2	171
Marshall Islands**	4.9	172
Timor-Leste**	4.26	173
Dominica	4.2	174
Comoros**	3.72	175
Central African Rep.**	3.24	176
Maldives**	2.95	177
Honduras**	2.2	178
Djibouti	1.73	179
Burundi	1.73	179
Eritrea**	1.73	179
Equatorial Guinea**	1.46	180
Dem. People's Rep. of Korea**	1.35	181
Micronesia*	0	182
Vatican*	0	182
Yemen*	0	182

* no data collected
** no response to the questionnaire

3.2 Regional scores and ranking of countries

Table 4: GCI results: Africa region

Country Name	Overall Score	Regional Rank
Mauritius	96.89	1
Tanzania	90.58	2
Ghana	86.69	3
Nigeria	84.76	4
Kenya	81.7	5
Benin	80.06	6
Rwanda	79.95	7
South Africa**	78.46	8
Uganda	69.98	9
Zambia	68.88	10
Côte d'Ivoire	67.82	11
Botswana	53.06	12
Cameroon	45.63	13
Chad	40.44	14
Burkina Faso**	39.98	15
Malawi	36.83	16
Zimbabwe	36.49	17
Senegal	35.85	18
Togo	33.19	19
Gambia	32.12	20
Ethiopia	27.74	21
Sierra Leone	25.31	22
Mozambique	24.18	23
Madagascar	23.33	24
Guinea**	20.53	25
Eswatini	18.23	26
Cabo Verde	17.74	27
Sao Tome and Principe	15.64	28
Congo (Rep. of the)**	14.72	29
Seychelles**	13.23	30
Angola	12.99	31
Namibia	11.47	32
Niger	11.36	33
Gabon	11.38	34
Mali**	10.14	35
Guinea-Bissau	9.85	36
Liberia	9.72	37
Lesotho	9.08	38
South Sudan**	5.75	39
Dem. Rep. of the Congo	5.3	40
Central African Rep.**	3.24	41
Burundi	1.73	42
Eritrea**	1.73	42
Equatorial Guinea**	1.46	43

* no data
** no response to the questionnaire/data collected by GCI Team

Table 5: GCI results: Americas region

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10
Paraguay	57.09	11
Peru	55.67	12
Argentina	50.12	13
Panama	34.11	14
Jamaica**	32.53	15
Suriname	31.2	16
Guyana	28.11	17
Venezuela	27.06	18
Ecuador	26.3	19

Table 5: GCI results: Americas region (continued)

Country Name	Overall Score	Regional Rank
Trinidad and Tobago	22.18	20
Barbados	16.89	21
Bolivia (Plurinational State of)	16.14	22
Antigua and Barbuda	15.62	23
Bahamas	13.37	24
El Salvador**	13.3	25
Guatemala	13.13	26
Saint Kitts and Nevis	12.44	27
Saint Vincent and the Grenadines**	12.18	28
Saint Lucia**	10.96	29
Belize	10.29	30
Grenada	9.41	31
Nicaragua	9	32
Haiti	6.4	33
Dominica	4.2	34
Honduras**	2.2	35

* no data
** no response to the questionnaire/data collected by GCI Team

Table 6: GCI results: Arab States region

Country Name	Overall Score	Regional Rank
Saudi Arabia	99.54	1
United Arab Emirates	98.06	2
Oman	96.04	3
Egypt	95.48	4
Qatar	94.5	5
Tunisia	86.23	6
Morocco	82.41	7
Bahrain	77.86	8
Kuwait	75.05	9
Jordan	70.96	10
Sudan	35.03	11
Algeria	33.95	12
Lebanon**	30.44	13
Libya	28.78	14
State of Palestine	25.18	15
Syrian Arab Republic**	22.14	16
Iraq**	20.71	17
Mauritania	18.94	18
Somalia	17.25	19
Comoros**	3.72	20
Djibouti	1.73	21
Yemen*	0	22

* no data
** no response to the questionnaire/data collected by GCI Team

Table 7: GCI results: Asia-Pacific region

Country Name	Overall Score	Regional Rank
Korea (Rep. of)	98.52	1
Singapore	98.52	1
Malaysia	98.06	2
Japan	97.82	3
India	97.49	4
Australia	97.47	5
Indonesia	94.88	6
Viet Nam	94.55	7
China	92.53	8
Thailand	86.5	9
New Zealand**	84.04	10
Bangladesh	81.27	11
Iran (Islamic Republic of)	81.06	12
Philippines	77	13
Pakistan	64.88	14
Sri Lanka	58.65	15
Brunei Darussalam	56.07	16
Nepal (Republic of)	44.99	17
Myanmar	36.41	18

Table 7: GCI results: Asia-Pacific region (continued)

Country Name	Overall Score	Regional Rank
Samoa	29.33	19
Fiji	29.08	20
Papua New Guinea**	26.33	21
Mongolia	26.2	22
Nauru**	21.42	23
Tonga**	20.95	24
Lao P.D.R.	20.34	25
Cambodia**	19.12	26
Bhutan	18.34	27
Kiribati	13.84	28
Vanuatu	12.88	29
Solomon Islands	7.08	30
Tuvalu**	5.78	31
Afghanistan	5.2	32
Marshall Islands**	4.9	33
Timor-Leste**	4.26	34
Maldives**	2.95	35
Dem. People's Rep. of Korea**	1.35	36
Micronesia*	0	37

* no data
** no response to the questionnaire/data collected by GCI Team

Table 8: GCI results: CIS region

Country Name	Overall Score	Regional Rank
Russian Federation	98.06	1
Kazakhstan	93.15	2
Azerbaijan	89.31	3
Uzbekistan	71.11	4
Belarus	50.57	5
Armenia**	50.47	6
Kyrgyzstan	49.64	7
Tajikistan**	17.1	8
Turkmenistan**	14.48	9

* no data
** no response to the questionnaire/data collected by GCI Team

Table 9: GCI results: Europe region

Country Name	Overall Score	Regional Rank
United Kingdom	99.54	1
Estonia	99.48	2
Spain	98.52	3
Lithuania	97.93	4
France	97.6	5
Turkey	97.5	6
Luxembourg	97.41	7
Germany	97.41	7
Portugal	97.32	8
Latvia	97.28	9
Netherlands**	97.05	10
Norway**	96.89	11
Belgium	96.25	12
Italy	96.13	13
Finland	95.78	14
Sweden	94.59	15
Greece	93.98	16
Austria	93.89	17
Poland	93.86	18
Denmark	92.6	19
Croatia	92.53	20
Slovakia	92.36	21
Hungary	91.28	22
Israel**	90.93	23
The Republic of North Macedonia	89.92	24
Serbia	89.8	25
Cyprus	88.82	26
Switzerland**	86.97	27
Ireland	85.86	28
Malta	83.65	29
Georgia	81.07	30
Iceland	79.81	31
Romania	76.29	32
Moldova	75.78	33
Slovenia	74.93	34
Czech Republic	74.37	35
Monaco	72.57	36

Table 9: GCI results: Europe region (continued)

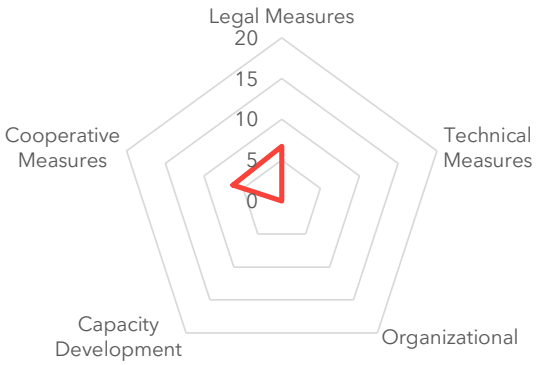
Country Name	Overall Score	Regional Rank
Bulgaria	67.38	37
Ukraine	65.93	39
Albania	64.32	40
Montenegro	53.23	41
Liechtenstein**	35.15	42
Bosnia and Herzegovina	29.44	43
Andorra**	26.38	44
San Marino	13.83	45
Vatican*	0	46

* no data
** no response to the questionnaire/data collected by GCI Team

4. Global Cybersecurity Index 2020: Country profiles

Africa region

Angola (Republic of)



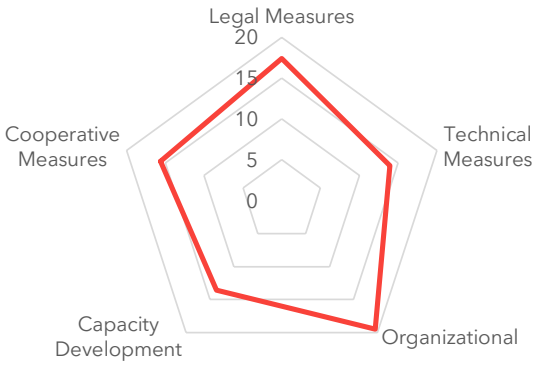
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
12.99	6.70	0.00	0.00	0.00	6.30

Source: ITU Global Cybersecurity Index v4, 2021

Benin (Republic of)



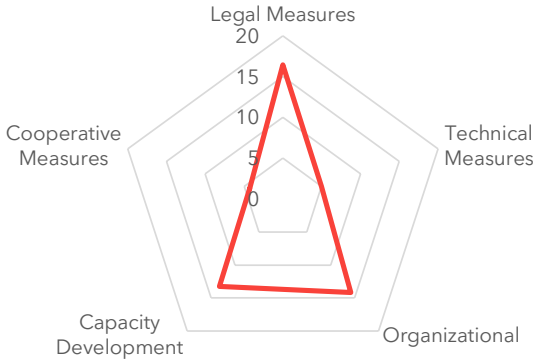
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
80.06	17.42	13.94	19.48	13.60	15.63

Source: ITU Global Cybersecurity Index v4, 2021

Botswana (Republic of)



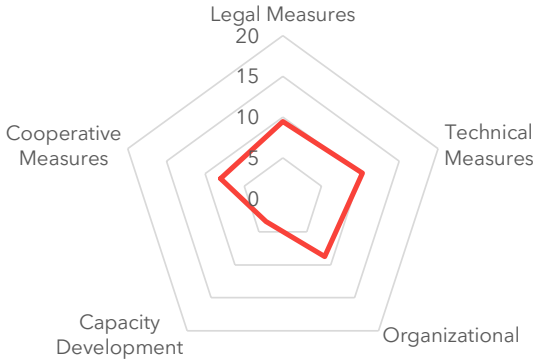
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal Measure
Area(s) of Potential Growth
Cooperative Measures, Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
53.06	16.44	4.95	14.16	13.23	4.26

Source: ITU Global Cybersecurity Index v4, 2021

*Burkina Faso***



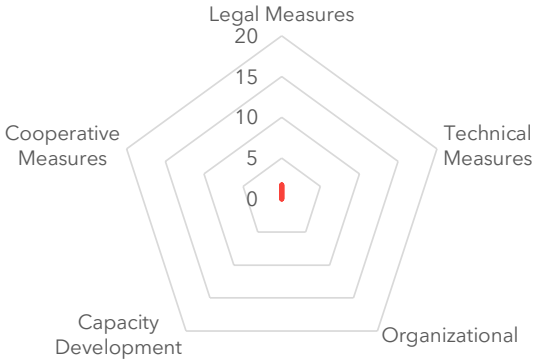
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
39.98	9.47	10.25	8.75	3.47	8.04

Source: ITU Global Cybersecurity Index v4, 2021

Burundi (Republic of)



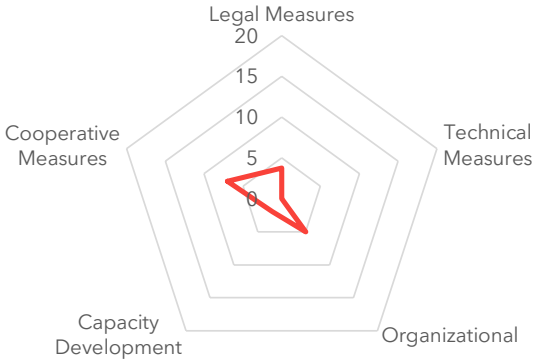
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
1.73	1.73	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Cabo Verde (Republic of)



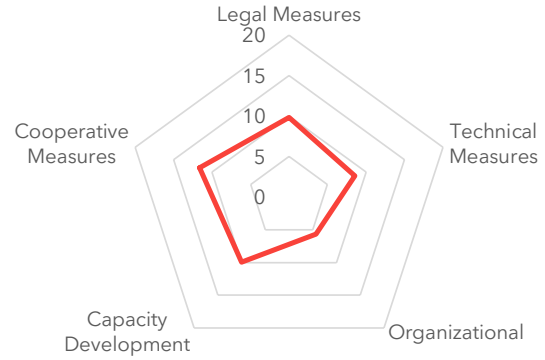
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
17.74	3.77	0.00	5.00	1.96	7.00

Source: ITU Global Cybersecurity Index v4, 2021

Cameroon (Republic of)



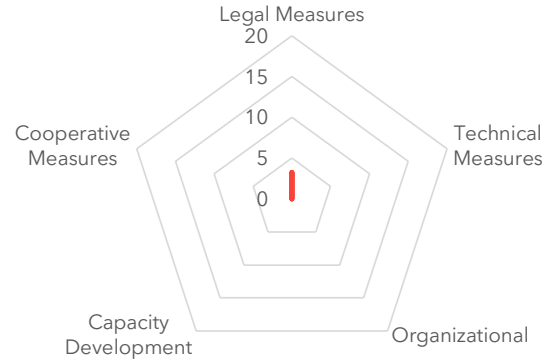
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
45.63	9.84	8.54	5.67	9.95	11.63

Source: ITU Global Cybersecurity Index v4, 2021

*Central African Republic***



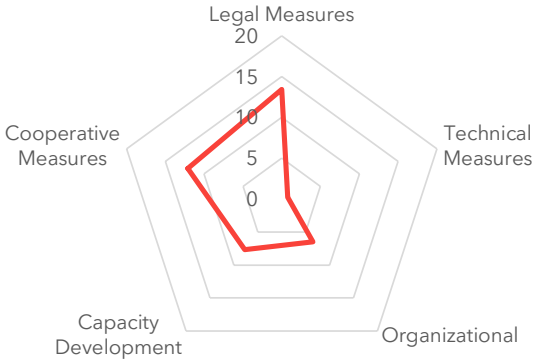
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Capacity Development, Cooperative

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
3.24	3.24	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Chad (Republic of)



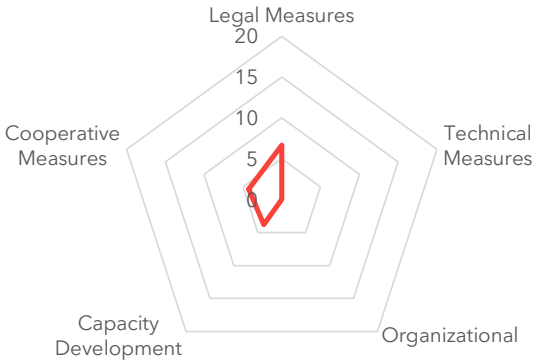
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
40.44	13.43	0.73	6.50	7.67	12.11

Source: ITU Global Cybersecurity Index v4, 2021

*Congo (Republic of the)***



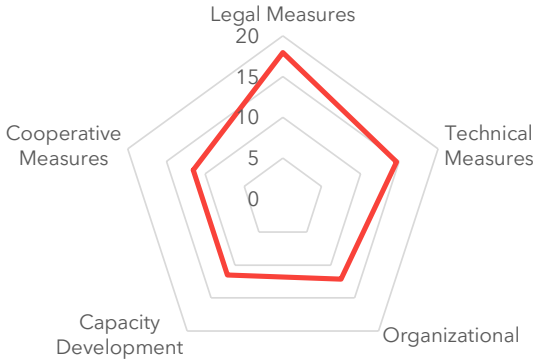
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
14.72	6.66	0.00	0.00	3.80	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Côte d'Ivoire (Republic of)



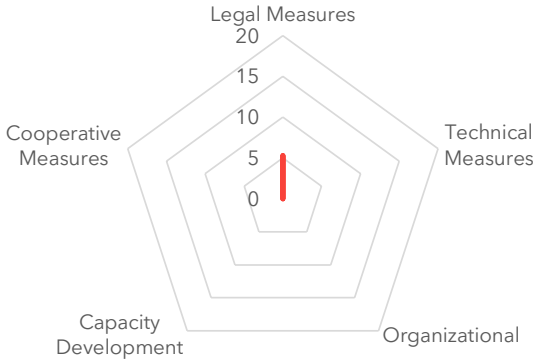
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
67.82	17.95	14.65	12.14	11.53	11.55

Source: ITU Global Cybersecurity Index v4, 2021

Democratic Republic of the Congo



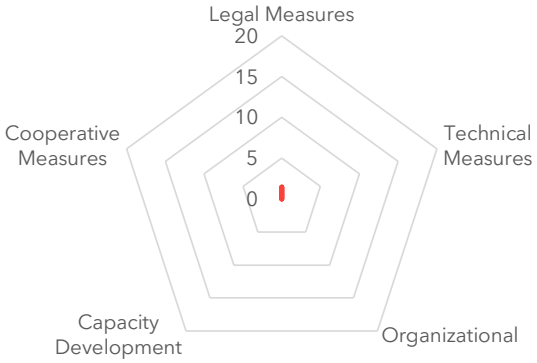
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
5.30	5.30	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*Equatorial Guinea (Republic of)***



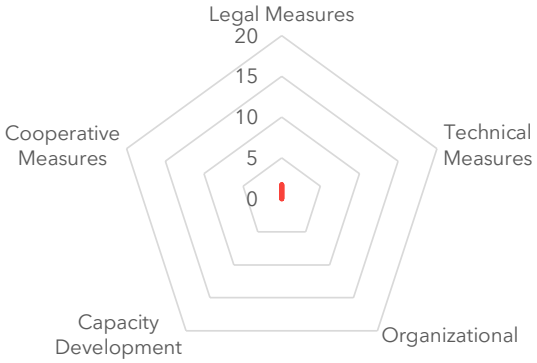
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
1.46	1.46	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*Eritrea***



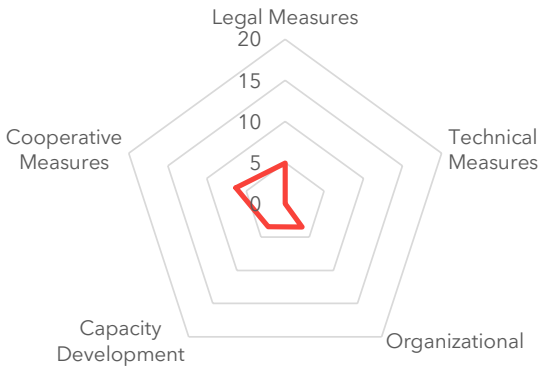
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
1.73	1.73	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Eswatini (Kingdom of)



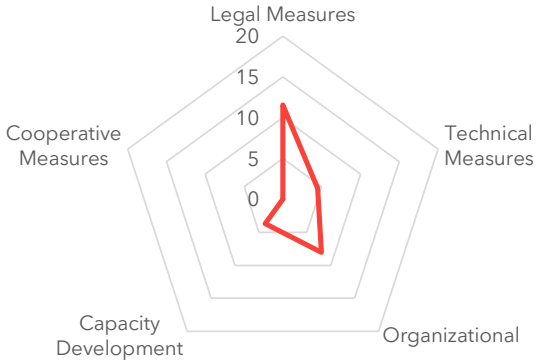
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
18.23	4.96	0.00	3.49	3.47	6.31

Source: ITU Global Cybersecurity Index v4, 2021

Ethiopia (Federal Democratic Republic of)



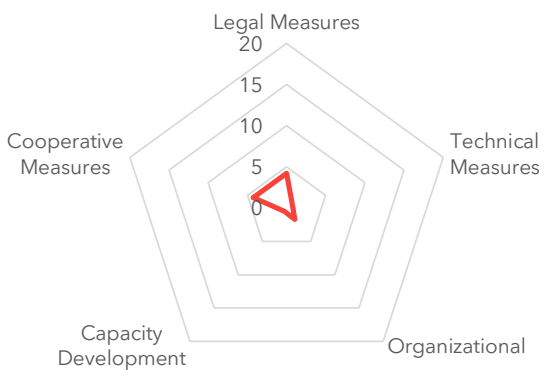
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
27.74	11.56	4.46	8.03	3.69	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Gabonese Republic



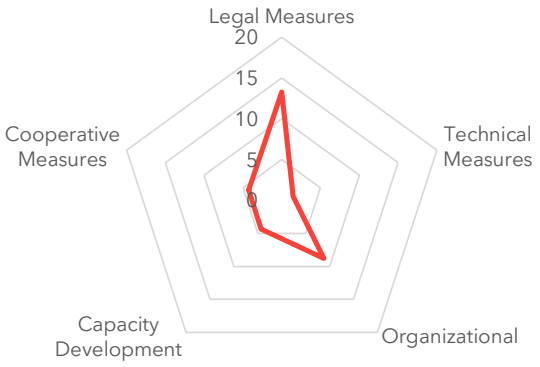
Development Level:
Developing Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
11.38	4.24	0.73	1.69	0.46	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Gambia (Republic of the)



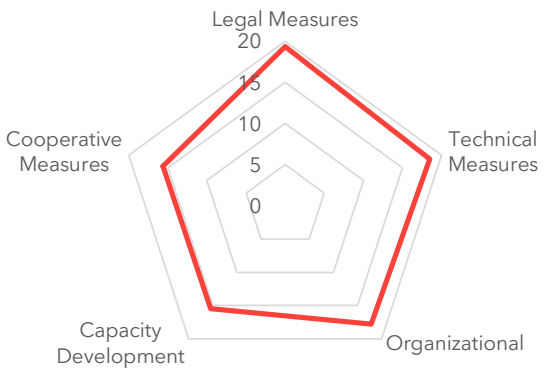
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
32.12	13.28	1.46	8.78	4.34	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Ghana



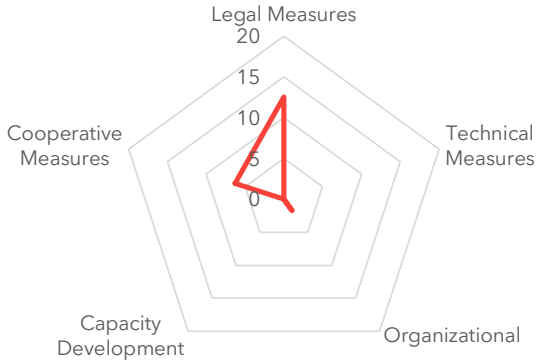
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Capacity Development, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
86.69	19.35	18.48	17.78	15.44	15.63

Source: ITU Global Cybersecurity Index v4, 2021

*Guinea (Republic of)***



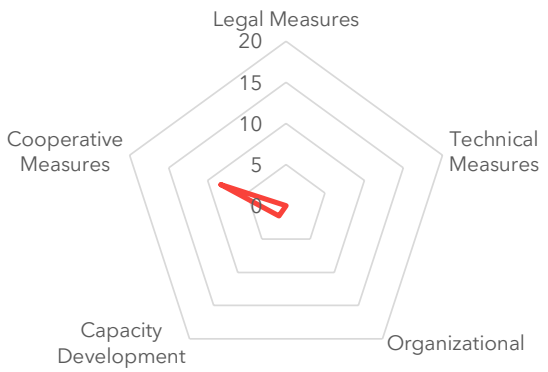
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
20.53	12.54	0.00	1.69	0.00	6.30

Source: ITU Global Cybersecurity Index v4, 2021

Guinea-Bissau (Republic of)



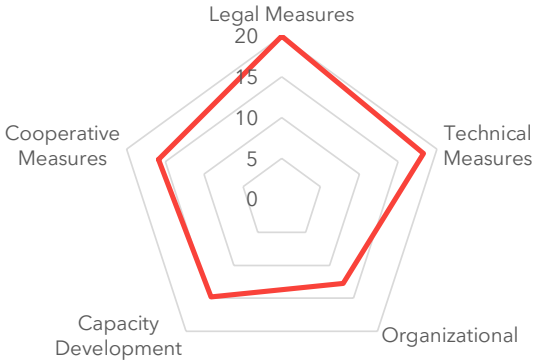
Development Level:
Developing Country, Least Developed Countries (LDC)
Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Legal, Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
9.85	0.00	0.00	0.00	1.52	8.33

