GCI scope and framework

Background

The Global Cybersecurity Index (GCI) is included under 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. Specifically, Member States are invited "*to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors*". The ultimate goal is to foster a global culture of cybersecurity and its integration at the core of information and communication technologies.

The first GCI survey was conducted in 2013/2014 in partnership with ABI Research. A total of 105 countries responded out of 193 ITU Member States and the final results were published in 2015: See www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

A second iteration which saw a response of 136 Member States was prepared in 2016 and published in 2017: See www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

The ITU prepared a third iteration (GCIv3) that unveiled the great interest of Member States for the GCI. This version saw a response of 155 countries and the draft version of the report was published in March 2019 upon request of Member States: See www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

The GCI has become a tool in which many Member States are showing interest. They expressed their wish for the launch of a new iteration as the GCI is being used as a benchmark by many to improve their cybersecurity situation. This is reflected in the achievements sent by the Member States to the ITU in order to improve their score and ranking.

As a result, the ITU is compiling a fourth iteration (GCIv4) that will be launched following the timeframe of the study group. The process of the GCI is submitted to the study group to allow active participation and transparency in the decision making of each step taken to arrive to the final report of the GCI.

The GCI is formulated around the data provided by the ITU membership, including interested individuals, experts and industry stakeholders as contributing partners with Grenoble university (France) as new partner joining the Australia Strategic Policy Institute, FIRST (Forum for Incident Response and Security Team), 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 combining evolving number of indicators per each iteration into one benchmark to monitor and compare the level of the cybersecurity commitment of countries with regard to the five pillars of the Global

Cybersecurity Agenda (GCA). These pillars form the five sub-indices of GCI. The main objectives of GCI are to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- progress in cybersecurity commitment of all countries from a global perspective;
- 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 help countries identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide. Through the collected information, GCI aims to illustrate the practices of others so that countries can implement selected aspects suitable to their national environment, with the added benefit of helping to harmonize practices, and foster a global culture of cybersecurity.

Framework

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:

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

These five designated areas form the basis of the indicators for GCI because they shape the inherent building blocks of a national cybersecurity culture.

Cybersecurity has a field of application that cuts across all industries, all sectors, 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 considering the long-term aim to increase efforts in the adoption and integration of cybersecurity on a global scale.

Figure 1: GCI 2019 indicators per pillar

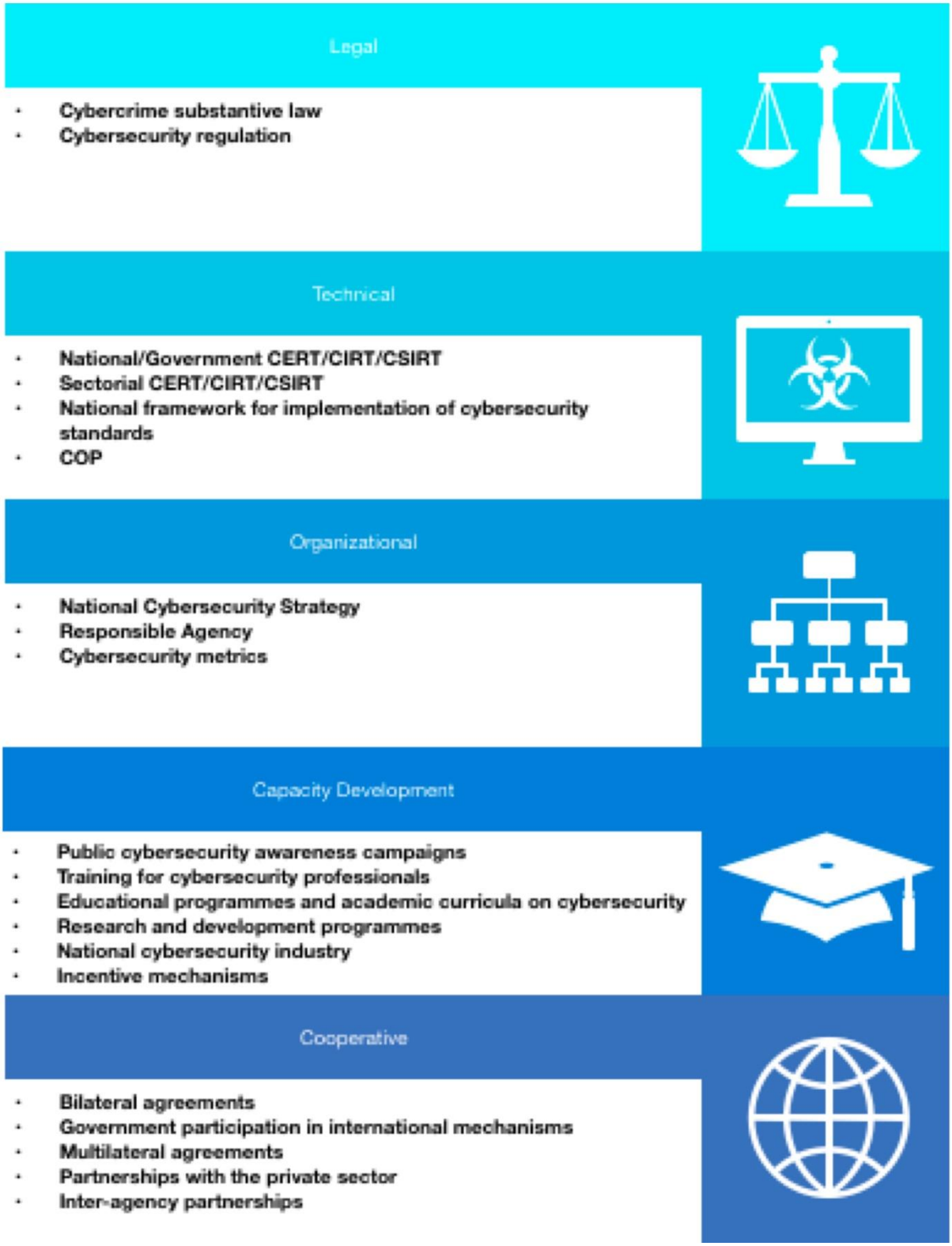

Figure 1: GCI 2019 indicators per pillar sets out the measures for each GCI pillar and its 20 indicators used to measure ITU Member State commitment to cybersecurity.

GCI 2019 indicators per pillar given in Figure 1 sets out the measures for each GCI pillar and its 20 indicators used to measure ITU Member State commitment to cybersecurity as referred to in the text below.

***Legal*:** Legal measures (including legislation, regulation and containment of spam legislation) authorize a nation 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. The legal context is evaluated based on the number of legal institutions and frameworks dealing with cybersecurity and cybercrime.

***Technical*:** Technology is the primary frontier of defence against cyber threats (including the use of computer emergency or incident response teams, standards implementation framework, technical mechanisms and capabilities deployed to address spam, child online protection, etc.). Without suitable technical skills to detect and respond to cyber-attacks, countries remain vulnerable. Efficient ICT development and use can only truly 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 creation of a national body with the aim of dealing with cyber incidents, an authoritative government entity and a national framework to watch, warn, and respond to incidents. Technical elements are evaluated based on the number of practical mechanisms to deal with cybersecurity.

Organizational: Organizational measures (including national strategies, responsible agencies, and cybersecurity metrics) are indispensable for the proper implementation of any national initiative. Broad strategic targets and goals need to be set by the nation 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. The organizational structures are evaluated based on the presence of institutions and strategies involving cybersecurity development at the national level.

Capacity building: Capacity building (including public awareness campaigns, framework for certification and accreditation of cybersecurity professionals, professional training courses in cybersecurity, educational programmes or academic curricula, etc.) 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. Capacity building is evaluated based on the number of research and development, education and training programmes, and certified professionals and public sector agencies.