Source: ITU Global Cybersecurity Index v4, 2021

Kenya (Republic of)



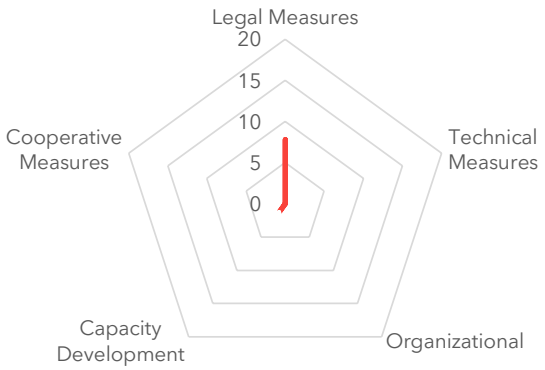
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.70	20.00	18.27	12.75	14.79	15.89

Source: ITU Global Cybersecurity Index v4, 2021

Lesotho (Kingdom of)



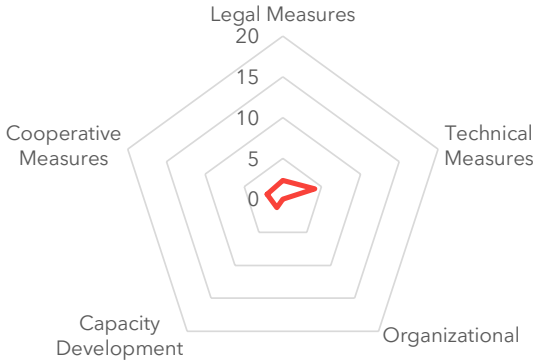
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Organizational, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
9.08	7.82	0.00	0.00	1.26	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Liberia (Republic of)



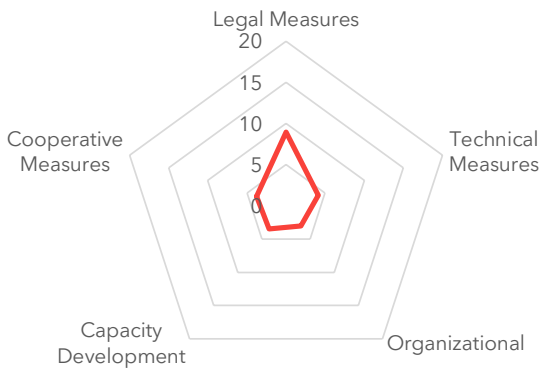
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
9.72	2.31	4.11	0.00	1.26	2.04

Source: ITU Global Cybersecurity Index v4, 2021

*Madagascar (Republic of)***



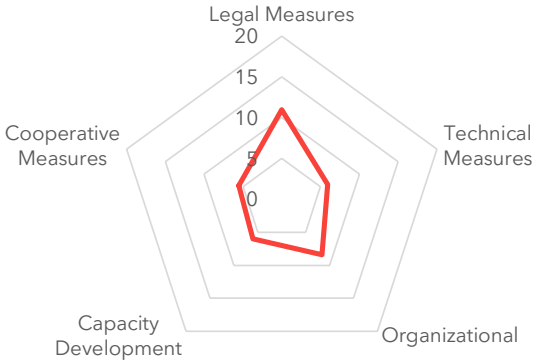
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
23.33	8.96	4.11	3.00	3.47	3.78

Source: ITU Global Cybersecurity Index v4, 2021

Malawi



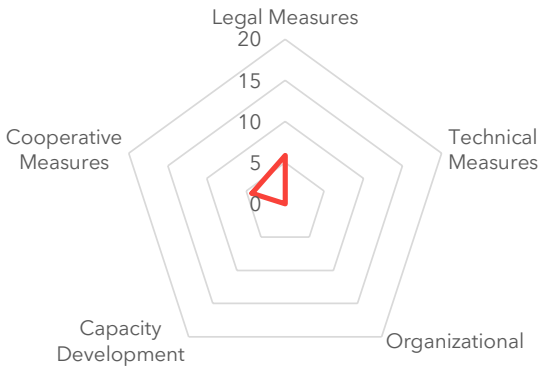
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal, Organizational Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
36.83	10.98	5.92	8.40	6.00	5.54

Source: ITU Global Cybersecurity Index v4, 2021

*Mali (Republic of)***



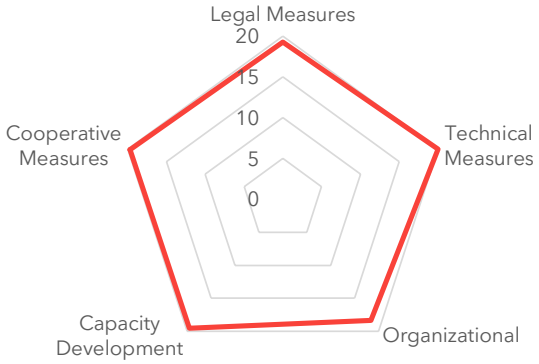
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
10.14	5.89	0.00	0.00	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Mauritius (Republic of)



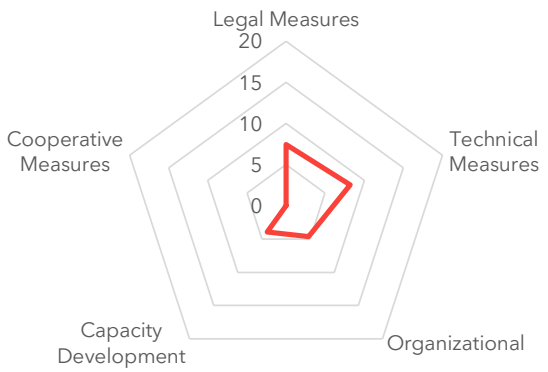
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Technical Measures, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.89	19.27	20.00	18.38	19.54	19.70

Source: ITU Global Cybersecurity Index v4, 2021

Mozambique (Republic of)



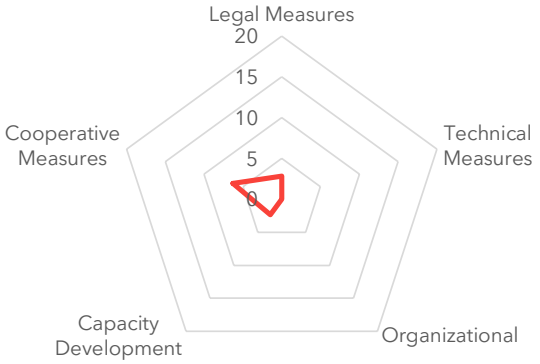
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Technical, Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
24.181	7.455	8.188	4.622	3.916	0.000

Source: ITU Global Cybersecurity Index v4, 2021

Namibia (Republic of)



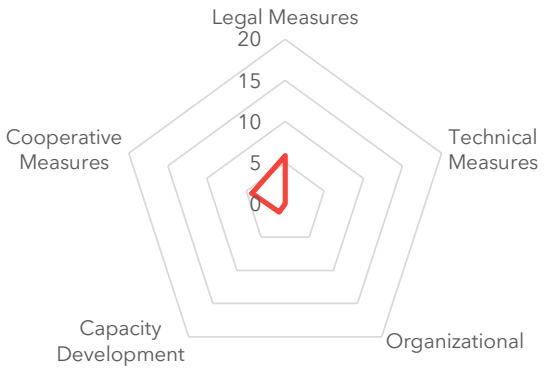
Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
11.47	2.84	0.00	0.00	2.34	6.30

Source: ITU Global Cybersecurity Index v4, 2021

Niger (Republic of the)



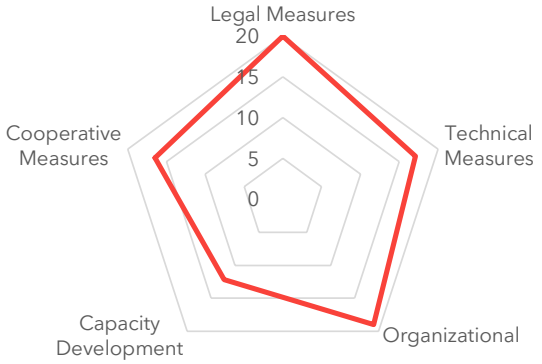
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal, Cooperative Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
11.36	5.87	0.00	0.00	1.23	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Nigeria (Federal Republic of)



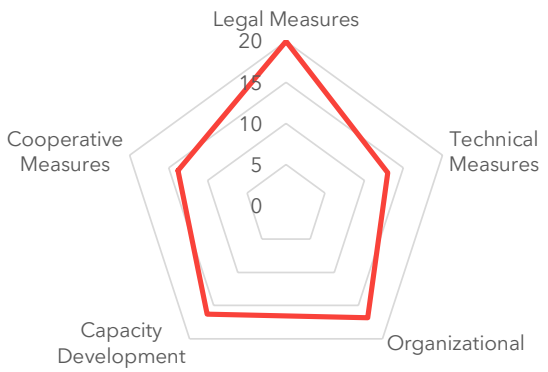
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
84.76	20.00	17.09	18.98	12.21	16.48

Source: ITU Global Cybersecurity Index v4, 2021

Rwanda (Republic of)



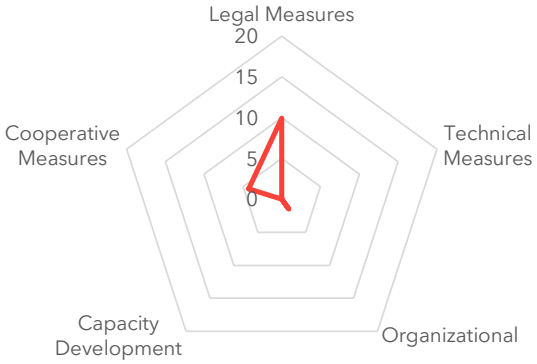
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
79.95	20.00	13.00	16.83	16.30	13.82

Source: ITU Global Cybersecurity Index v4, 2021

Sao Tome and Principe (Democratic Republic of)



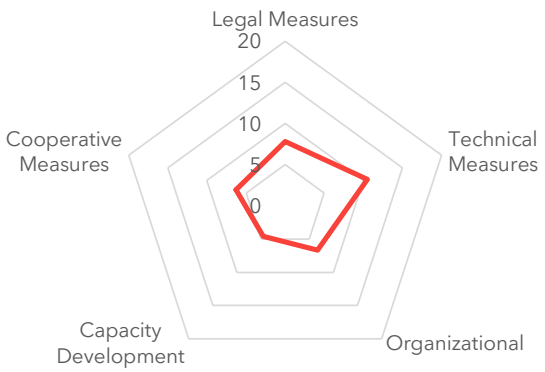
Development Level:
Developing Country, Least Developed Countries (LDC), Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
15.64	9.94	0.00	1.44	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Senegal (Republic of)



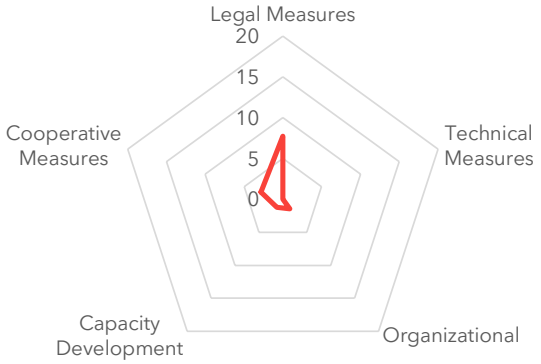
Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
35.85	7.82	10.50	6.66	4.58	6.30

Source: ITU Global Cybersecurity Index v4, 2021

*Seychelles (Republic of)***



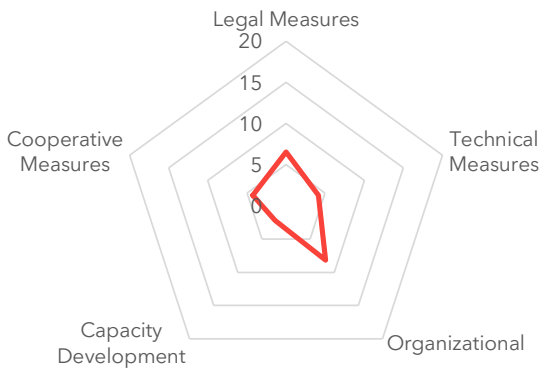
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
13.23	7.73	0.00	1.44	1.23	2.83

Source: ITU Global Cybersecurity Index v4, 2021

Sierra Leone



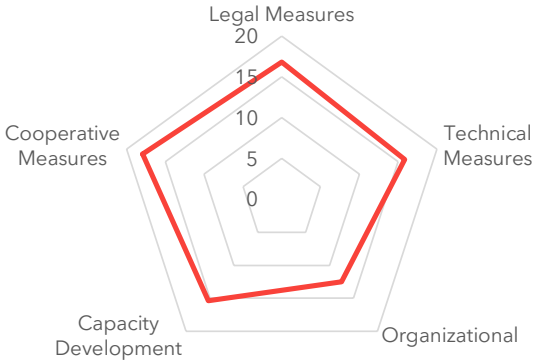
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
25.31	6.54	4.11	8.16	2.24	4.26

Source: ITU Global Cybersecurity Index v4, 2021

*South Africa (Republic of)***



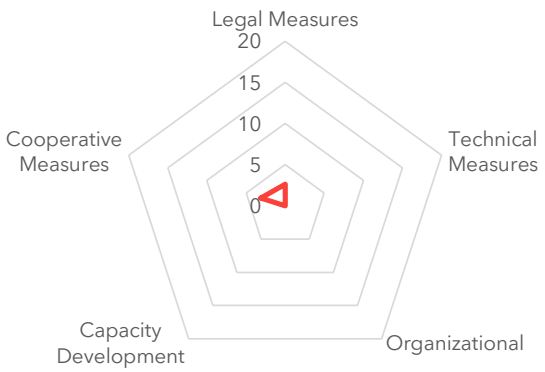
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
78.46	16.82	15.85	12.50	15.37	17.93

Source: ITU Global Cybersecurity Index v4, 2021

*South Sudan (Republic of)***



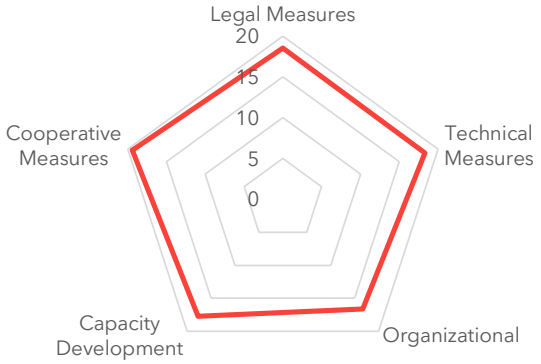
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical, Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
5.75	2.63	0.00	0.00	0.00	3.12

Source: ITU Global Cybersecurity Index v4, 2021

Tanzania (United Republic of)



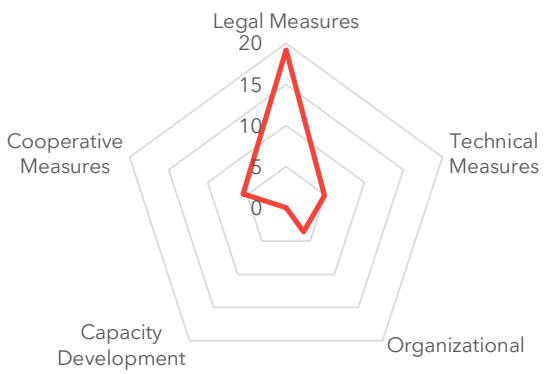
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
90.58	18.54	18.31	16.60	17.72	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Togolese Republic



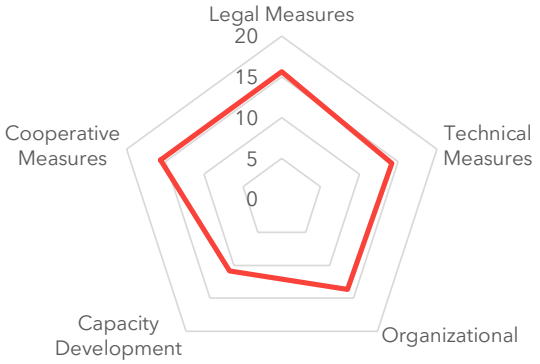
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
33.19	19.19	4.90	3.61	0.00	5.49

Source: ITU Global Cybersecurity Index v4, 2021

Uganda (Republic of)



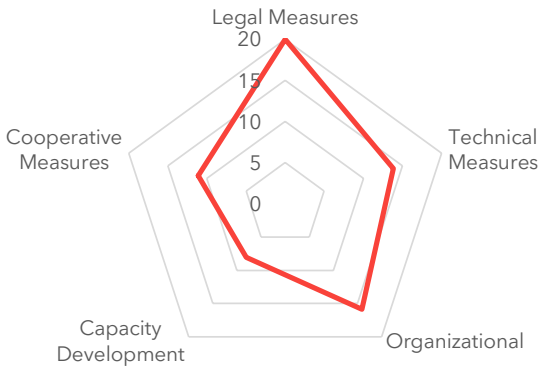
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
69.98	15.64	14.19	13.65	10.87	15.63

Source: ITU Global Cybersecurity Index v4, 2021

Zambia (Republic of)



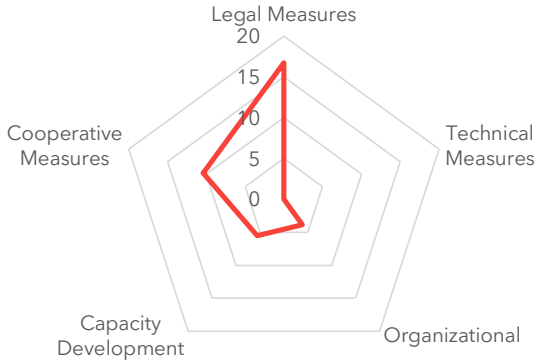
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.88	20.00	13.82	15.86	8.07	11.12

Source: ITU Global Cybersecurity Index v4, 2021

Zimbabwe (Republic of)



Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
36.49	16.73	0.00	3.84	5.52	10.40

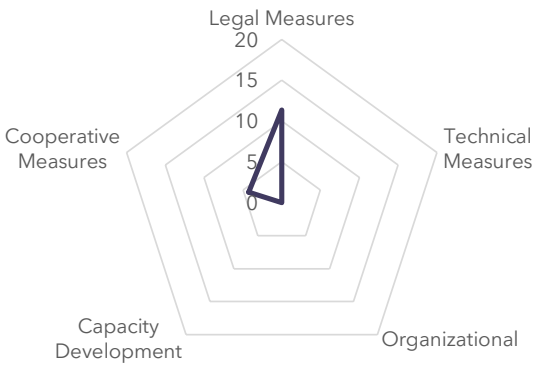
Source: ITU Global Cybersecurity Index v4, 2021

** no response to the questionnaire/data collected by GCI Team

* no data

Americas region

Antigua and Barbuda



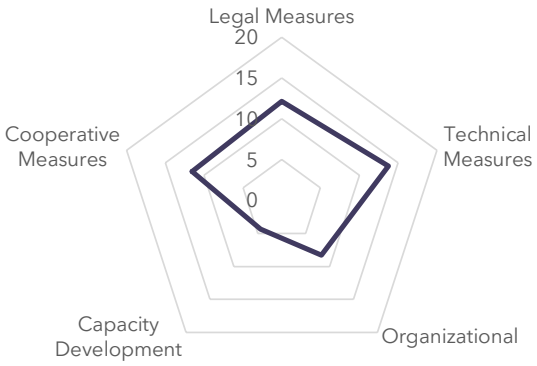
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures, Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
15.62	11.36	0.00	0.00	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Argentine Republic



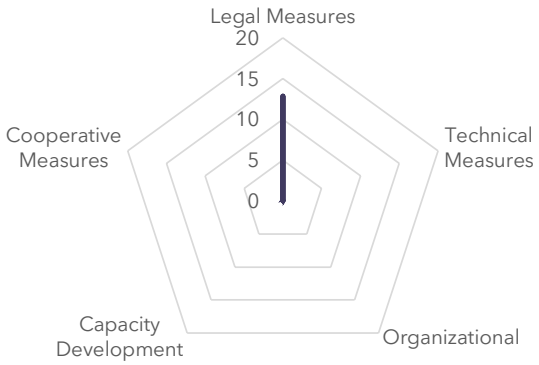
Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
50.12	12.15	13.75	8.29	4.38	11.55

Source: ITU Global Cybersecurity Index v4, 2021

Bahamas (Commonwealth of the)



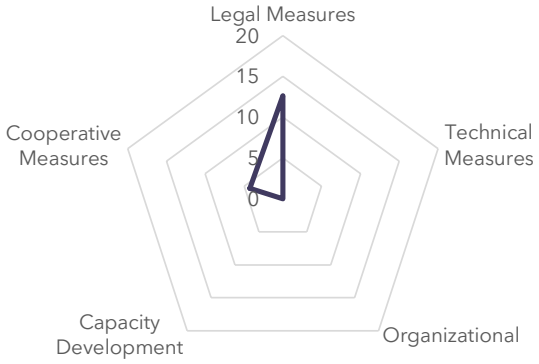
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
13.37	12.85	0.00	0.00	0.52	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Barbados



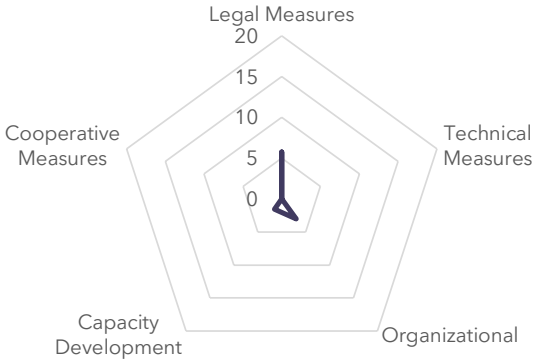
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
16.89	12.63	0.00	0.00	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Belize



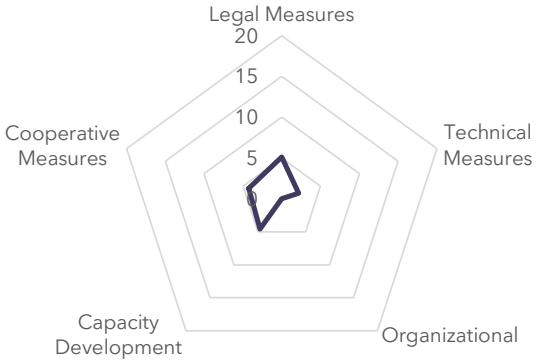
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
10.29	5.77	0.00	3.01	1.52	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Bolivia (Plurinational State of)



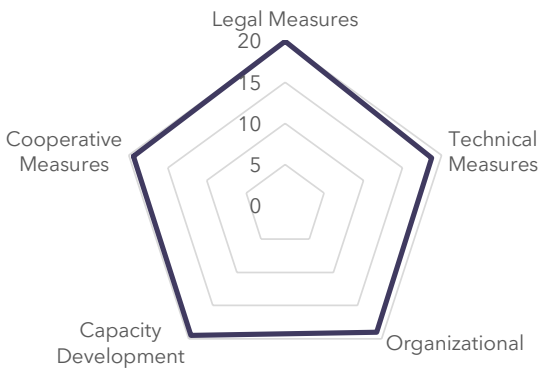
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal Measures, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
16.14	5.13	2.18	0.00	4.58	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Brazil (Federative Republic of)



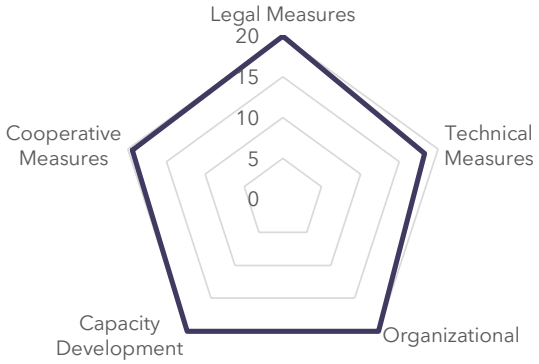
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.60	20.00	18.73	18.98	19.48	19.41

Source: ITU Global Cybersecurity Index v4, 2021

*Canada***



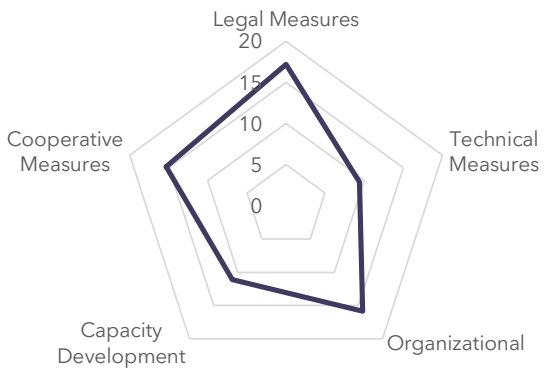
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.67	20.00	18.27	20.00	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Chile



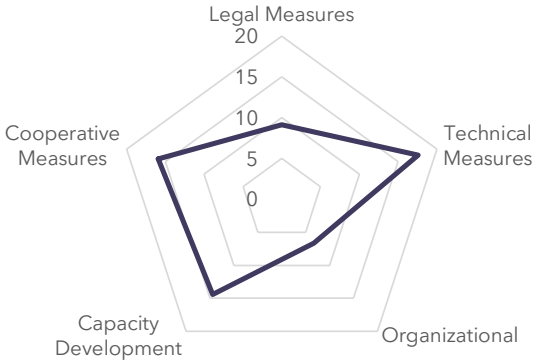
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.83	17.20	9.39	15.84	11.07	15.33

Source: ITU Global Cybersecurity Index v4, 2021

Colombia (Republic of)



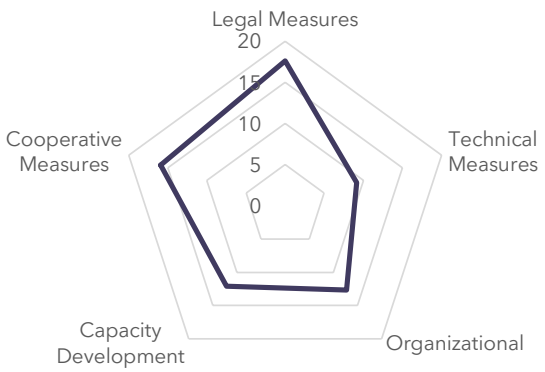
Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
63.72	9.14	17.58	6.67	14.42	15.93

Source: ITU Global Cybersecurity Index v4, 2021

Costa Rica



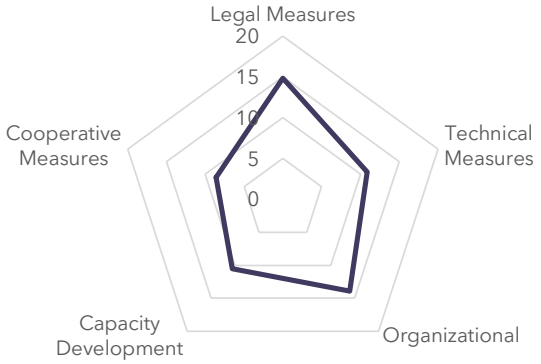
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
67.45	17.62	9.14	12.66	12.11	15.93

Source: ITU Global Cybersecurity Index v4, 2021

Cuba



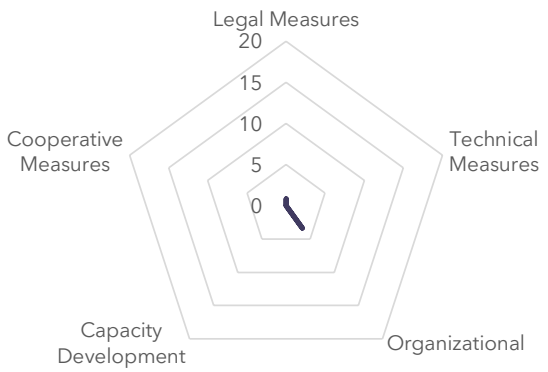
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
58.76	14.85	10.87	13.91	10.52	8.61

Source: ITU Global Cybersecurity Index v4, 2021

Dominica (Commonwealth of)



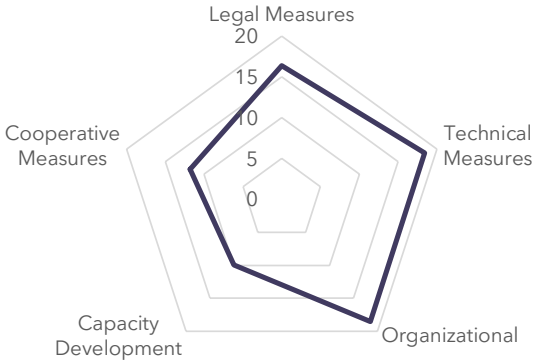
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Technical, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
4.20	0.85	0.00	3.35	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Dominican Republic



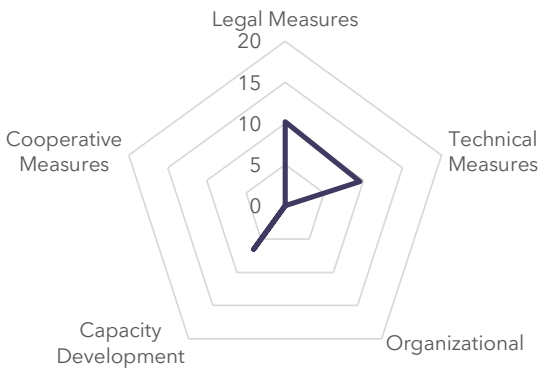
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.07	16.38	18.42	18.52	9.94	11.81

Source: ITU Global Cybersecurity Index v4, 2021

Ecuador



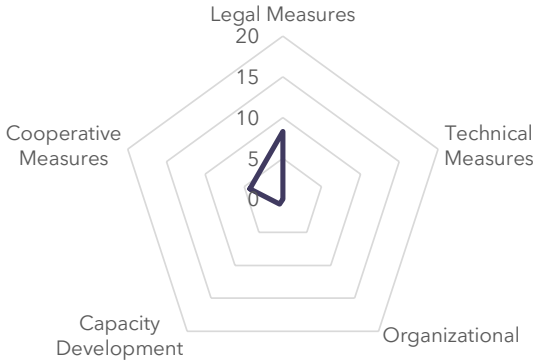
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
26.30	10.22	9.55	0.00	6.53	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*El Salvador (Republic of)***



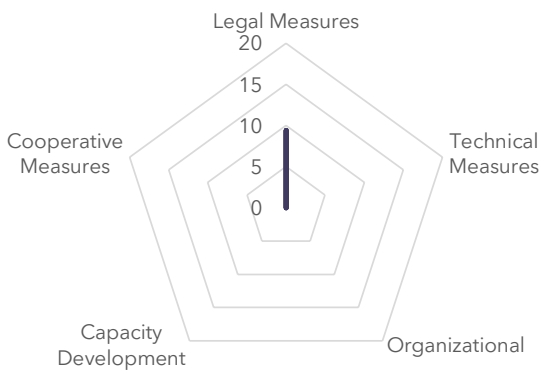
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
13.30	8.32	0.00	0.00	0.72	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Grenada



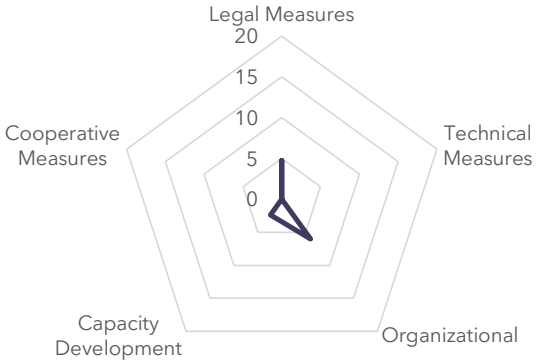
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
9.41	9.41	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Guatemala (Republic of)



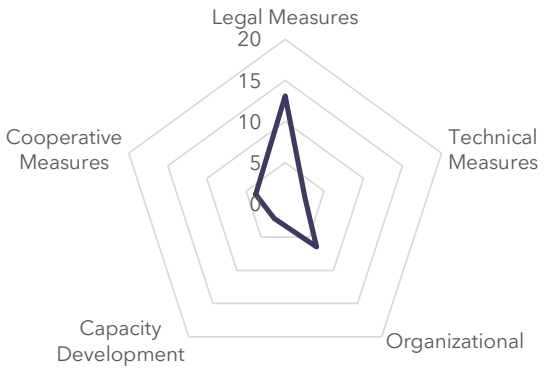
Development Level:
Developing Country

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Technical, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
13.13	4.76	0.00	6.01	2.36	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Guyana



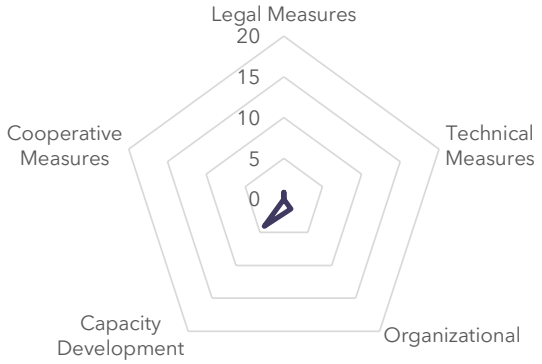
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
28.11	13.12	2.50	6.47	2.24	3.78

Source: ITU Global Cybersecurity Index v4, 2021

Haiti (Republic of)



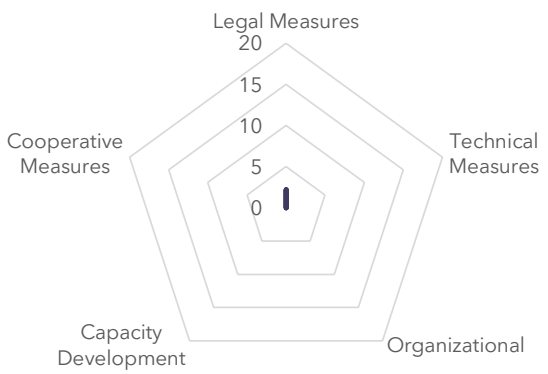
Development Level:
Developing Country, Least Developed Countries (LDC), Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
6.40	0.85	0.00	1.46	4.09	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*Honduras (Republic of)***



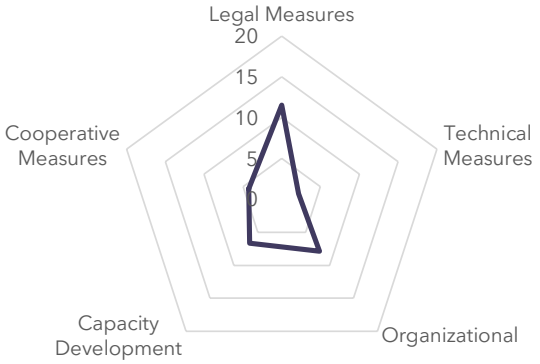
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measure
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
2.20	2.20	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*Jamaica***



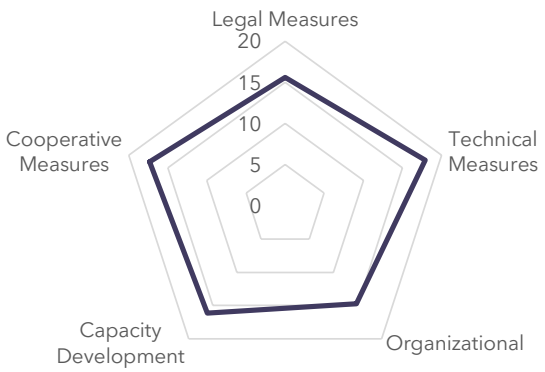
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
32.53	11.54	2.18	7.87	6.68	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Mexico



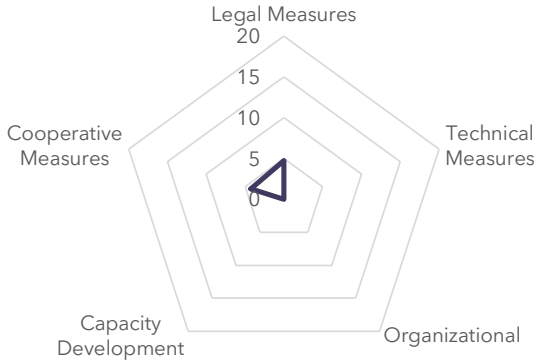
Development Level:
Developing Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.68	15.61	17.90	14.70	16.13	17.34

Source: ITU Global Cybersecurity Index v4, 2021

*Nicaragua***



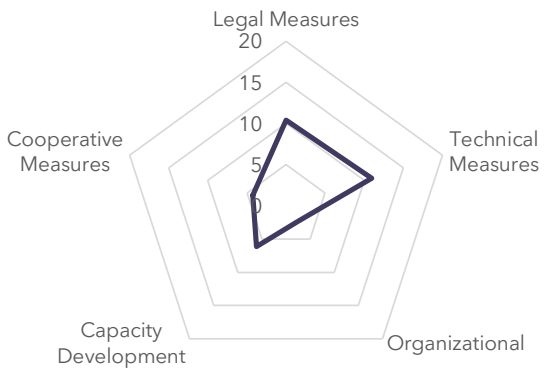
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures, Capacity Development
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures,

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
9.00	4.74	0.00	0.00	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Panama (Republic of)



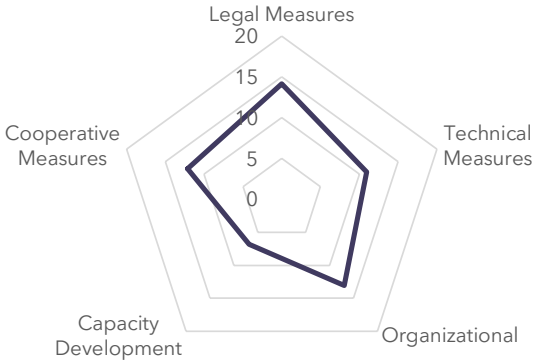
Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures, Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
34.11	10.41	10.94	2.37	6.12	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Paraguay (Republic of)



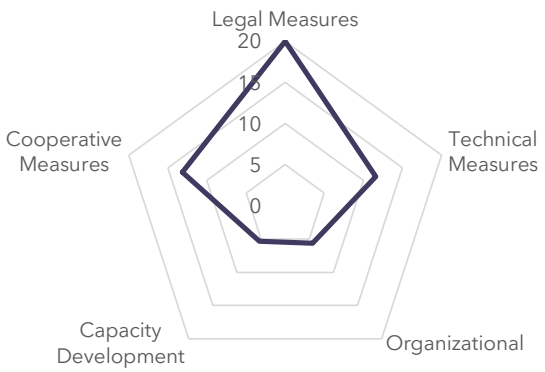
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
57.09	14.15	10.94	13.06	6.79	12.14

Source: ITU Global Cybersecurity Index v4, 2021

Peru



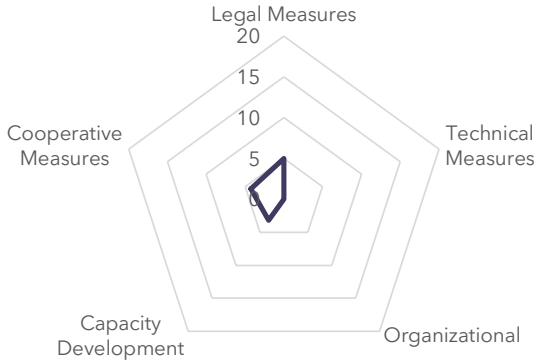
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
55.67	20.00	11.58	5.63	5.32	13.15

Source: ITU Global Cybersecurity Index v4, 2021

Saint Kitts and Nevis (Federation of)



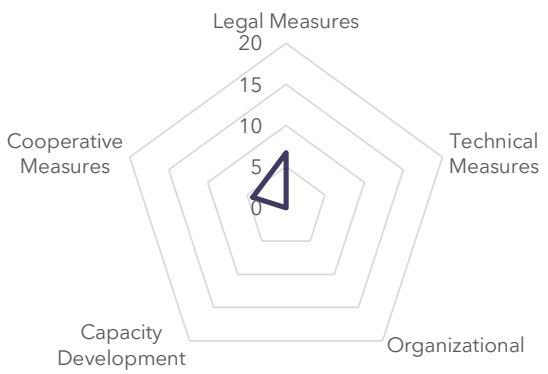
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
12.44	5.00	0.00	0.00	3.18	4.26

Source: ITU Global Cybersecurity Index v4, 2021

*Saint Lucia***



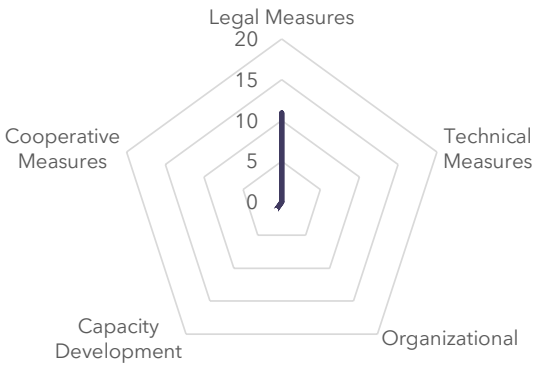
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
10.96	6.70	0.00	0.00	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

*Saint Vincent and the Grenadines***



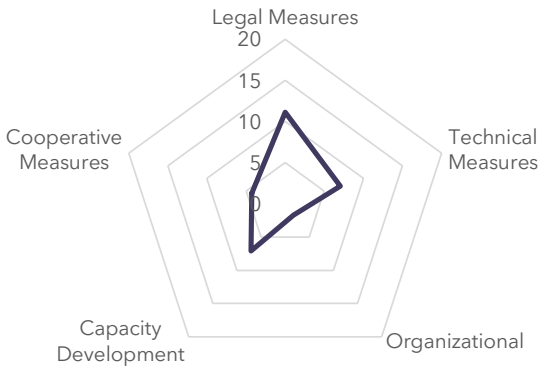
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
12.18	10.95	0.00	0.00	1.23	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Suriname (Republic of)



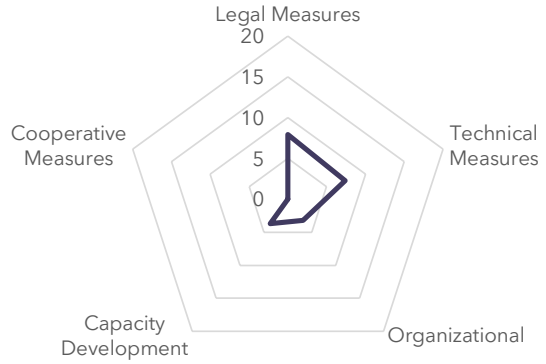
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
31.20	11.13	7.04	1.69	7.08	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Trinidad and Tobago



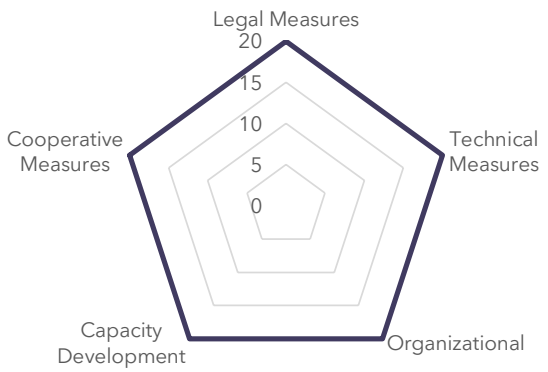
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
22.18	7.94	7.38	3.18	3.69	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*United States of America***



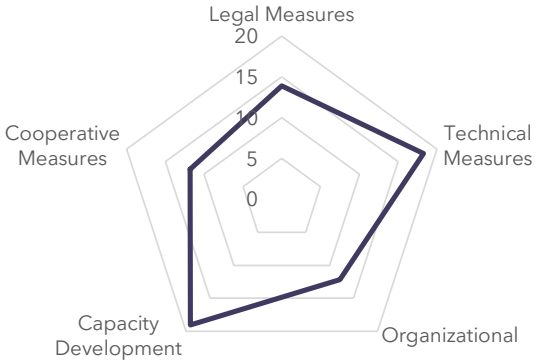
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
N/A

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
100.00	20.00	20.00	20.00	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Uruguay (Eastern Republic of)



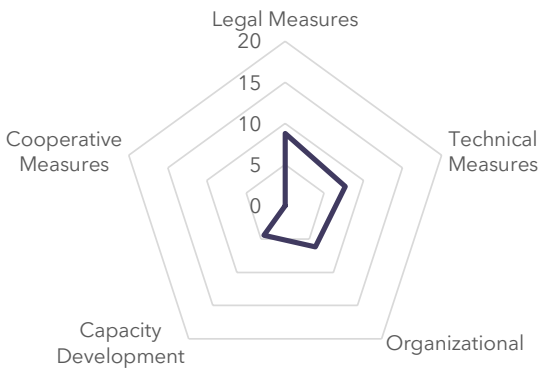
Development Level:
Developing Country

Area(s) of Relative Strength
Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Cooperative Measures	Capacity Development
75.15	13.90	18.27	12.13	19.04	11.81

Source: ITU Global Cybersecurity Index v4, 2021

Venezuela (Bolivarian Republic of)



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Cooperative Measures	Capacity Development
27.06	8.80	7.67	6.17	4.41	0.00

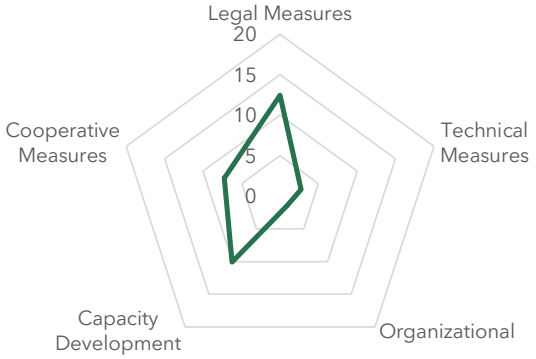
Source: ITU Global Cybersecurity Index v4, 2021

** no response to the questionnaire/data collected by GCI Team

* no data

Arab States region

Algeria (People's Democratic Republic of)



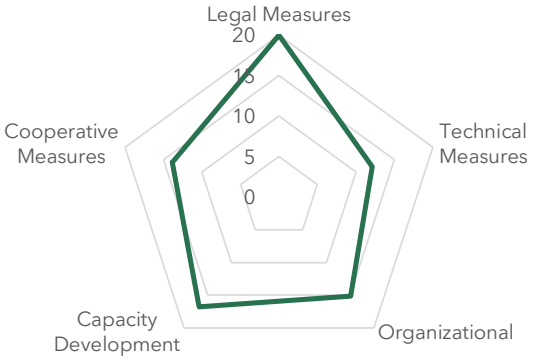
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
33.95	12.46	2.73	1.44	10.07	7.25

Source: ITU Global Cybersecurity Index v4, 2021

Bahrain (Kingdom of)



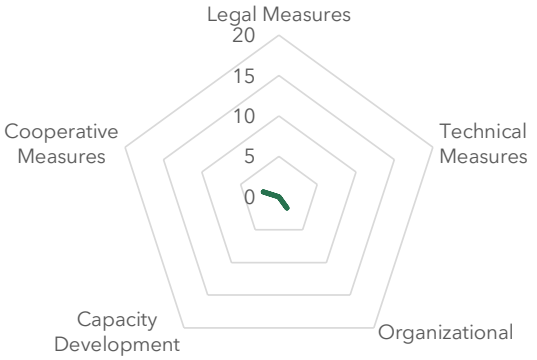
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
77.86	20.00	12.12	15.11	16.77	13.86