Cooperation: Cybercrime is a global problem and is unrestricted to national borders or sectoral distinctions. As such, tackling cybercrime requires a multi-stakeholder approach with inputs from all sectors and disciplines (including bilateral and multilateral agreements, participation of international fora/associations, public-private partnerships, inter-agency

partnerships, best practice, etc.). Greater cooperation can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats and enable better investigation, apprehension and prosecution of malicious agents. National and international cooperation is evaluated based on the number of partnerships, cooperative frameworks and information sharing networks.

Methodology

The questionnaire used for the 2019 GCI provides a value for the 20 indicators constructed through 82 binary, pre-coded, and open-ended questions. This achieves the required level of granularity and improves the accuracy and quality of the answers.

The indicators used to calculate the GCI were selected on the basis of the following criteria:

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

The concept of the GCI is based on a cybersecurity development map with pre-coded and binary answers that define possible paths, and which a country might take into account in order to enhance their cybersecurity commitment. Each of the five pillars have a specific colour. The depth of the path indicates a higher development level of commitment.

Figure 2: GCI/GCA mapping of the organizational pillar

Figure 2: The GCI/GCA mapping of the organizational pillar is a graphical representation, in layers, of national action, cybersecurity strategy, action plans, relevant government implementing bodies, and metrics used to measure the GCA impact.

Figure 2 illustrates the relationship between the GCA, the pillars, indicators, and questions (expanded only for the organizational pillar illustrating the need for policy coordination institutions and strategies for cybersecurity development at the national level).

The various levels of cybersecurity development among countries, as well as different cybersecurity needs reflected by national ICT development status, were taken into consideration. The concept is based on an assumption that the more developed cybersecurity is, the more complex the solutions will be. Therefore, the further a country goes along the path for each pillar by confirming the presence of pre-identified cyber solutions, the more comprehensive and sophisticated the cybersecurity development will be within that country, allowing it to get a higher GCI score.

Using binary answers eliminates opinion-based evaluation and any possible bias towards certain types of answers. Moreover, a simple binary concept allows quicker and more complex evaluation as it does not require lengthy answers, which accelerates and streamlines the process of providing answers and further evaluation. The respondent should only confirm presence of, or lack of, certain pre-identified cybersecurity solutions. An online survey mechanism, which is used for gathering answers and uploading relevant material, enables the extraction of good practice, and a set of thematic qualitative evaluations by a panel of experts.

The key difference in methodology from the previous GCI surveys is that the structure has been modified back to the use of a binary system and a three-level system with closed-ended questions. The binary system evaluates the existence or absence of a specific measure, activity

or department. Unlike GCI version three, it does not take into consideration partial and pre-coded answers.

The pre-coded questions require a box with a "YES or NO" to be ticked, saving the respondent time when writing the answers. The option to add further details in the comment box has also been removed in order for countries to give specific relevant information.

Furthermore, partial answers have been excluded to ensure that countries are properly ranked. A feature of uploading supporting documents and URLs has also been added as a way to provide proof, accuracy, and more information to substantiate the pre-coded response. A number of questions have been removed or re-defined and new questions have been added in each of the five pillars to refine precision and increase the depth of research.

A comment section has been added to each pillar to allow Member States provide best practices that accurately tell the impact story of their cybersecurity evolution. Member States are urged to document in achievements, drafts documents/implementation progress as they have the best knowledge of what is taking place on ground. This section has to be accompanied by links and documents.

To this end, the questionnaire and any relevant GCI related documentation will be submitted by the BDT Secretariat to the Q3 rapporteur group meeting in October 2019, to be revised and agreed by the meeting before the starting launch of the survey. In March 2020 during the SG2 meeting, BDT will update Q3 with the status and will initiate the analysis of the data, engaging a group of experts formed through an open consultation process with Member States, Sector Members and BDT partners. The approach for the establishment of such expert group will be presented and discussed during the Q3 meeting in October 2019.

The overall GCI process is as follows:

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.[1]

[1] https://www.itu.int/online/mm/scripts/gensel8