Source: ITU Global Cybersecurity Index v4, 2021

*Comoros (Union of the)***



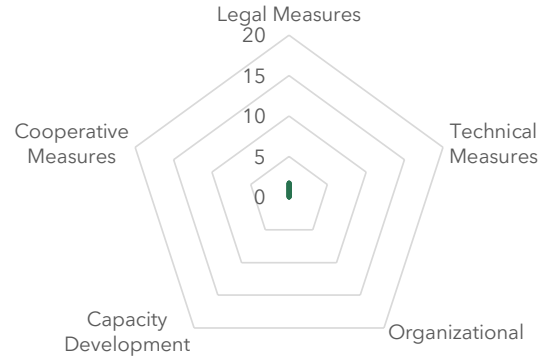
Development Level:
Developing Country, Least Developed Countries (LDC), Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Legal, Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
3.72	0.00	0.00	1.69	0.00	2.04

Source: ITU Global Cybersecurity Index v4, 2021

Djibouti (Republic of)



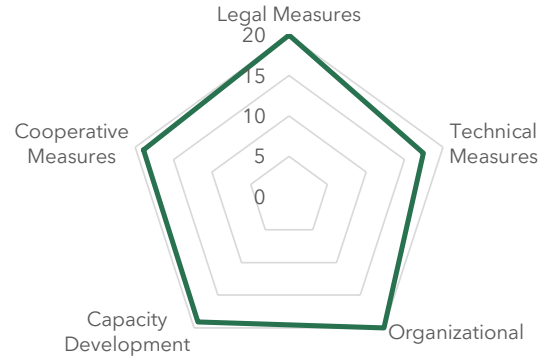
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, and Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
1.73	1.73	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Egypt (Arab Republic of)



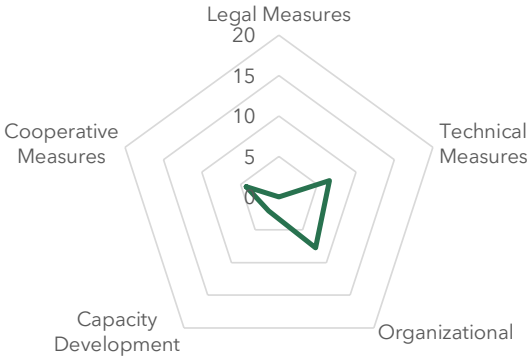
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Organizational Measures, Capacity Development
Area(s) of Potential Growth

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
95.48	20.00	17.45	20.00	19.12	18.91

Source: ITU Global Cybersecurity Index v4, 2021

*Iraq (Republic of)***



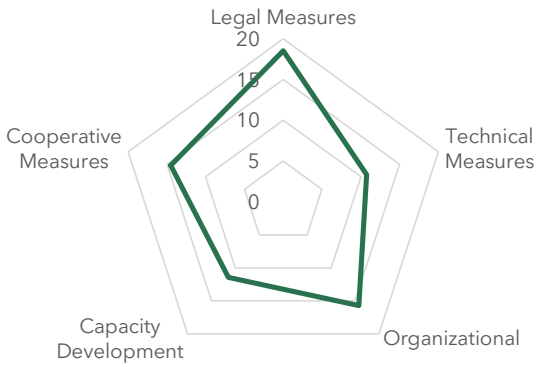
Development Level:
Developing Country

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
20.71	0.00	6.56	7.75	2.14	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Jordan (Hashemite Kingdom of)



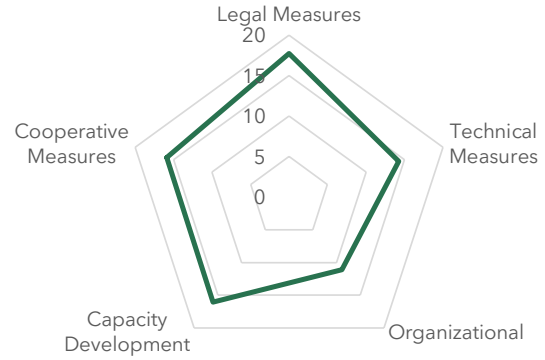
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
70.96	18.53	10.74	15.70	11.47	14.51

Source: ITU Global Cybersecurity Index v4, 2021

Kuwait (State of)



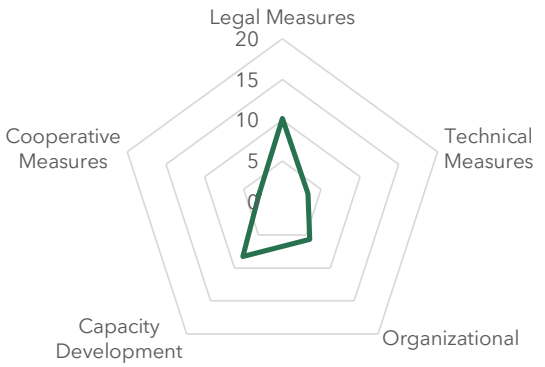
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.05	17.74	14.25	11.13	16.05	15.90

Source: ITU Global Cybersecurity Index v4, 2021

*Lebanon***



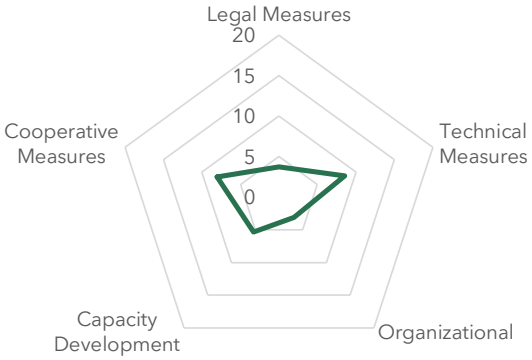
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
30.44	10.24	3.27	5.69	8.26	2.99

Source: ITU Global Cybersecurity Index v4, 2021

Libya (State of)



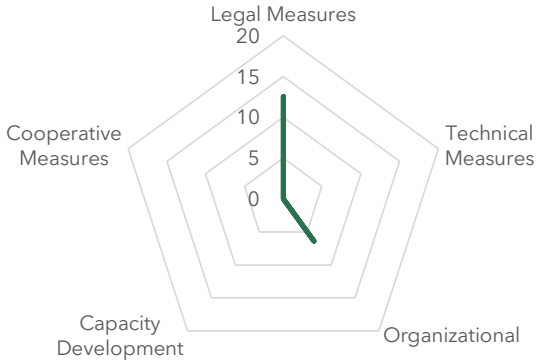
Development Level:
Developing Country

Area(s) of Relative Strength
Technical, Cooperative Measures
Area(s) of Potential Growth
Legal, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
28.78	3.73	8.54	3.13	5.34	8.04

Source: ITU Global Cybersecurity Index v4, 2021

Mauritania (Islamic Republic of)



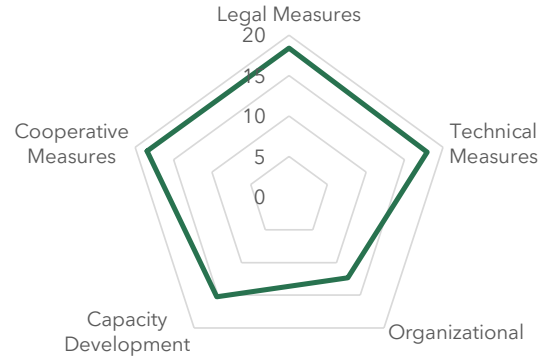
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
18.94	12.55	0.00	6.39	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Morocco (Kingdom of)



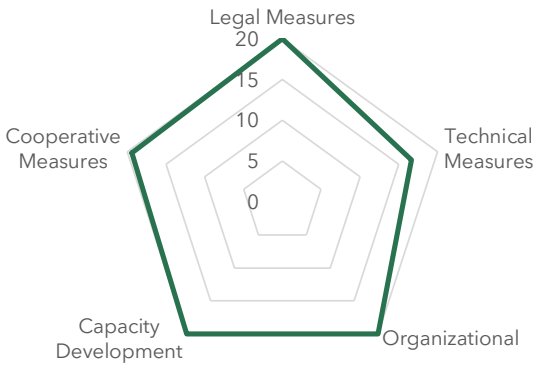
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
82.41	18.40	17.94	12.37	15.24	18.46

Source: ITU Global Cybersecurity Index v4, 2021

Oman (Sultanate of)



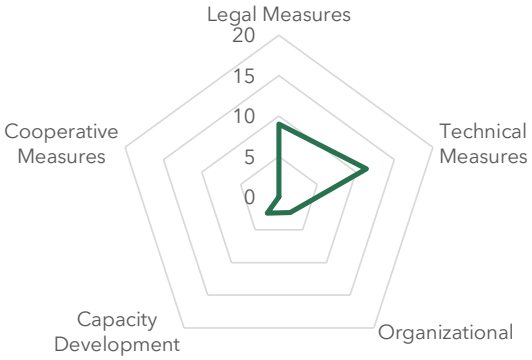
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Organizational Measures, Capacity Development
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.04	20.00	16.64	20.00	20.00	96.04

Source: ITU Global Cybersecurity Index v4, 2021

State of Palestine



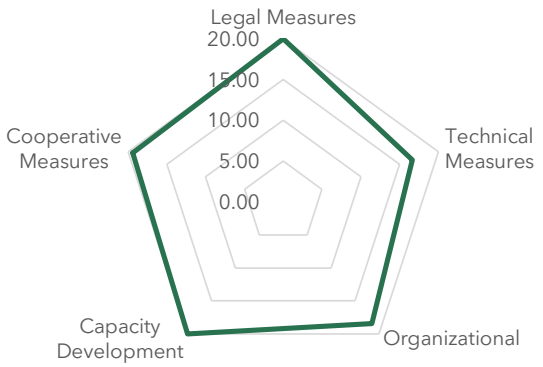
Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
25.18	9.02	11.36	2.34	2.46	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Qatar (State of)



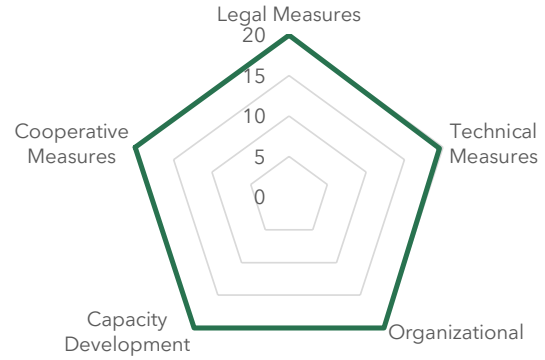
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures, Capacity Development
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.50	20.00	16.64	18.46	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Saudi Arabia (Kingdom of)



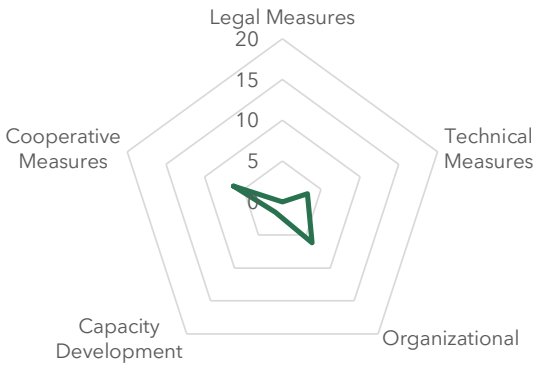
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
99.54	20.00	19.54	20.00	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Somalia (Federal Republic of)



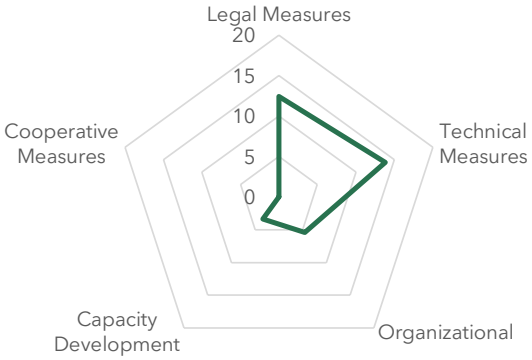
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Organizational, Cooperative Measures
Area(s) of Potential Growth
Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
17.25	0.00	3.25	6.17	1.52	6.31

Source: ITU Global Cybersecurity Index v4, 2021

Sudan (Republic of the)



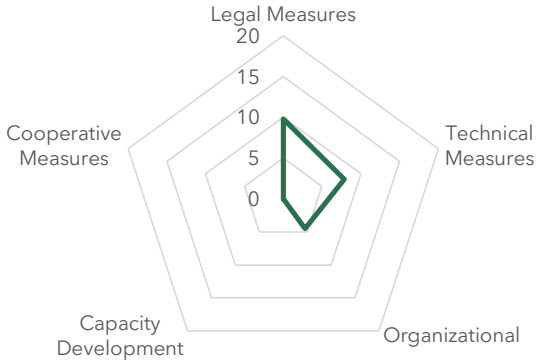
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
35.03	12.43	13.81	5.41	3.38	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*Syrian Arab Republic***



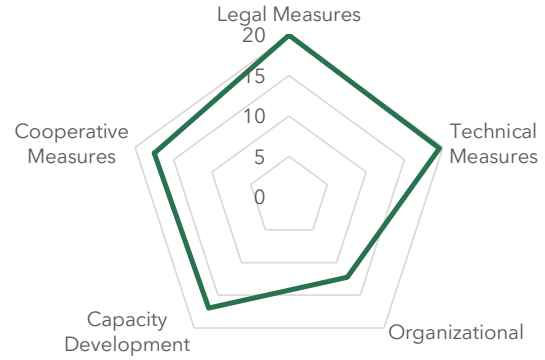
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
22.14	9.80	7.85	4.49	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Tunisia



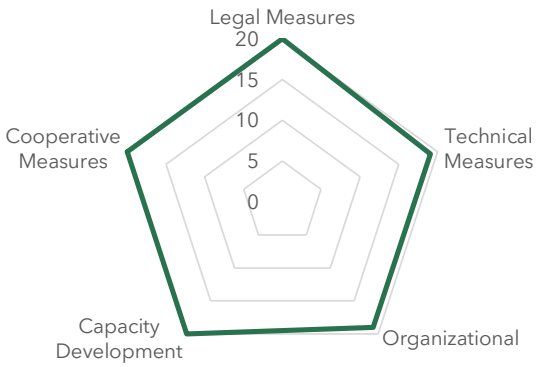
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures, Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
86.23	20.00	19.54	12.21	16.96	17.52

Source: ITU Global Cybersecurity Index v4, 2021

United Arab Emirates



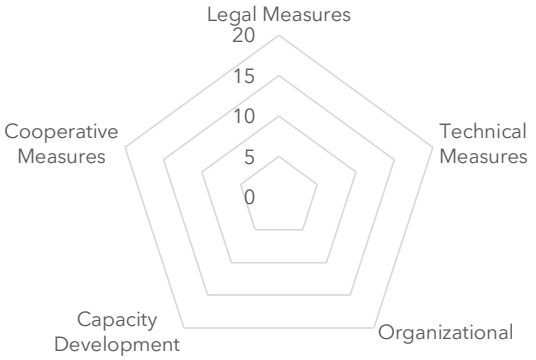
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.06	20.00	19.08	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

*Yemen (Republic of)**



Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
N/A
Area(s) of Potential Growth
N/A

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
0	0	0	0	0	0

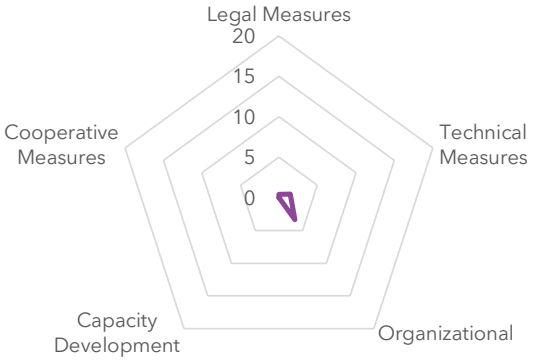
Source: ITU Global Cybersecurity Index v4, 2021

** no response to the questionnaire/data collected by GCI Team

* no data

Asia-Pacific region

Afghanistan



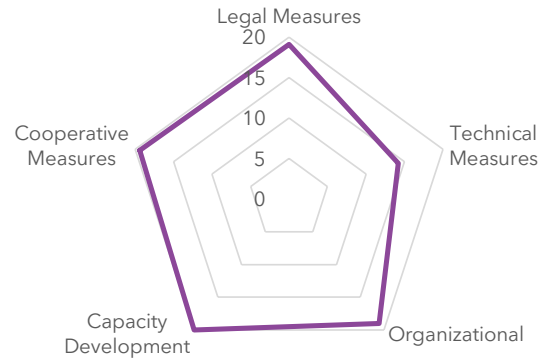
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Capacity Development, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
5.20	0.40	1.46	3.35	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Australia



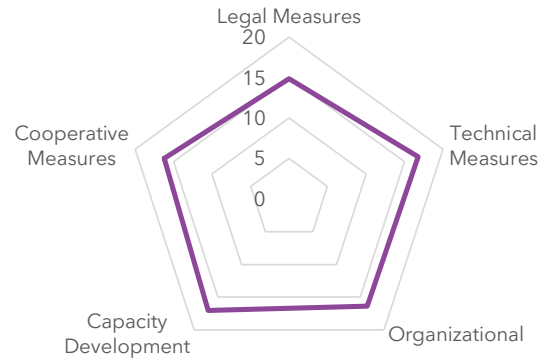
Development Level:
Developed Country

Area(s) of Relative Strength
Capacity Development, Cooperative Measures, Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.47	20.00	19.08	18.98	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Bangladesh (People's Republic of)



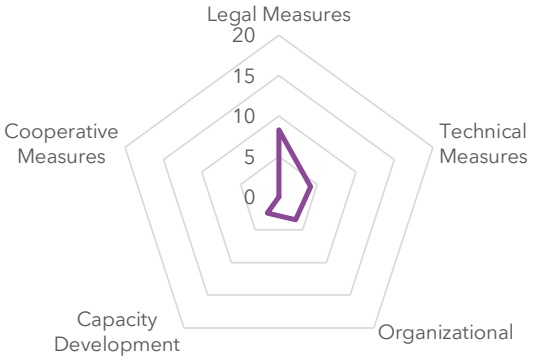
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Capacity Development, Technical Measures
Area(s) of Potential Growth
Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.27	14.86	16.77	16.39	17.03	16.22

Source: ITU Global Cybersecurity Index v4, 2021

Bhutan (Kingdom of)



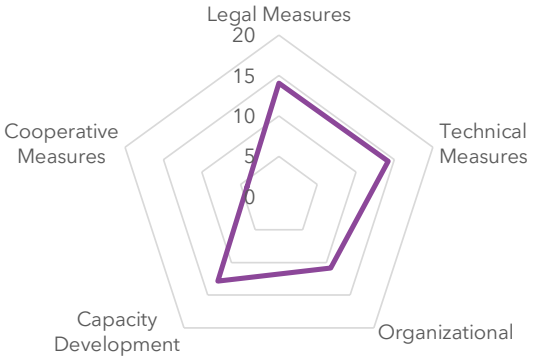
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
18.34	8.30	4.12	3.47	2.45	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Brunei Darussalam



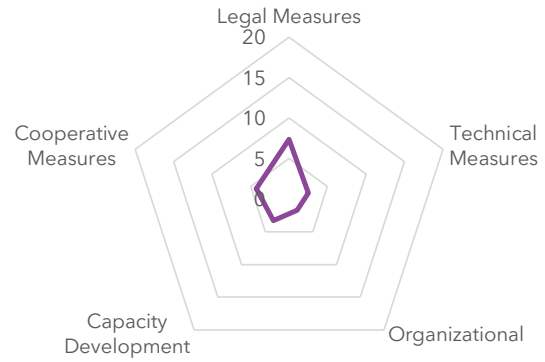
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
56.07	14.06	14.19	10.84	12.85	4.12

Source: ITU Global Cybersecurity Index v4, 2021

*Cambodia (Kingdom of)***



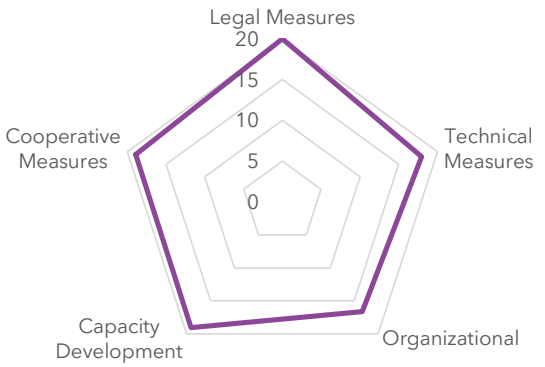
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
19.12	7.38	2.50	1.69	3.29	4.26

Source: ITU Global Cybersecurity Index v4, 2021

China (People's Republic of)



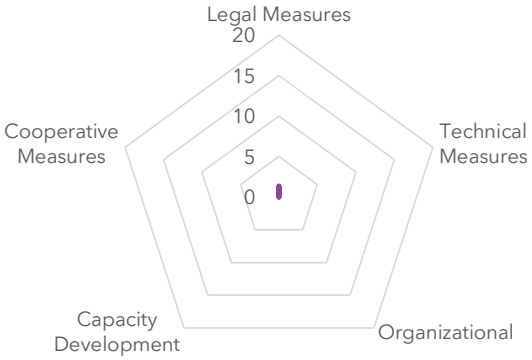
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
92.53	20.00	17.94	16.63	19.04	18.91

Source: ITU Global Cybersecurity Index v4, 2021

*Democratic People's Republic of Korea***



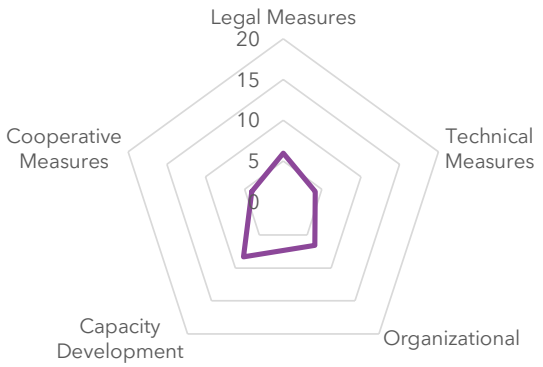
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
1.35	1.35	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

Fiji (Republic of)



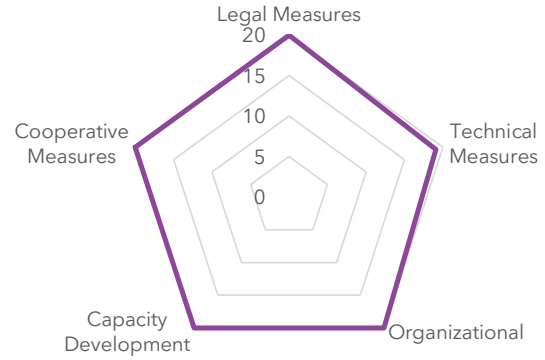
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Capacity Development
Area(s) of Potential Growth
Technical, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
29.08	5.99	4.11	6.59	8.31	4.07

Source: ITU Global Cybersecurity Index v4, 2021

India (Republic of)



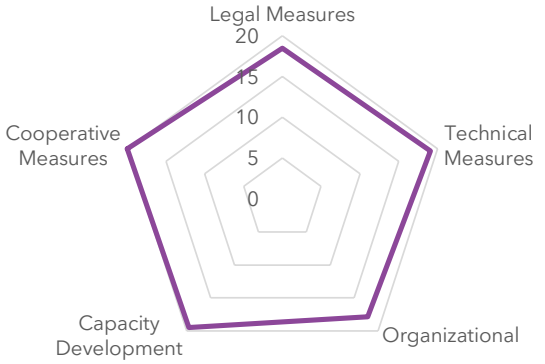
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.49	20.00	19.08	18.41	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Indonesia (Republic of)



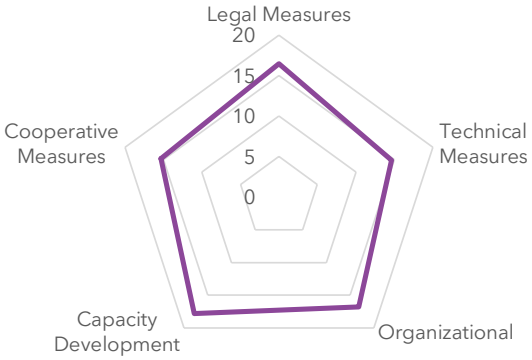
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Cooperative, Technical Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.88	18.48	19.08	17.84	19.48	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Iran (Islamic Republic of)



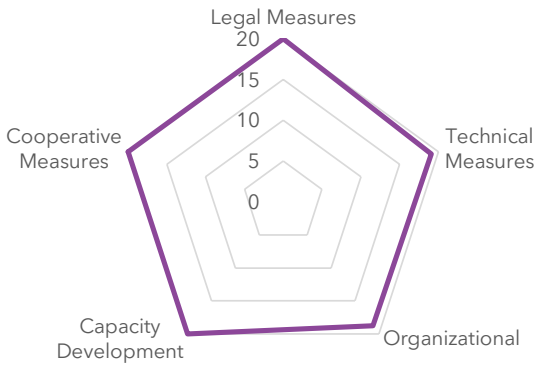
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Capacity Development, Organizational Measures
Area(s) of Potential Growth
Technical, Legal, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.06	16.48	14.63	16.82	17.80	15.33

Source: ITU Global Cybersecurity Index v4, 2021

Korea (Republic of)



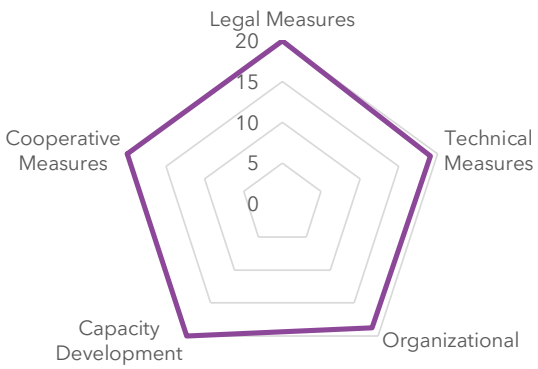
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.52	20.00	19.54	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Japan



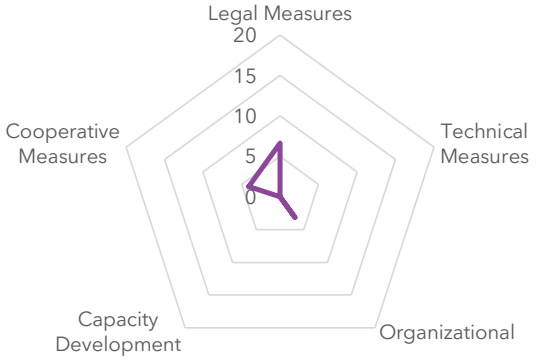
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.82	20.00	19.08	18.74	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Kiribati (Republic of)



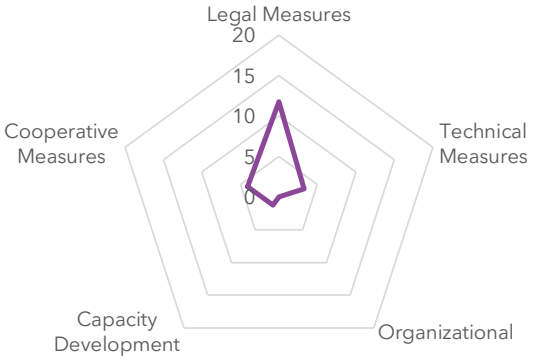
Development Level:
Developing Country, Least Developed Countries (LDC), Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
13.84	6.64	0.00	3.13	0.00	4.07

Source: ITU Global Cybersecurity Index v4, 2021

Lao People's Democratic Republic



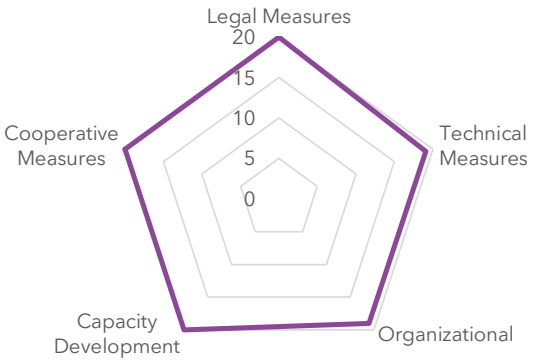
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
20.34	11.77	3.27	0.00	1.23	4.07

Source: ITU Global Cybersecurity Index v4, 2021

Malaysia



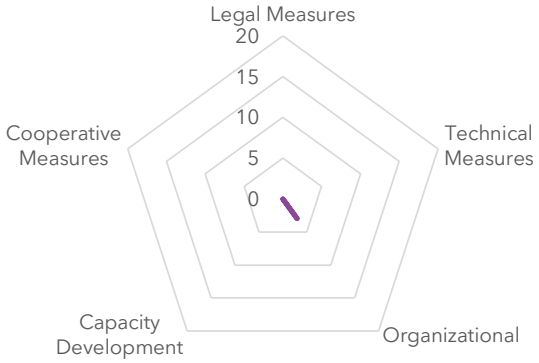
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.06	20.00	19.08	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

*Maldives (Republic of)***



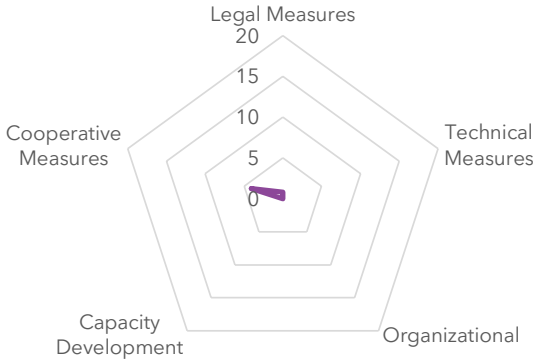
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Legal, Technical, Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
2.95	0.00	0.00	2.95	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*Marshall Islands (Republic of the)***



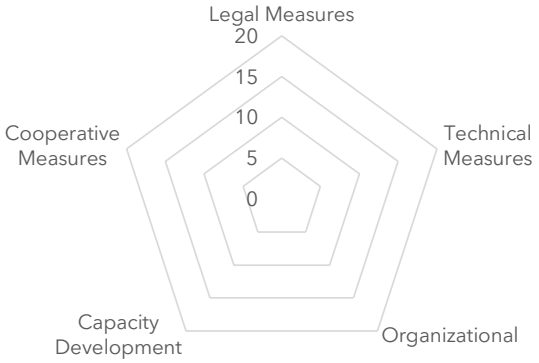
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical, Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
4.90	0.83	0.00	0.00	0.00	4.07

Source: ITU Global Cybersecurity Index v4, 2021

*Micronesia (Federated States of)**



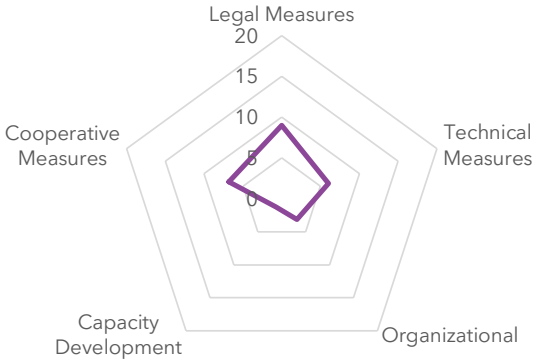
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
N/A
Area(s) of Potential Growth
N/A

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
0	0	0	0	0	0

Source: ITU Global Cybersecurity Index v4, 2021

Mongolia



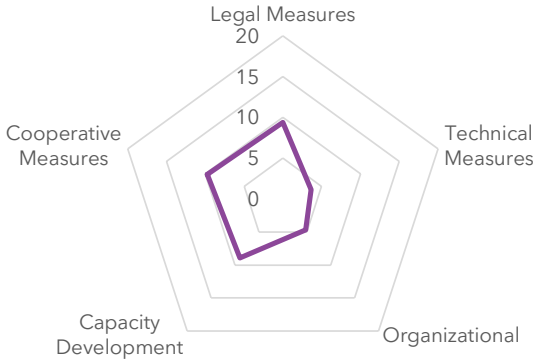
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
26.20	9.00	6.02	3.13	1.23	6.82

Source: ITU Global Cybersecurity Index v4, 2021

Myanmar (Union of)



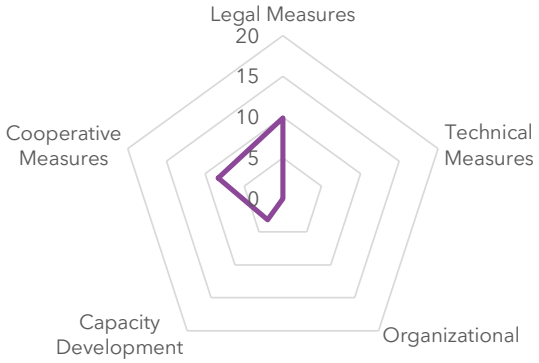
Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Cooperative, Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
36.41	9.39	3.64	4.71	8.92	9.75

Source: ITU Global Cybersecurity Index v4, 2021

*Nauru (Republic of)***



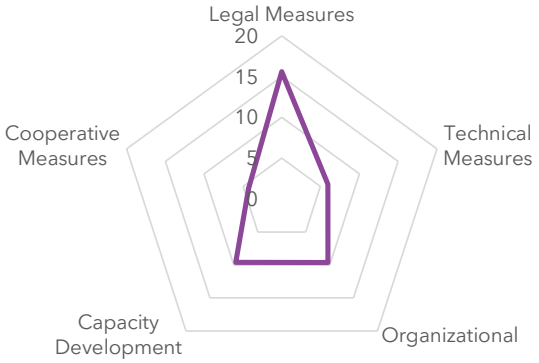
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
21.42	9.91	0.00	0.00	3.18	8.33

Source: ITU Global Cybersecurity Index v4, 2021

*Nepal (Federal Democratic Republic of)***



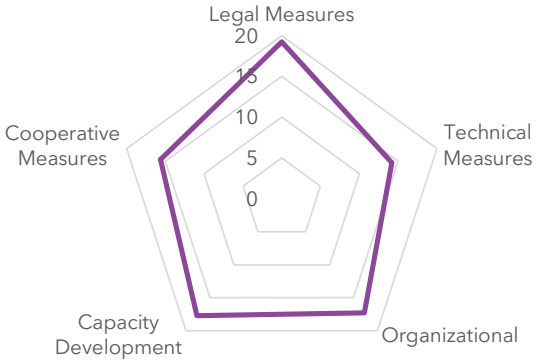
Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
44.99	15.61	5.94	9.58	9.60	4.26

Source: ITU Global Cybersecurity Index v4, 2021

*New Zealand***



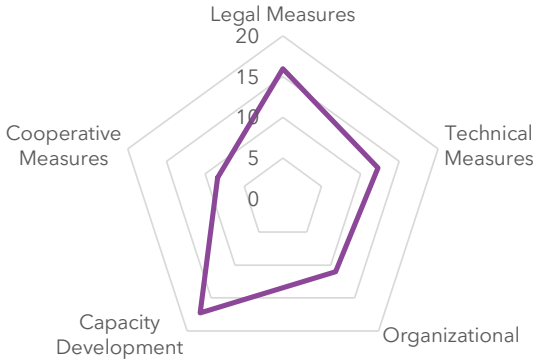
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
84.04	19.24	14.19	17.27	17.71	15.63

Source: ITU Global Cybersecurity Index v4, 2021

Pakistan (Islamic Republic of)



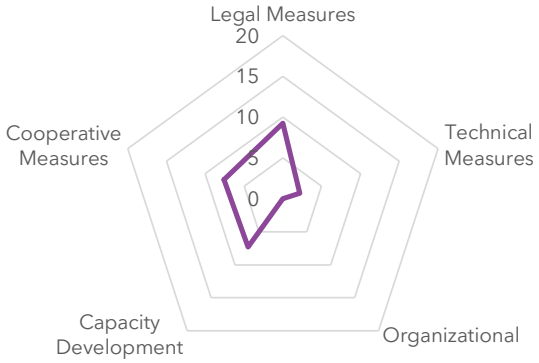
Development Level:
Developing Country

Area(s) of Relative Strength
Capacity Development
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
64.88	15.97	12.26	11.01	17.25	8.38

Source: ITU Global Cybersecurity Index v4, 2021

*Papua New Guinea***



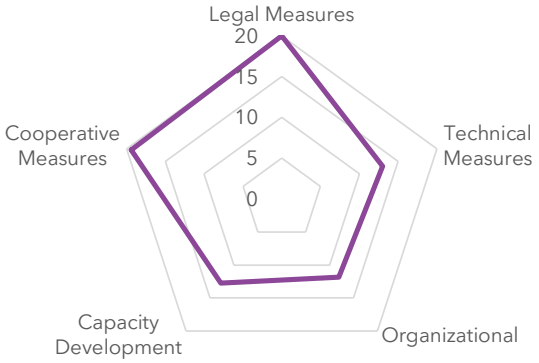
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Capacity Development
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
26.33	9.26	2.18	0.00	7.30	7.59

Source: ITU Global Cybersecurity Index v4, 2021

Philippines (Republic of the)



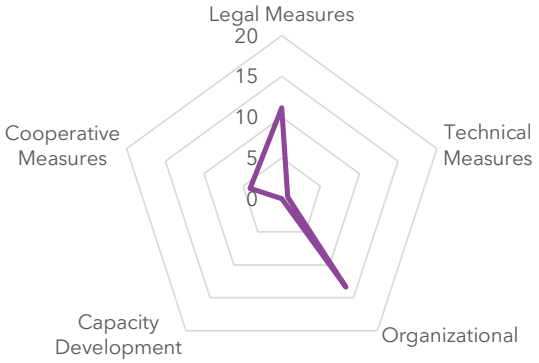
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
77.00	20.00	13.00	11.85	12.74	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Samoa (Independent State of)



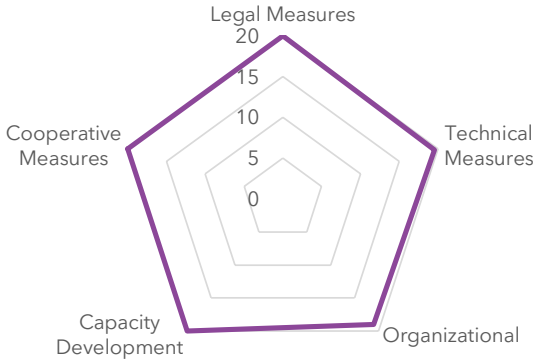
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Capacity Development, Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
29.33	11.15	0.73	13.37	0.00	4.07

Source: ITU Global Cybersecurity Index v4, 2021

Singapore (Republic of)



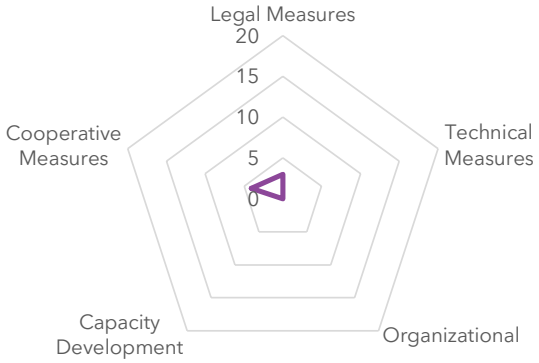
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.52	20.00	19.54	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Solomon Islands



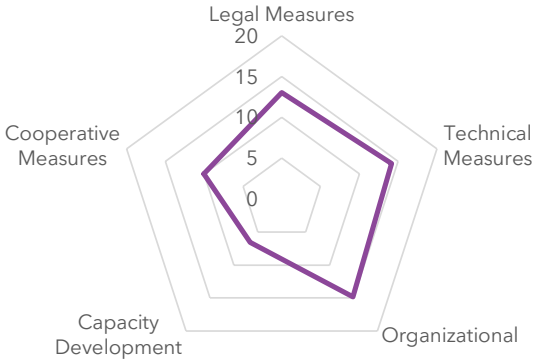
Development Level:
Developing Country, Least Developed Countries (LDC), Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures, Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
7.08	3.00	0.00	0.00	0.00	4.07

Source: ITU Global Cybersecurity Index v4, 2021

Sri Lanka (Democratic Socialist Republic of)



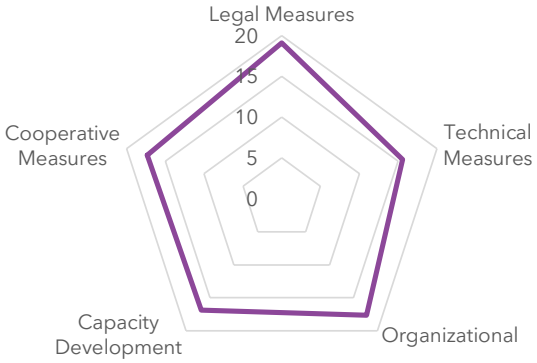
Development Level:
Developing Country

Area(s) of Relative Strength
Organizational, Technical Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
58.65	13.05	14.15	14.82	6.58	10.04

Source: ITU Global Cybersecurity Index v4, 2021

Thailand



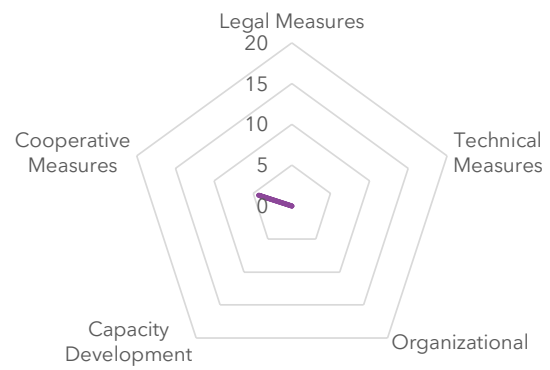
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
86.50	19.11	15.57	17.64	16.84	17.34

Source: ITU Global Cybersecurity Index v4, 2021

*Timor-Leste (Democratic Republic of)***



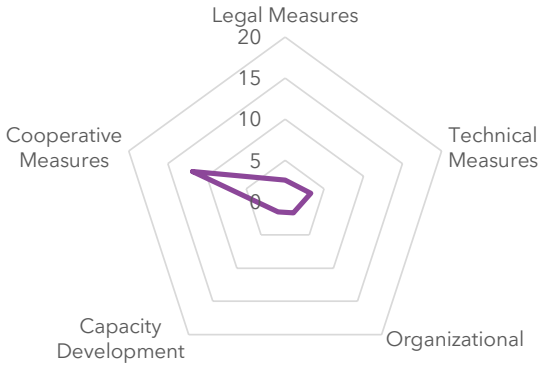
Development Level:
Developing Country, Least Developed Countries (LDC), Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Legal, Technical, Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
4.26	0.00	0.00	0.00	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

*Tonga (Kingdom of)***



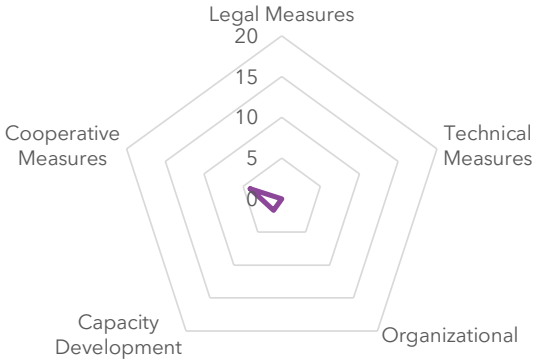
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Capacity Development, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
20.95	2.63	3.27	1.69	1.52	11.85

Source: ITU Global Cybersecurity Index v4, 2021

*Tuvalu***



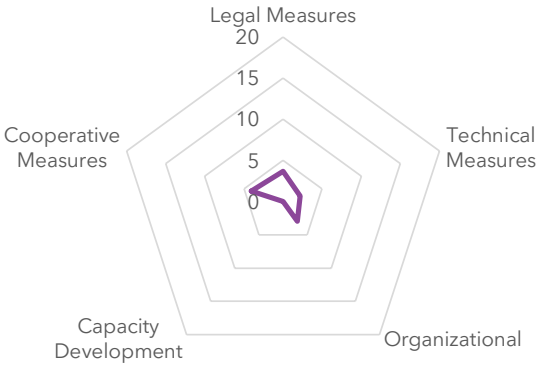
Development Level:
Developing Country, Least Developed Countries (LDC), Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Legal, Technical, Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
5.78	0.00	0.00	0.00	1.71	4.07

Source: ITU Global Cybersecurity Index v4, 2021

Vanuatu (Republic of)



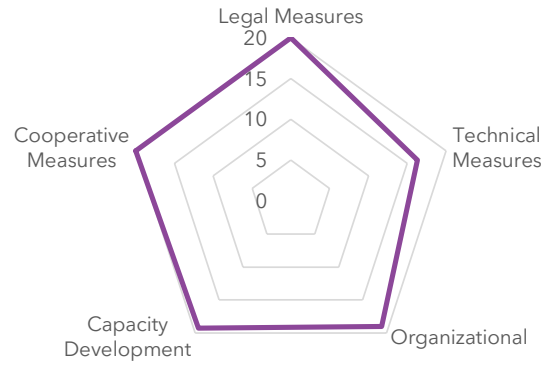
Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
12.88	3.69	2.18	2.95	0.00	4.07

Source: ITU Global Cybersecurity Index v4, 2021

Viet Nam (Socialist Republic of)



Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Cooperative Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.55	20.00	16.31	18.98	19.26	20.00

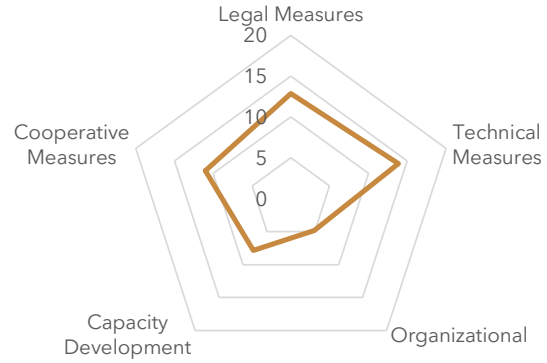
Source: ITU Global Cybersecurity Index v4, 2021

** no response to the questionnaire/data collected by GCI Team

* no data

Commonwealth of Independent States region

*Armenia (Republic of)***



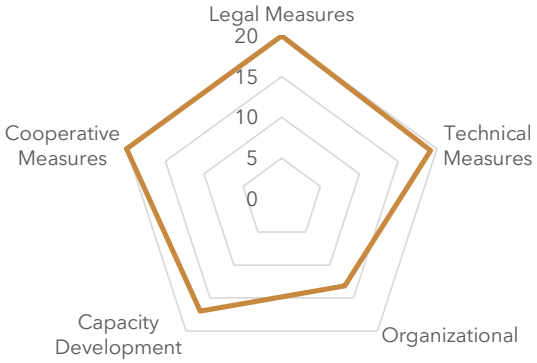
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
50.47	12.87	13.86	4.87	7.85	11.02

Source: ITU Global Cybersecurity Index v4, 2021

Azerbaijan (Republic of)



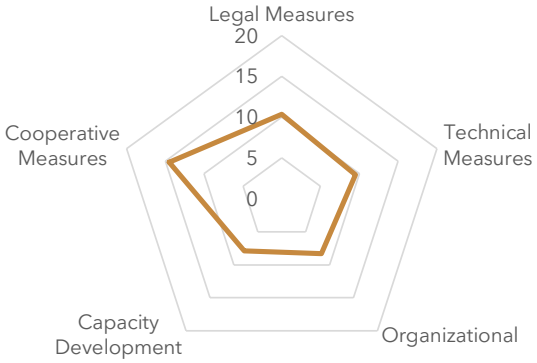
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
89.31	20.00	19.19	13.14	16.99	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Belarus (Republic of)



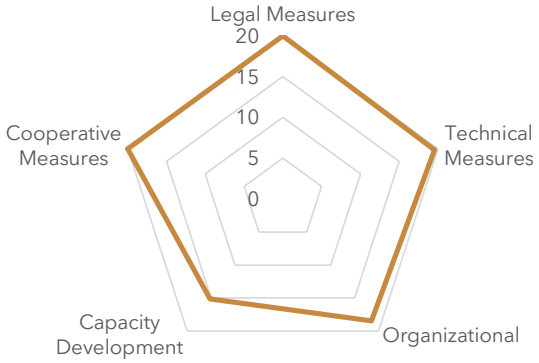
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
50.57	10.36	9.50	8.31	7.88	14.51

Source: ITU Global Cybersecurity Index v4, 2021

Kazakhstan (Republic of)



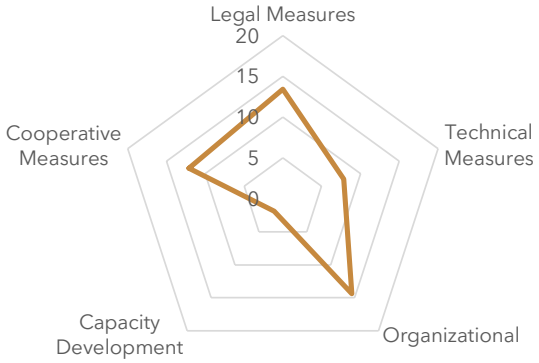
Development Level:
Developing Country

Area(s) of Relative Strength
Cooperative, Technical Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
93.15	20.00	19.54	18.46	15.15	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Kyrgyz Republic



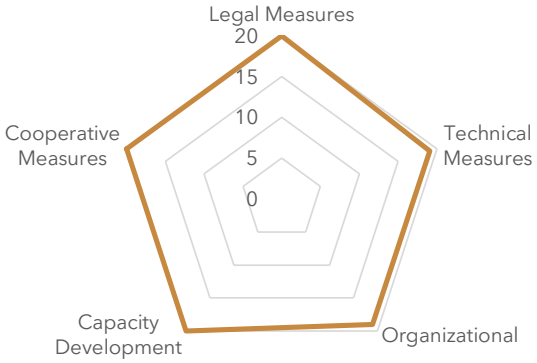
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Organizational, Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
49.64	13.43	7.85	14.37	1.87	12.11

Source: ITU Global Cybersecurity Index v4, 2021

Russian Federation



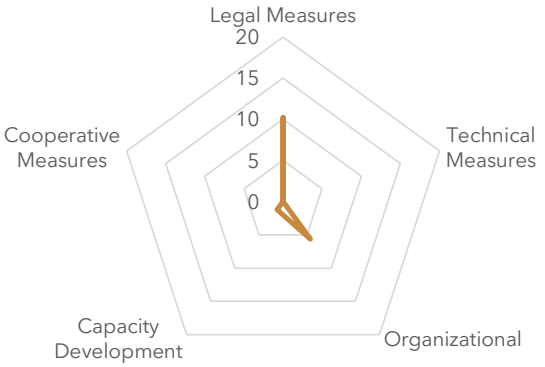
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.06	20.00	19.08	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

*Tajikistan (Republic of)***



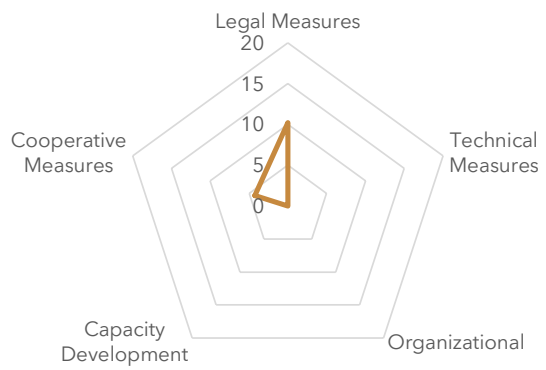
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
17.10	10.22	0.00	5.63	1.25	0.00

Source: ITU Global Cybersecurity Index v4, 2021

*Turkmenistan***



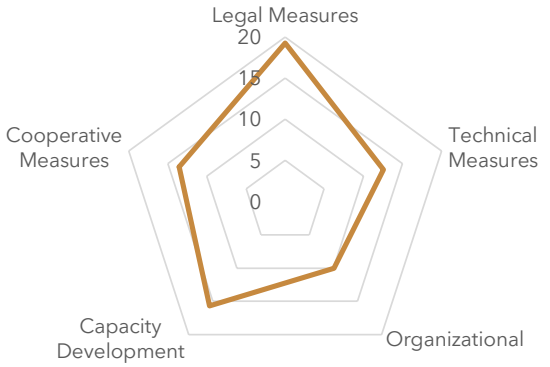
Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical, Organizational Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
14.48	10.22	0.00	0.00	0.00	4.26

Source: ITU Global Cybersecurity Index v4, 2021

Uzbekistan (Republic of)



Development Level:
Developing Country, Landlocked Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
71.11	19.27	12.56	10.05	15.68	13.56

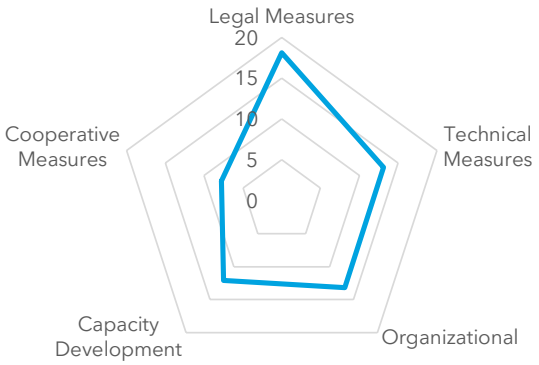
Source: ITU Global Cybersecurity Index v4, 2021

** no response to the questionnaire/data collected by GCI Team

* no data

Europe

Albania (Republic of)



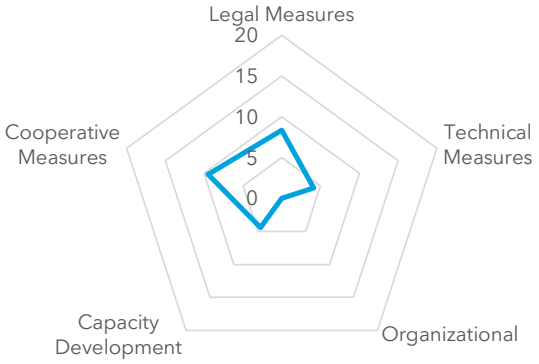
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
64.32	18.13	13.12	13.18	12.12	7.78

Source: ITU Global Cybersecurity Index v4, 2021

*Andorra (Principality of)***



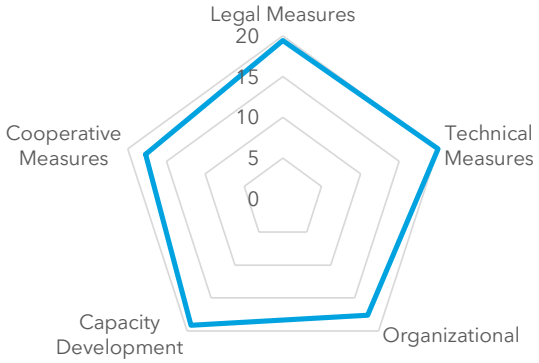
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
26.38	8.37	4.11	0.00	4.41	9.49

Source: ITU Global Cybersecurity Index v4, 2021

Austria



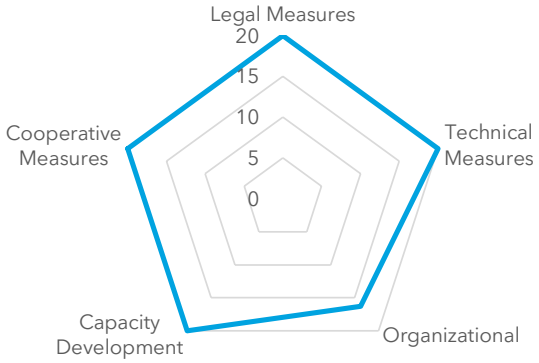
Development Level:
Developed Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
93.89	19.43	20.00	17.64	19.13	17.70

Source: ITU Global Cybersecurity Index v4, 2021

Belgium



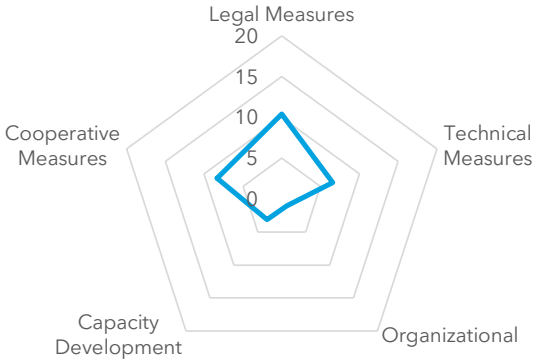
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.25	20.00	20.00	16.25	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Bosnia and Herzegovina



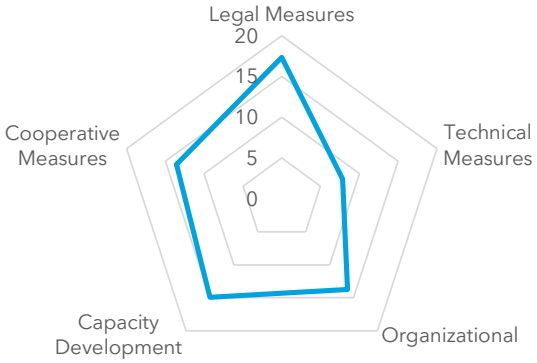
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
29.44	10.41	6.56	1.02	3.12	8.33

Source: ITU Global Cybersecurity Index v4, 2021

Bulgaria (Republic of)



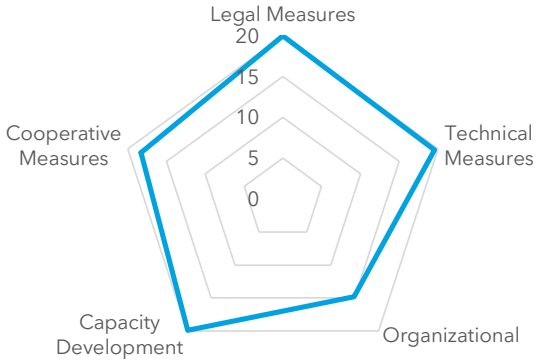
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
67.38	17.34	7.84	13.72	14.92	13.57

Source: ITU Global Cybersecurity Index v4, 2021

Croatia (Republic of)



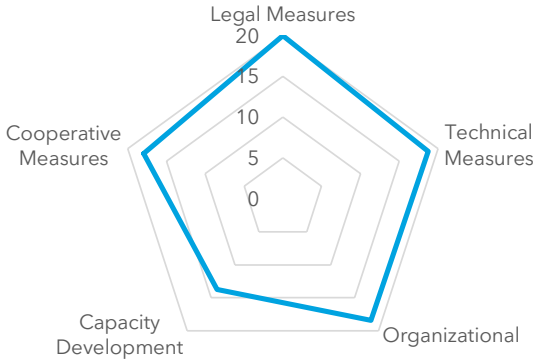
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures, Capacity Development
Area(s) of Potential Growth
Organizational, Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
92.53	20.00	19.54	14.80	19.89	18.29

Source: ITU Global Cybersecurity Index v4, 2021

Cyprus (Republic of)



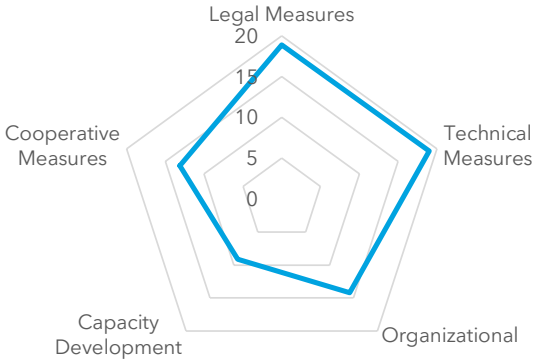
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
88.82	20.00	18.73	18.41	13.73	17.94

Source: ITU Global Cybersecurity Index v4, 2021

Czech Republic



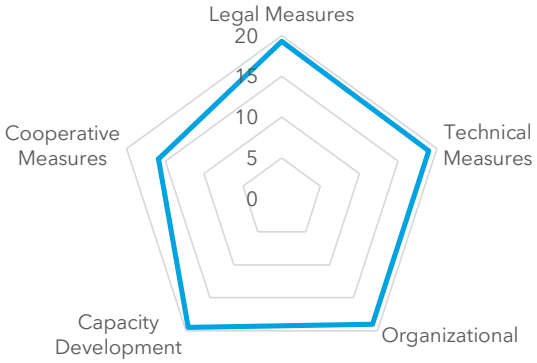
Development Level:
Developed Country

Area(s) of Relative Strength
Technical, Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
74.37	18.89	19.00	14.20	9.14	13.14

Source: ITU Global Cybersecurity Index v4, 2021

Denmark



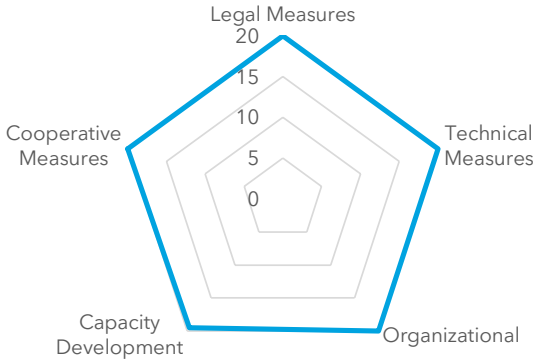
Development Level:
Developed Country

Area(s) of Relative Strength
Capacity Development, Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
92.60	19.30	18.94	18.98	19.48	15.89

Source: ITU Global Cybersecurity Index v4, 2021

Estonia (Republic of)



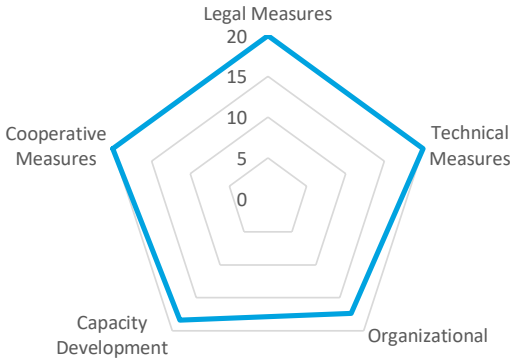
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
99.48	20.00	20.00	20.00	19.48	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Finland



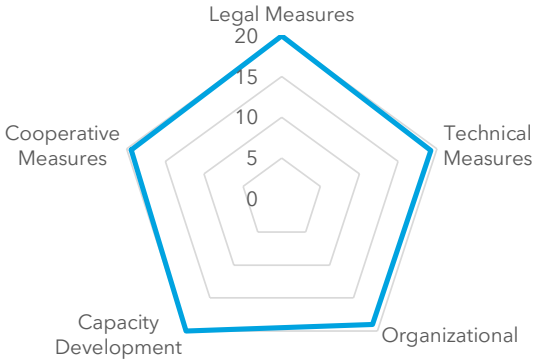
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
92.07	20.00	20.00	14.33	17.74	20.00

Source: ITU Global Cybersecurity Index v4, 2021

France



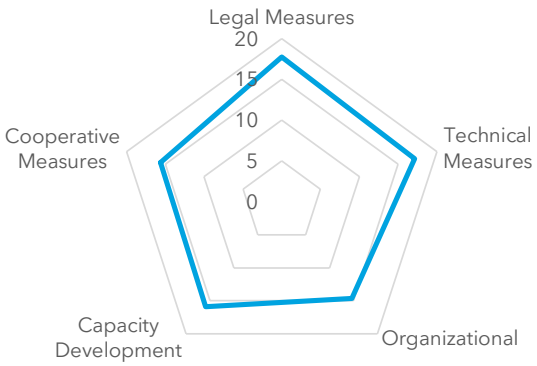
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.60	20.00	19.21	18.98	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Georgia



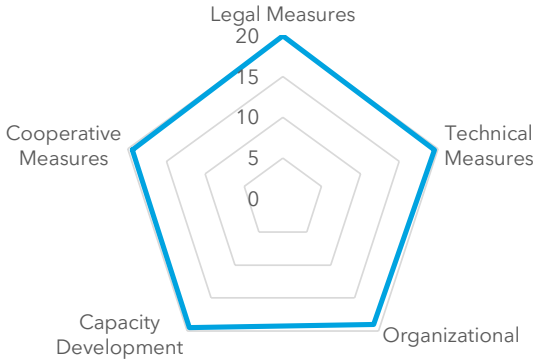
Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.07	17.75	17.13	14.67	15.89	15.63

Source: ITU Global Cybersecurity Index v4, 2021

Germany (Federal Republic of)



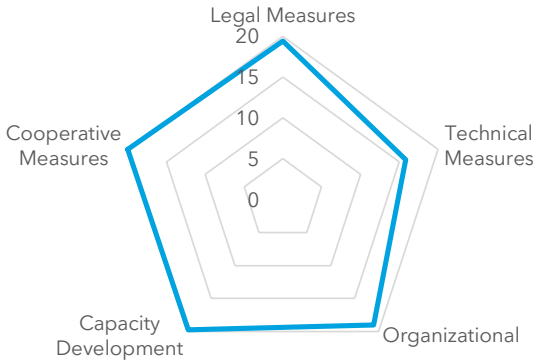
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures, Capacity Development, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.41	20.00	19.54	18.98	19.48	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Greece



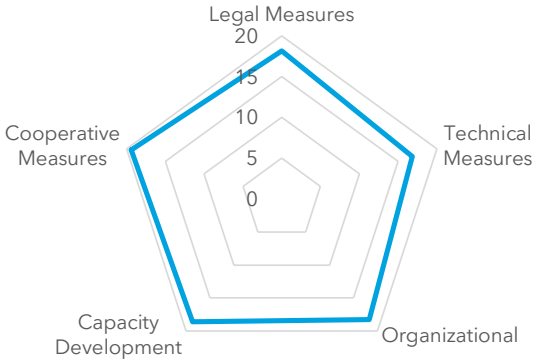
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures, Capacity Development, Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
93.98	19.43	15.83	18.98	19.74	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Hungary



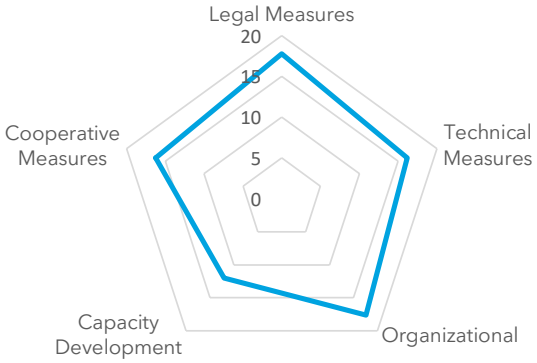
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures, Capacity Development, Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
91.28	18.16	16.82	18.29	18.60	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Iceland



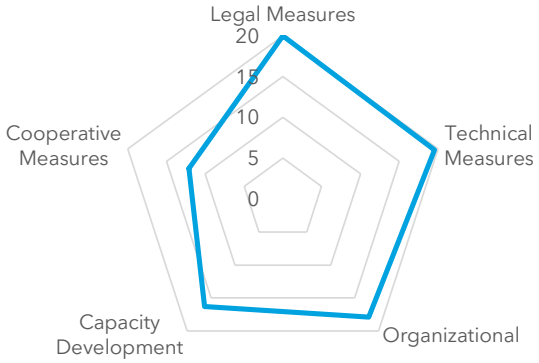
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Organizational Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
79.81	17.78	16.17	17.62	11.99	16.25

Source: ITU Global Cybersecurity Index v4, 2021

Ireland



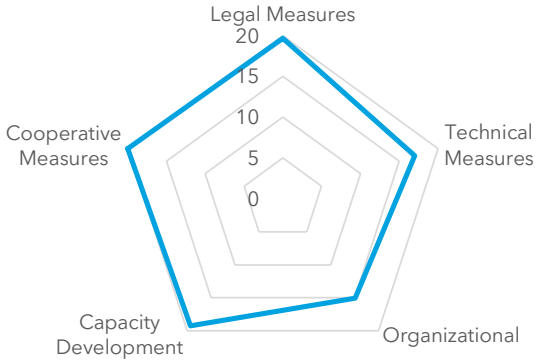
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
85.86	20.00	19.54	17.89	16.32	12.11

Source: ITU Global Cybersecurity Index v4, 2021

*Israel (State of)***



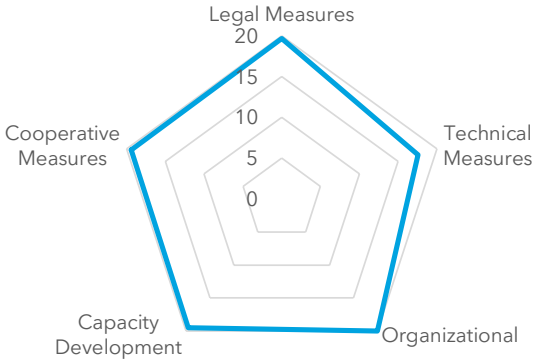
Development Level:
Developed Country

Area(s) of Relative Strength
Technical Measures, Capacity Development
Area(s) of Potential Growth
Legal, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
90.93	19.68	16.99	15.02	19.24	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Italy



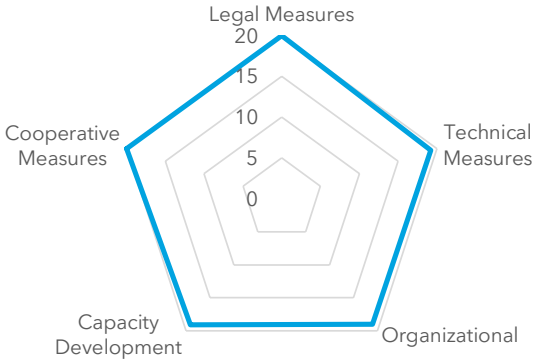
Development Level:
Developed Country

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.13	19.68	17.56	20.00	19.48	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Latvia (Republic of)



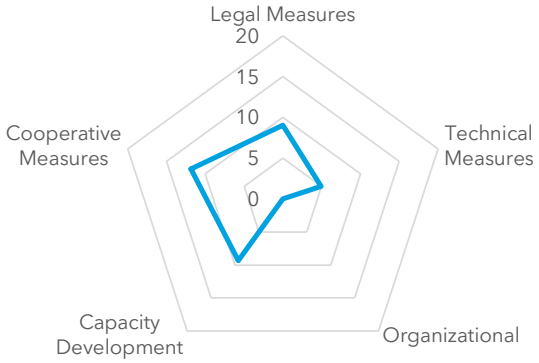
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Cooperative, Technical, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.28	20.00	19.21	18.98	19.09	20.00

Source: ITU Global Cybersecurity Index v4, 2021

*Liechtenstein (Principality of)***



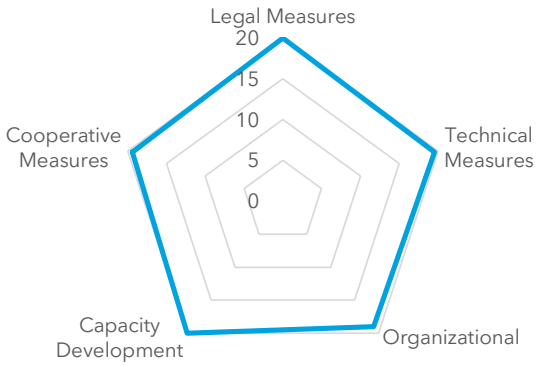
Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
35.15	9.04	4.93	0.00	9.34	11.85

Source: ITU Global Cybersecurity Index v4, 2021

Lithuania (Republic of)



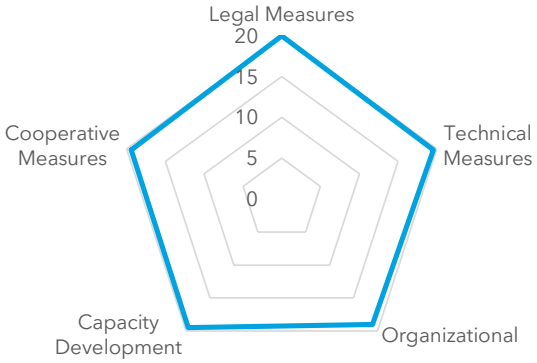
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Capacity Development, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.93	20.00	19.54	18.98	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Luxembourg



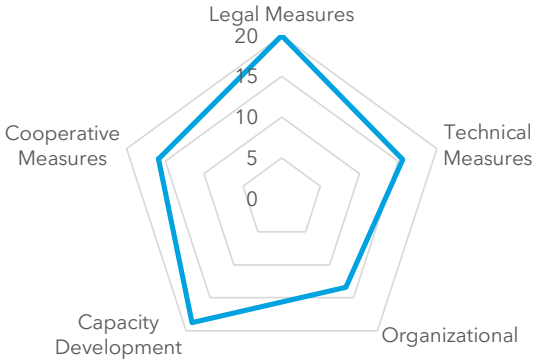
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Capacity Development, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.41	20.00	19.54	18.98	19.48	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Malta



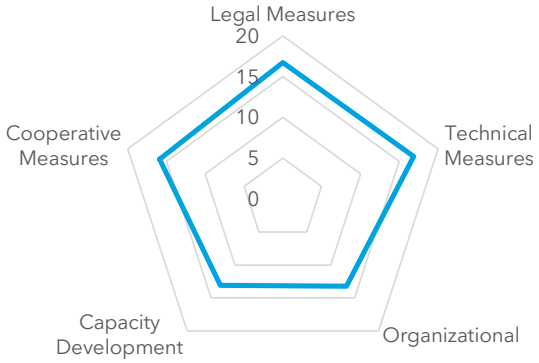
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
83.65	20.00	15.59	13.41	18.76	15.89

Source: ITU Global Cybersecurity Index v4, 2021

Moldova (Republic of)



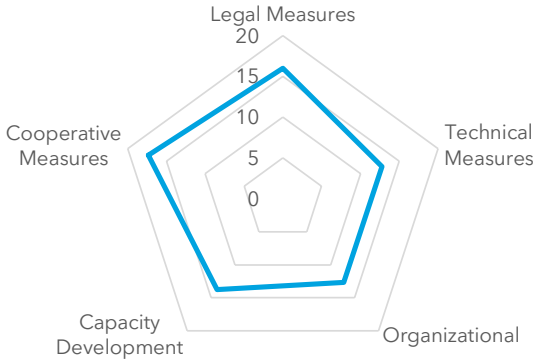
Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Organizational, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.78	16.73	16.86	13.21	13.09	15.89

Source: ITU Global Cybersecurity Index v4, 2021

Monaco (Principality of)



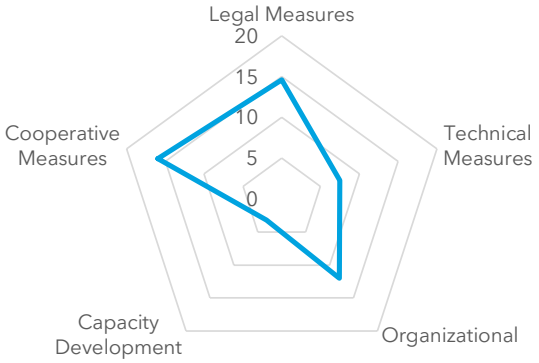
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical, Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
72.57	16.00	12.77	12.70	13.75	17.34

Source: ITU Global Cybersecurity Index v4, 2021

Montenegro



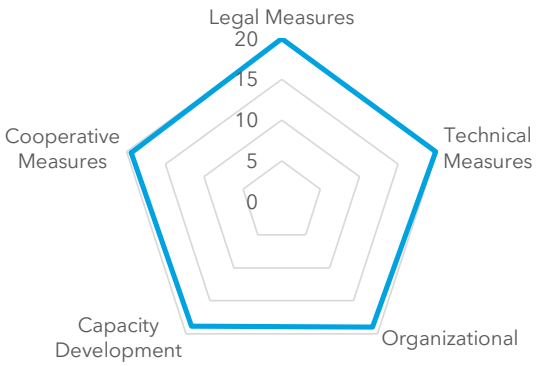
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
53.23	14.61	7.48	12.00	3.18	15.97

Source: ITU Global Cybersecurity Index v4, 2021

*Netherlands (Kingdom of the)***



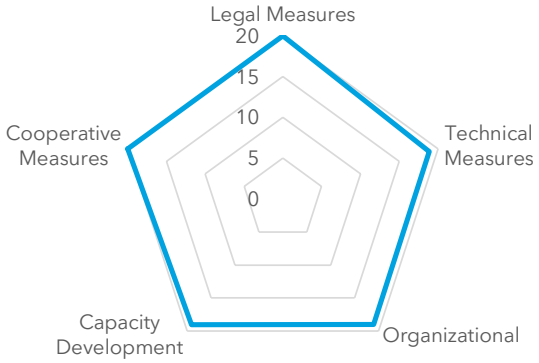
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.05	20.00	19.84	18.98	18.82	19.41

Source: ITU Global Cybersecurity Index v4, 2021

*Norway***



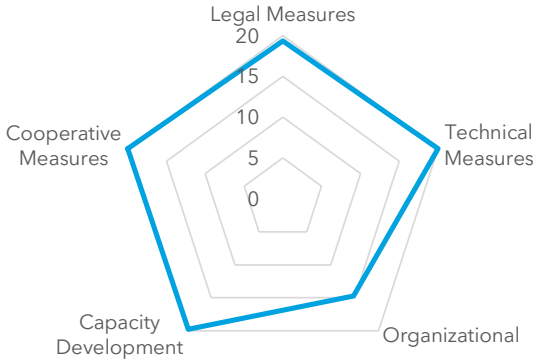
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures, Cooperative Measures
Area(s) of Potential Growth
Capacity Development, Technical, Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.89	20.00	18.86	18.98	19.04	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Poland (Republic of)



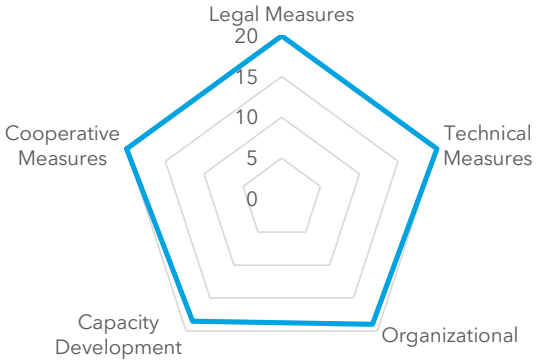
Development Level:
Developed Country

Area(s) of Relative Strength
Technical, Cooperative Legal, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
93.86	19.35	20.00	14.74	19.77	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Portugal



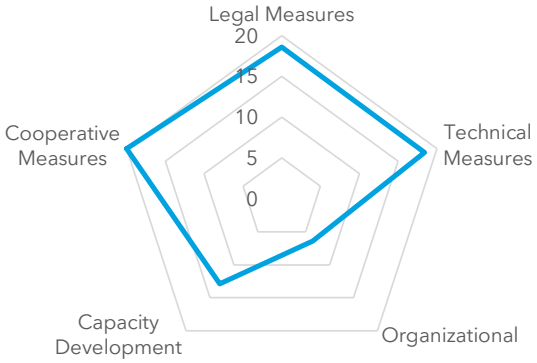
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.32	20.00	20.00	18.98	18.34	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Romania



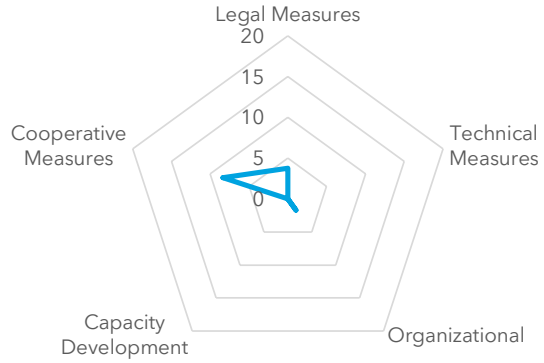
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
76.29	18.60	18.40	6.42	12.88	20.00

Source: ITU Global Cybersecurity Index v4, 2021

San Marino (Republic of)



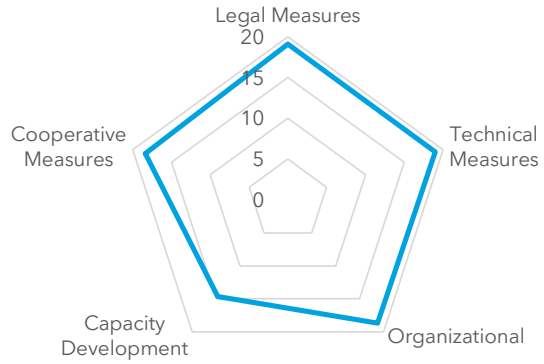
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Technical Measures, Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
13.83	3.77	0.00	1.69	0.00	8.37

Source: ITU Global Cybersecurity Index v4, 2021

Serbia (Republic of)



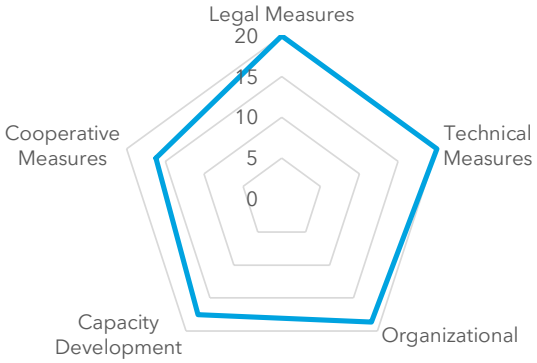
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Organizational, Cooperative Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
89.80	89.80	89.80	89.80	89.80	89.80

Source: ITU Global Cybersecurity Index v4, 2021

Slovak Republic



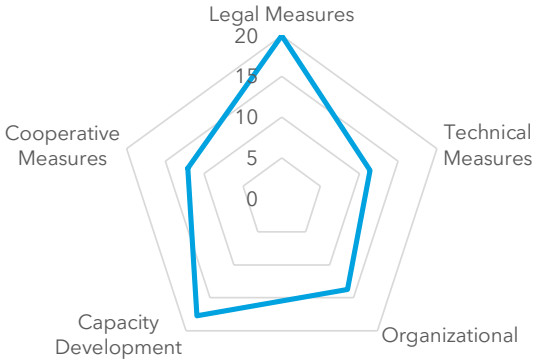
Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
92.36	92.36	92.36	92.36	92.36	92.36

Source: ITU Global Cybersecurity Index v4, 2021

Slovenia (Republic of)



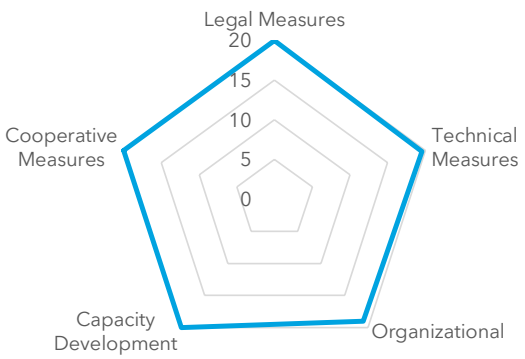
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
74.93	74.93	74.93	74.93	74.93	74.93

Source: ITU Global Cybersecurity Index v4, 2021

Spain



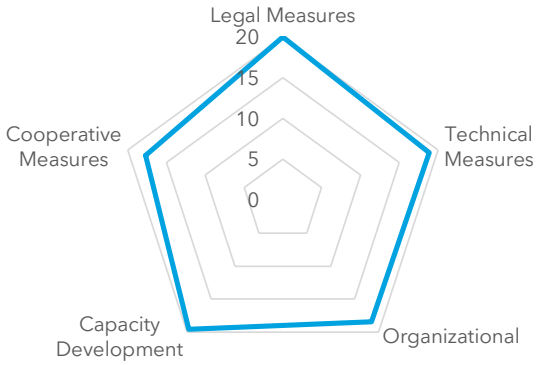
Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development, Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.52	20.00	19.54	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Sweden



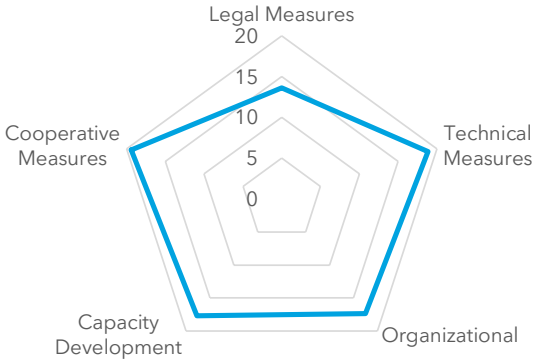
Development Level:
Developed Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.59	20.00	18.86	18.46	19.57	17.70

Source: ITU Global Cybersecurity Index v4, 2021

*Switzerland (Confederation of)***



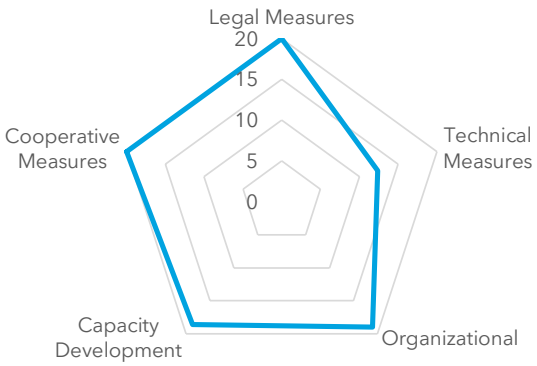
Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
Technical Measures, Cooperative Measures
Area(s) of Potential Growth
Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
86.97	13.62	18.85	17.40	17.69	19.41

Source: ITU Global Cybersecurity Index v4, 2021

North Macedonia (Republic of)



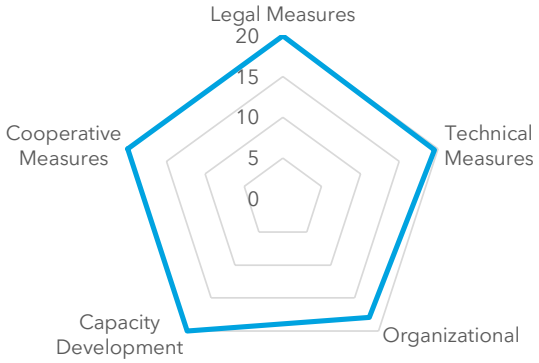
Development Level:
Developed Country, Landlocked

Area(s) of Relative Strength
Legal, Cooperative Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
89.92	20.00	12.37	18.98	18.57	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Turkey



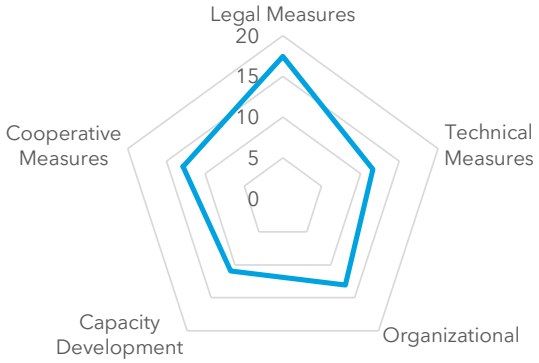
Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Technical Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.50	20.00	19.54	17.96	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Ukraine



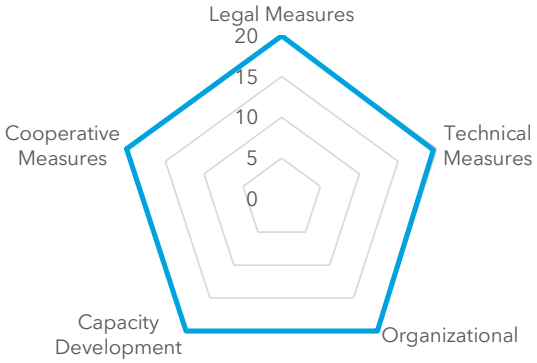
Development Level:
Developed Country

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Cooperative Measures	Capacity Development
65.93	17.46	11.60	13.06	10.94	12.87

Source: ITU Global Cybersecurity Index v4, 2021

United Kingdom of Great Britain and Northern Ireland



Development Level:
Developed Country

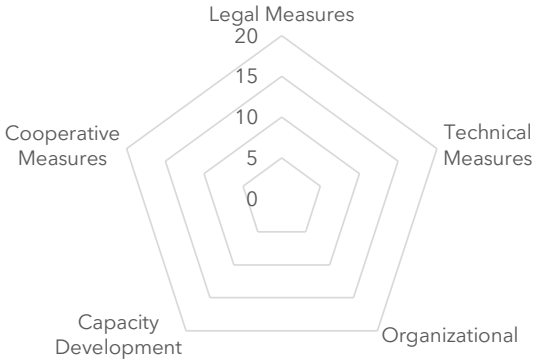
Area(s) of Relative Strength
Legal, Organizational, Cooperative, Capacity Development

Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Cooperative Measures	Capacity Development
99.54	20.00	19.54	20.00	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

*Vatican**



Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
N/A

Area(s) of Potential Growth
N/A

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Cooperative Measures	Capacity Development
0	0	0	0	0	0

Source: ITU Global Cybersecurity Index v4, 2021

** no response to the questionnaire/data collected by GCI Team

* no data

Glossary

Abbreviation	Definition
CERT	Computer Emergency Response Team, trademarked by Carnegie Mellon University
CI	Critical Infrastructure
CIRT*	Computer Incident Response Team, *see related terms CSIRTs, CERTs*
CSIRT	Computer Security Incident Response Team
DPP	Data and Privacy Protection
EU	European Union
GCI-1/2/3/4	The iteration of the Global Cybersecurity Index
GDPR	General Data Protection Regulation (EU)
ICT	Information and Communication Technology
ITU	International Telecommunication Union
LDC	Least Developed Countries
LLDCs	Landlocked Developed Countries
MLAT	Mutual Legal Assistance Treaty
MSMEs	Micro, small, and medium-sized enterprise
NCS	National Cybersecurity Strategy
NGO	Non-Government Organization
ODC	Other Developing Countries
OT	Operational Technology
PPP	Public Private Partnership
SIDS	Small Island Development States
SME	Small and medium-sized enterprises
UN	United Nations

Annex A: Methodology

A1. GCI scope and framework

The mandate for the Global Cybersecurity Index (GCI) derives from ITU Plenipotentiary Resolution 130 (Rev. Dubai, 2018) on strengthening the role of ITU in building confidence and security in the use of information and communication technologies (ICTs). Specifically, countries are invited "*to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors*". The goal of the GCI is to foster a global culture of cybersecurity and its integration at the core of ICTs.

Table A1: Global Cybersecurity Index participation and years of data collection

	GCI-1	GCI-2	GCI-3	GCI-4
Countries providing a focal point	105	136	155	169
Data collection years	2013-2014	2016	2017-2018	2020
Publishing year	2015	2017	2019	2021

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

GCI scope

The Global Cybersecurity Index (GCI) is a composite index of indicators, evolving for each iteration, that monitors the level of cybersecurity commitment in the five pillars of the Global Cybersecurity Agenda (GCA), its main objectives are to measure:

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

The goal of the GCI is to assist countries in identifying areas for improvement in the field of cybersecurity and encourage them to take action towards those areas. This would also be the opportunity to helping to raise the overall level of cybersecurity commitment worldwide, harmonizing practices and fostering a global culture of cybersecurity. The GCI aims to illustrate successful examples in cybersecurity that might serve as good practice and guidelines to countries with similar national environments.

A2. ITU cybersecurity cooperation framework

Cybersecurity is a multidisciplinary field, and its application involves all sectors, industries and stakeholders, both vertically and horizontally. In order to increase the development of national capabilities, efforts have to be made by political, economic and social forces. This can be done by law enforcement, justice departments, educational institutions, ministries, private sector operators, developers of technology, public private partnerships, and intra-state cooperation.

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

Table A2: GCI 2020 pillar descriptions

Legal measures	
	Measures based on the existence of legal frameworks dealing with cybersecurity and cybercrime.
	Legal measures (including legislation, regulation, and containment of spam legislation) authorize a state to set up basic response mechanisms through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. A legislative framework sets the minimum foundation of behaviour on which further cybersecurity capabilities can be built. Fundamentally, the objective is to have sufficient legislation in place in order to harmonize practices at the regional/ international level and simplify international combat against cybercrime.
Technical measures	
	Measures based on the existence of technical institutions and framework dealing with cybersecurity.
	Efficient ICT development and use can only prosper in an environment of trust and security. Countries therefore need to build and install accepted minimum-security criteria and accreditation schemes for software applications and systems. These efforts need to be complemented by the implementation of a national body dealing with cyber incidents, an authoritative government entity and a national framework to watch, warn, and respond to incidents.
Organizational measures	
	Measures based on the existence of coordination institutions, policies, and strategies for 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 their implementation. 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 an all-inclusive plan in implementation, delivery, and measurement. National agencies must be present to implement the strategy and evaluate the outcome. Without a national strategy, governance model, and supervisory body, efforts in different sectors become conflicted, preventing efforts to obtain an effective harmonization in cybersecurity development.
Capacity building measures	

Table A2: GCI 2020 pillar descriptions (continued)

	Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity building.
	Capacity building includes public awareness campaigns, framework 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 building is essential to raise awareness, knowledge and the know-how across sectors, for systematic and appropriate solutions, and to promote the development of qualified professionals.
Cooperative measures	
	Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.
	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.

A3. Key changes by pillar

Legal measures

Legal measures gauge legal interventions in cybersecurity and have been updated to better reflect cybersecurity-related national substantive law.

- Based on the BDT Management Consultation Group recommendations, procedural law is no longer measured in the Global Cybersecurity Index. Instead, more clarity is emphasized in several areas, including identity theft, online harassments, racism.
- The questions under the legal measures have been initially developed following the recommendations of conventions such as the Budapest Convention on Cybercrime. However, the answers now focus on highlighting the implemented national laws only, and no longer gather the ratifications of such conventions. Nevertheless, given the impact of international conventions and their role in creating binding commitments, international conventions like the Budapest Convention are now measured under international activities of cooperative measures.
- As people are increasingly online, a trustworthy cyberspace that also promotes diversity and inclusion requires examining issues such as privacy, as well as harassment, bullying, grooming, child pornography, and racism. This iteration of the Global Cybersecurity Index added questions on these issues.

Technical measures

The technical pillar has been restructured to better reflect how CIRTs operate, including:

- Computer Incident Response Team – Government and National CIRTs have been combined into a single indicator.

- CIRT certification is an important element in providing insights on the capacity to tackle cyber incident. To assess national CIRT[1] maturity levels, SIM3 certification scheme was added. The TF-CSIRT / Trusted Introducer uses SIM3 as basis for assessment and "Certified" members having the highest stage of maturity. Future iterations of the Global Cybersecurity Index will go deeper in exploring Security Maturity Models for CIRTs.

Organizational measures

- As cybersecurity is an ongoing process, countries are encouraged to regularly revisit and revise national cybersecurity strategies (at least every five years) to assess if the NCS is still relevant considering the changing risk environment, if it still reflects the national objectives and understand what adjustments are necessary. Based on this recommendation, countries which have not reaffirmed or updated their NCS in the past five years received partial points on indicators on NCS.
- Developing mechanisms to protect children online should be among the vital priorities of countries especially when the COVID-19 pandemic has forced children to study online. While the Internet brings significant benefits to children's education and growth, it also exposes them to online risks. Most countries have undertaken initiatives in support of child online protection through efforts such as creating websites and social media with dedicated educational materials, informational games and guides for children, parents, and educators. To distinguish between ad-hoc interventions and those structured within a larger, defined strategy, the latter received full marks, while countries with one-time or sporadic initiatives received partial marks.

Capacity development measures

This pillar has been stable with its indicators since the second iteration of the GCI. In this iteration, the scope expanded to include raising awareness on government support to small- and medium-sized enterprises (SMEs) as they play a significant role as actors in digital economy and supply chains, and this comes in a period of shift towards e-commerce and SMEs need support on cyber risk management.

Cooperation measures

This pillar reflects if agreements are signed or ratified regardless as to whether they are legally-binding. What agreements qualify under bilateral and multilateral agreements have been clarified. The Budapest Convention, which was previously counted under multilateral agreement, is now counted under international activity.

A4. Computational methodology

The questionnaire used for the GCI provides a value for the 20 indicators constructed through 82 questions. This achieves the required level of granularity and improves the accuracy and quality of the answers. The indicators can be found in the GCI questionnaire (Annex B).

The indicators used to calculate the GCI were selected based on:

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

[1] Also known as CSIRT/CERT, CIRTs are organizational entities assigned responsibility for coordinating and supporting the response to computer security events or incidents on a national level.

The GCI is based on a cybersecurity development map that a country might take into account when improving its cybersecurity commitment. The questionnaire was built upon five different pillars differentiated by five specific colours. In the charts of this report, the depth of the path indicates a higher development level of commitment.

This report provides the regional and world trends. To ensure accuracy, countries were required to support their answer through a feature of uploading supporting documents and URLs. A comment section was added to each pillar to allow countries provide good practices that tell the impact story of their cybersecurity evolution.

Countries were offered binary or trinary answers for the 82 questions of the 20 indictors of the 5 pillars, the comment section was used to details the stage of implementation in case an item was on a draft or under implementation phase.

Once the questionnaires had been returned, they went under two validations by two different validators, partial points were provided if the answer would refer to a draft or under implementation stage / or if it would not specifically answer all items of the question. This ternary assessment mode has avoided opinion-based evaluation and subjective bias through a table with specific items to be present for a positive and partial answer.

To this end, the fourth edition of the Global Cybersecurity Index questionnaire and any related documentation were submitted by the BDT Secretariat to the Study Group 2, question 3 rapporteur group meeting in October 2019, where the questionnaire was approved before the launch of the questionnaire. In March 2020 during the SG2 meeting, BDT updated Q3 with the status and consulted countries to appoint experts in the cybersecurity field to participate in the weightage distribution process.

Overall GCI process flow

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

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

Weightage

Unlike previous iterations, which have a scale of 0 to 1, this 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 are assigned a weight given the relative importance to the indicator group. Weightage can have a significant impact on final scores, and different techniques will produce different rankings.

The GCI took a participatory approach, using the budget allocation process (BAP). This considered that weights are, fundamentally, value judgements, and needed to take into account a wide variety of expert input.

Within the budget allocation approach, experts had a given "budget" which they could allocate within an indicator group, allocating a greater amount towards indicators that were assessed as more important. Experts were asked to contribute weightage recommendations for pillars in which they had expertise.

As all country responses underlying the data was reported survey data, verified by the ITU team, weighting did not account for the statistical quality of the data.

Weightage expert group involvement

In October 2020, ITU Member States and private sector membership were invited via circular letter to nominate experts to participate in this iteration of the Global Cybersecurity Index. Nominated experts were affiliated with academia, think tanks, ICT ministries, regulators, and standards organizations.

Experts that contributed to previous iterations of the Global Cybersecurity Index were also invited to contribute weightage recommendations.

A total of 84 experts participated, who were asked to provide weightage recommendations in pillars related to their areas of expertise.

Aggregation

Indicator groups were aggregated using weighted arithmetic averages. This meant that a country scoring poorly in one area could recoup some of their score by doing well elsewhere.

As noted in the OECD Handbook on Composite Indices, *"the marginal utility from an increase in low absolute score would be much higher than in a high absolute score under geometric aggregation. Consequently, a country would have a great incentive to address those sectors/activities/alternatives with low score if the aggregation were geometric rather than linear"* (33). However, for the purposes of clarity and comprehension, a linear approach was deemed more understandable and actionable.

Sensitivity analysis

Given the importance of weightage to final country scores, sensitivity analyses were conducted, which included:

- inclusion/exclusion of individual indicators;
- different weightage schemes (equal weighting, budget allocation method, extremes of expert recommendations);

- different aggregation systems (Weighted Averages, Additive).

Ranks

Countries have been ranked by their final score, using a "dense" ranking method. Equal scores result in the same rank. The next following country after two or more equally ranked countries receives the next ordinal number.

Annex B: Global Cybersecurity Index questionnaire (4th edition)

This questionnaire has been elaborated and reviewed by the ITU-D Rapporteur Study Group meeting for Question 3/2: Securing information and communication networks: Good practices for developing a culture of cybersecurity. The meeting was used as a channel to seek Members State approval to launch the 4th edition of the ITU Global Cybersecurity Index.

The questionnaire is composed of five sections, where questions in all sections expect yes/no responses are accompanied by tick-boxes. The questionnaire was designed to be completed online. Each respondent was provided (via an official e-mail from ITU) with a unique URL and login information to provide in responses. It also enables respondents to upload relevant documents (and URLs) for each question as supporting information. Information being provided by respondents to this questionnaire is not expected to be of a confidential nature.

Table B1: GCI Questionnaire: Legal measures

1. Cybercrime substantive law **EXP**: Substantive law refers to all categories of public and private law, including the law of contracts, real property, torts, wills, and criminal law that essentially creates, defines, and regulates rights.
1.1 Do you have substantive law on illegal online behaviour? ☐ *YES* ☐ *No* **Provide links/URL** **Provide document**
1.1.1 Do you have substantive laws on illegal access on devices, computer systems and data? **EXP**: Access - the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components, and functions (NICCS); **Computer system** or **system** - any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data (COE - Convention on Cybercrime); **Computer data** - any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (COE - Convention on Cybercrime); ☐ *YES* ☐ *No* **Provide links/URL** **Provide document**

Table B1: GCI Questionnaire: Legal measures (continued)

1.1.2 Do you have substantive law on illegal interferences (through data input, alteration, and suppression) on devices, data and computer system?

EXP: **Computer system interference** - both intentional and unauthorized serious hindering of the functioning of a computer system. It may include inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Data interference - either intentional and unauthorized damaging, deletion, deterioration, alteration, or suppression of computer data.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.1.3 Do you have substantive laws on illegal interception on devices, computer systems and data?

EXP: Illegal interception - both intentional and unauthorized, non-public transmission of computer data to, from or within a computer or another electronic system, made by technical means.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.1.4 Do you have substantive laws on online identity and data theft?

EXP: Online identity theft- stealing personal information such as names, addresses, date of birth, contact information or bank account. Can occur as a result of phishing, hacking online accounts, retrieving information from social media or illegal access to databases.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.2 Do you have dispositions on computer-related forgery (piracy / copyright infringements)?

EXP: Unauthorized input, alteration, or deletion of computer data resulting to inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, *to perpetuate* a fraudulent or dishonest design.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.3 Do you have substantive laws on online safety?

EXP: Online Safety - refers to maximizing Internet safety-related to various security risks on private and personal or property associated information, as well as enhancing users' self-protection from cybercrimes.

Table B1: GCI Questionnaire: Legal measures (continued)

1.3.1 Do you have dispositions/legal measures on offences related to racist and xenophobic online materials?

EXP: Measures to prevent different forms of online hate speech and other forms of intolerances because of race, colour, religion, descent or national or ethnic origin, sexual orientation or gender identity, disability, social status or other characteristics.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.3.2 Do you have dispositions/legal measures on online harassment and abuse against personal dignity/integrity?

EXP*: Cyber harassment or bullying - messages sent by email, direct messaging, or derogatory websites aimed to bully or otherwise harass an individual or a group of individuals via personalized attacks.*

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.3.3 Do you have dispositions/legal measures related to Child Online Protection?

EXP: Laws which makes it clear that any and every crime that can be committed against a child in the real world can also be committed on the Internet or any other electronic network. It is necessary to develop new laws or adopt existing ones to outlaw certain types of behaviour which can only take place on the Internet, for example the remote enticement of children to perform or watch sexual acts or grooming children to meet in the real world for a sexual purpose (ITU Guidelines for policy makes on Child Online Protection).

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2. Is there any cybersecurity regulation related to…

EXP: Regulation is rule based and meant to carry out a specific piece of legislation. Regulations are enforced usually by a regulatory agency formed or mandated to carry out the purpose or provisions of a legislation.

Cybersecurity regulation designates the principles, to be abided by various stakeholders, emanating from and being part of the implementation of laws dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection, digital signatures and e-transactions, and the liability of Internet service providers.

Table B1: GCI Questionnaire: Legal measures (continued)

2.1 Personal data/privacy protection?

EXP: Regulations about protection personal data from unauthorized access, alteration, destruction, or use. Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences; An example of such legislation may be in the Data Protection Act.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.2 Data breach/incident notification?

EXP: Breach notification laws or regulations are ones that require an entity that has been subject to a breach to notify the authorities, their customers and other parties about the breach, and take other steps to remediate injuries caused by the breach. These laws are enacted in response to an escalating number of breaches of consumer databases containing personally identifiable information;

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.3 Cybersecurity audit requirements?

EXP: A security audit means a systematic and periodic evaluation of the information system's security. Typical audit may include assessment of the security of the system's physical configuration and environment, software, information handling processes, and user practices.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B1: GCI Questionnaire: Legal measures (continued)

2.4 Implementation of standards?

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

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.7 Identifying and protecting the national critical information infrastructures?

EXP: Critical infrastructure constitutes basic systems crucial for safety, security, economic security, and public health of a nation. Those systems may include, but are not limited to defense systems, banking and finance, telecommunications, energy, and other. Attach any links or documents that define critical infrastructures or documents/news that confirms definitions of those.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Please provide some of the best practices/achievements/on-going developments that your country has/is been/being involved in pertaining to the legal areas as part of cybersecurity activities?

Use the comment box for a detailed practice/s and include links for proof

Or provide document/s including links for proof

Table B2: GCI Questionnaire: Technical measures

1. National/Government CIRT/CSIRT/CERT.

EXP: CIRT-CSIRT-CERT: computer incident response teams, staffed concrete organizational entities that are assigned the responsibility for coordinating and supporting the response to computer security events or incidents on national or government level.

NOTE: Sometimes distinctions are made between Government and National CIRTs as separate/different entities – Government CIRT serves Governmental constituents, and National CIRT serves the national constituents, including the private sector and citizens. Sometimes they referred to them as the same entity.

1.1 Is there a National/Government CIRT/CSIRT/CERT?

EXP: Supported by a government's decision or is part of governmental or national structures.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.2 Does your National or Government CIRT/CSIRT/CERT…

Table B2: GCI Questionnaire: Technical measures (continued)

1.2.1 Develop and execute cybersecurity awareness activities?

EXP: Efforts to promote widespread publicity campaigns to reach the nation about safe cyber-behaviour online.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.2.2 Conduct regular cyber security exercises such as CyberDrills?

EXP: A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to, or recovering from the disruption. Are the exercises organized periodically or repeatedly?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.2.3 Provide publicly available Advisories?

EXP: CIRT Advisories: the sharing of information with the general public on emerging cyber-threats and the recommended actions to take.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.2.4 Contribute to the issues of Child Online Protection?

EXP: The CIRT/CSIRT/CERT provides support such as awareness creation campaigns, reporting of incidents related to children, providing educational materials on Child Online Protection and others.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.3 Are the above mentioned CIRTs (CSIRT or CERT) affiliated with FIRST?

EXP: A Full Member or Liaison Member of the Forum of Incident Response and Security Teams. www.first.org

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B2: GCI Questionnaire: Technical measures (continued)

1.4 Are the above CIRT/s (CSIRT or CERT) affiliated with a regional CERT?

EXP: A formal or informal relation with any other CERT within, or outside the country, as a part of any regional CERT group. Examples of regional CERTS include APCERT, AFRICACERT, EGC, OIC, and OAS.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.5 Was the maturity level of above CIRT, CSIRT or CERT services certified by the TI certification scheme under TF-CSIRT –SIM3?

Exp: SIM3 is a basis for CIRT certification.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2. Sectoral CIRT/CSIRT/CERT

EXP: A sectoral CIRT/CSIRT/CERT is an entity that responds to computer security or cybersecurity incidents which affect a specific sector. Sectoral CERTs are usually established for critical sectors such as healthcare, public utilities, academia, emergency services and the financial sector. The sectoral CERT provides its services to constituents from a single sector only.

2.1 Are there sectoral CIRTs/CSIRTs/CERTs in your country?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.2. Does your sectoral CIRT/s, CSIRT/s, CERT/s:

2.2.1 Develop and execute cybersecurity awareness activities for a sector?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.2.2 Actively participate in national CyberDrills?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B2: GCI Questionnaire: Technical measures (continued)

2.2.3 Share sectoral related incidents within its constituency?

EXP: sharing of information on emerging cyberthreats and the recommended actions to take.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3. National framework for implementation of cybersecurity standards

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

3.1 Is there a framework for implementation/adoption of cybersecurity standards?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3.2 Does the framework include international or other related standards?

EXP: ITU-T, ISO/IEC, NIST, ANSI/ISA and others.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

4. Child Online Protection

EXP: This indicator measures the existence of a national agency dedicated to Child Online Protection, the availability of a national telephone number to report issues associated with children online, any technical mechanisms and capabilities deployed to help protect children online, and any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online telephone number, email address, web forms and other, where the interested parties can report incidents or concerns related to Child Online Protection (COP).

4.1 Are there any reporting mechanisms and capabilities deployed to help protect children online?

EXP: Such as hotlines, helplines etc.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Please provide some of the best practices/ achievements/on-going development your country has been/is being involved in pertaining to the technical areas as part of cybersecurity activities.

Use the comment box for a detailed practice/s and include links for proof

Or provide document/s including links for proof

Table B3: GCI Questionnaire: Organizational measures

1. National Cybersecurity Strategy

EXP: The development of policy to promote cybersecurity as one of national top priorities. A national cybersecurity strategy should define the maintaining of resilient and reliable national critical information infrastructures including the security and the safety of citizens; protect the material and intellectual assets of citizens, organizations and the nation; respond, prevent cyber-attacks against critical infrastructures; and minimize damage and recovery time from cyber-attacks.

1.1 Does your country have a national cybersecurity strategy/policy?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Does it address the protection of national critical information infrastructures, including in the telecommunication sector?

EXP: Any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any from including data, voice, or video that is vital to the functioning of a critical infrastructure; so vital that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety.

☐ *YES*

☐ *No*

Provide links/U*RL*

Provide document

Does it include reference to the national cybersecurity resilience?

EXP: A national cybersecurity resiliency plan ensures that the country has the ability to resist, absorb, accommodate to and recover from the effects of any hazard (including natural or human-made) in a timely and efficient manner, including through the preservation and restoration of its essential services and functions with reliance on external service.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Is the national cybersecurity strategy revised and updated on a continuous basis?

EXP: The life cycle management of the strategy is defined, the strategy is updated according to national, technological, social, economic and political developments that may affect national cybersecurity situation.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B3: GCI Questionnaire: Organizational measures (continued)

Is the cybersecurity strategy open to any form of consultation with national experts in cybersecurity?

EXP: The strategy is open for consultation by all relevant stakeholders, including operators of critical infrastructures, ISPs, academia and others.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.2 Is there a defined action plan/roadmap for the implementation of cybersecurity governance?

EXP: A strategic plan that defines the national cybersecurity outcomes including steps and milestones needed to implement it.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.3 Is there a national strategy for Child Online Protection?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2. Responsible Agency

EXP: A responsible agency for implementing the national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils, or cross-disciplinary centres. Such a body may also be directly responsible for the national CIRT. The responsible agency may exist within the government and may have the authority to compel other agencies and national bodies to implement policies and adopt standards.

2.1 Is there an agency responsible for cybersecurity coordination at a national level?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.1.1 Does this agency oversee National Critical Information Infrastructure Protection?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.2 Is there a national agency overseeing national cybersecurity capacity development?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B3: GCI Questionnaire: Organizational measures (continued)

2.3 Is there any agency overseeing the child online protection initiatives at the national level?
EXP: Existence of a national agency dedicated to oversee and promote Child Online Protection.

☐ *YES*

☐ *No*

Provide links/URL

Provide do*cument*

3. Cybersecurity metrics

EXP: Existence of any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development, risk-assessment strategies, cybersecurity audits, and other tools and activities for a rating or evaluating resulting performance for future improvements. For example, based on ISO/IEC 27004, which is concerned with measurements relating to information security management.

3.1 Are there any cybersecurity audits performed at a national level?

EXP: A security audit is a systematic evaluation of the security of an information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. Privately managed critical infrastructures may be requested by the regulatory bodies to perform security posture assessments periodically and report on findings.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3.2 Are there metrics for assessing cyberspace associated risks at a national level?

EXP: *It is a* process comprising risk identification, risk analysis and risk evaluation.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3.3 Are there measures for assessing the level of cybersecurity development at a national level?

EXP: It is an approach to measure the development level of cybersecurity in a nation state.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Please provide some of the best practices/achievements/on-going development your country has been/is being involved in pertaining to the organizational measures as part of cybersecurity activities.

Use the comment box for a detailed practice/s and include links for proof

Or provide documents including links for proof

Table B4: GCI Questionnaire: Capacity development measures

1. Public cybersecurity awareness campaigns

EXP: Public awareness includes efforts to promote campaigns to reach as many citizens as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centres, community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behaviour online. This includes actions such as setting up portals and websites to promote awareness, disseminating support materials and other relevant activities.

1.1 Are there public awareness campaigns targeting specific sector such as SMEs, private sector companies, and government agencies?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.2 Are there public awareness campaigns targeting civil society?

EXP: NGOs, community-based organisations.

☐ *YES*

☐ *No*

Provide links/UR*L*

Provide document

1.3 Are there public awareness campaigns targeting citizens?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.4 Are there public awareness campaigns targeting the elderly?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.5 Are there public awareness campaigns targeting persons with special needs?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

1.6 Are there public awareness campaigns involving parents, educators and children (COP related)?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B4: GCI Questionnaire: Capacity development measures (continued)

2. Training for Cybersecurity professionals

EXP: The existence of sector-specific professional training programs for raising awareness for the general public (i.e., national cybersecurity awareness day, week, or month), promoting cybersecurity education for the workforce of different profiles (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector.

It also includes cybersecurity training for law enforcement officers, judicial and other legal actors designate professional and technical training that can be recurring for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession. This indicator also includes the existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of professionals by internationally recognized cybersecurity standards. These certifications, accreditations, and standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC^2), and other.

2.1 Does your government develop/support professional training courses in cybersecurity?

EXP: Promoting cybersecurity courses in the workforce (technical, social sciences, etc. and promoting certifications for professionals in either the public or the private sector.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.2 Is there an accreditation program for cybersecurity professionals in your country?

EXP: Institutes accrediting cybersecurity professionals, or any other related mechanisms.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.3 Are there a national sector-specific educational programmes/trainings/courses for professionals in cybersecurity?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.3.1 Are there a national sector-specific educational programmes/trainings/courses for law enforcement?

EXP: Cybersecurity formal process for educating legal actors (police officers and enforcement agents) about computer security

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B4: GCI Questionnaire: Capacity development measures (continued)

2.3.2 Are there a national sector-specific educational programmes /trainings/courses for judicial and other legal actors?

EXP: Cybersecurity training or technical training that can be recurring for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.3.3 Are there a national sector-specific educational programmes/trainings/courses for SMEs/ private companies?

EXP: Good practices trainings / capacity development on cybersecurity to guard their businesses, etc. by proper use of online services.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2.3.4 Are there a national sector-specific educational programmes/trainings/courses for other public sector/government officials?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3. Does your government/organization develop or support any educational programmes or academic curricula in cybersecurity…

EXP: Existence and the promotion of national education courses and programmes to train the younger generation in cybersecurity-related skills and professions in schools, colleges, universities and other learning institutes. Cybersecurity-related professions include, but are not limited to, cryptanalysts, digital forensics experts, incident responders, security architects and penetration testers.

3.1 In primary education?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3.2 In secondary education?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B4: GCI Questionnaire: Capacity development measures (continued)

3.3 In higher education?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

4. Cybersecurity research and development programmes

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

4.1 Are there cybersecurity R&D activities at the national level?

☐ *YES*

☐ *No*

Provide links/URL

Provide docume*nt*

4.1.1 Are there private sector cybersecurity R&D programmes?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

4.1.2 Are there public sector cybersecurity R&D programmes?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

4.1.3 Are higher education institutions such as academia and universities engaged in R&D activities?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

5. National cybersecurity industry

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

Table B4: GCI Questionnaire: Capacity development measures (continued)

5.1 Is there a national cybersecurity industry?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

6. Are there any government incentive mechanisms in place...

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

6.1 To encourage capacity development in the field of cybersecurity?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

6.2 For the development of a cybersecurity industry?

EXP: support to start-ups cybersecurity services in academia and other

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Please provide some of the best practices/achievements/on-going development your country has been/is being involved in pertaining to the capacity building measures as part of cybersecurity activities.

Use the comment box for a detailed practice/s and include links for proof

Or provide document/s including links for proof

Table B5: GCI Questionnaire: Cooperative measures

1. Bilateral agreements on cybersecurity cooperation with other countries

EXP: Bilateral agreements (one-to-one agreements) refer to any officially recognized national or sector-specific partnerships for sharing cybersecurity information or assets across borders by the government with one other foreign government and regional entity (i.e., the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether information sharing of threat intelligence. Capacity building refers to the sharing of professional tools, advanced envelopment of experts, and others.

1.1 Do you have bilateral agreements on cybersecurity cooperation with other countries?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Is information sharing part of the agreement(s)?

EXP: Information-sharing refers to the practices around sharing on non-sensitive information.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Is capacity building part of the agreement(s)?

EXP: The ability to encourage trainings to strengthen the skills, competencies and abilities of National cybersecurity professionals through cooperation to ensure collective efforts against cyber threats.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Is mutual legal assistance part of the agreement(s)?

EXP: Mutual assistance between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

2. Government participation in international mechanisms related to cybersecurity activities

EXP: It may also 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.

2.1 Does your government/organization participate in international mechanisms related to cybersecurity activities?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B5: GCI Questionnaire: Cooperative measures (continued)

3. Cybersecurity multilateral agreements

EXP: Multilateral agreements (one to multiparty agreements) refers to any officially recognized national or sector-specific programmes for sharing cybersecurity information or assets across borders by the government with multiple foreign governments or international organizations (i.e. the cooperation or exchange of information, expertise, technology and other resources).

3.1 Does your government have multilateral agreements on cybersecurity cooperation?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3.1.1 Is information sharing part of the agreement(s)?

EXP: Information-sharing refers to the practices around sharing on non-sensitive information.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

3.1.2 Is capacity building part of the agreement(s)?

EXP: The ability to encourage trainings to strengthen the skills, competencies and abilities of National cybersecurity professionals through cooperation to ensure collective efforts against cyber threats.

☐ *YES*

☐ *No*

Provide links/URL

Provide document

4. Partnerships with the private sector (PPPs)

EXP: Public-private partnerships (PPP) refer to ventures between the public and private sector. This performance indicator measures the number of officially recognized national or sector-specific PPPs for sharing cybersecurity information and assets (people, processes, tools) between the public and private sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources), whether nationally or internationally.

4.1 Does your government engage in PPPs with locally established companies?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

4.2 Does your government engage in PPPs with foreign owned companies in your country?

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Table B5: GCI Questionnaire: Cooperative measures (continued)

5. Inter-agency partnerships

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

5.1 Are there inter-agency partnerships/agreements among different governmental bodies in relation to cybersecurity?

EXP: Cooperation between ministries or specialized agencies

☐ *YES*

☐ *No*

Provide links/URL

Provide document

Please provide some of the best practices/ achievements/on-going developments that your country has been/is being involved in pertaining to the cooperation measures as part of cybersecurity activities.

Use the comment box for a detailed practice/s and include links for proof

Or provide document/s including links for proof

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
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
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)

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

Digital Knowledge Hub Department (DKH)

Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)

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

Africa

Ethiopia

International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

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

Cameroon

Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

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

Senegal

Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

International Telecommunication Union (ITU) Area Office
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

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

Barbados

International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

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

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

Asia-Pacific

Thailand

International Telecommunication Union (ITU) Regional Office
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication Union (ITU) Area Office
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

CIS

Russian Federation

International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International
Telecommunication
Union
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-33921-0

Published in Switzerland
Geneva, 2021
Photo credits: Shutterstock