ITU/BDT Cyber Security Programme
Global Cybersecurity Index (GCI)

Reference Model

Version 1.0

28 February 2018

TABLE OF CONTENTS

1 BACKGROUND

The Global Cybersecurity Index (GCI) is included under ITU Plenipotentiary Resolution 130 (Rev. Busan, 2014) 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.

A first iteration of the GCI was conducted in 2013/2014 in partnership with ABI Research where a total of 105 countries responded out of 193 ITU Member States and the final results was published in 2015

(see http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx).

Following feedback received from various communities and Member States, a second iteration was prepared in 2016 and the final results published in 2017

(see http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx).

This version was formulated around an extended participation from Member States, interested individuals, experts and industry stakeholders as contributing partners (namely World Bank and Red Team Cyber as new GCI partners joining the Australia Strategic Policy Institute, FIRST, Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet and Security Agency, NTRA Egypt, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica and UNODC). A total of 134 countries responded to the online survey that was administered to the 193 ITU Member States in 2016 compared to the 105 who responded in 2014

As a result of high attention received from Member States, media and interested bodies who believes in the vision of GCI, ITU is therefore compiling a third iteration still based on multi stakeholder participation.

2 REFERENCE MODEL

The Global Cybersecurity Index (GCI) is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of the cybersecurity commitment of Member States with regards to the five pillars of the Global Cybersecurity Agenda (GCA). These pillars form the 5 sub-indices of GCI. GCI is continuously being enhanced in response to ITU Member States request to develop a cybersecurity index that can be published on a regular basis.

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 objective 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 Member States can implement selected aspects suitable to their national environment, with the added benefit of helping harmonise practices and foster a global culture of cybersecurity.

3 CONCEPTUAL FRAMEWORK

GCI is rooted in the GCA, the ITU framework for international multi-stakeholder cooperation in cybersecurity that aims at building synergies with current and future initiatives. It 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 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 programs; 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 the national capabilities, efforts by political, economic and social forces has to be made. This can be done by law enforcement, Justice department, educational institutions and ministries, private sector operators and developers of technology, public private partnerships and intra-state cooperation considering the long term aim to drive further efforts in the adoption and integration of cybersecurity on a global scale.

The figure below is an illustration of the GCI pillars and sub-pillars


LEGAL
Cybercriminal Legislation, Substantive law,
Procedural cybercriminal law,
Cybersecurity Regulation.
TECHNICAL
National CIRT, Government CIRT, Sectoral CIRT,
Standards for organisations,
Standardisation body.
ORGANIZATIONAL
Strategy,
Responsible agency,
Cybersecurity metrics.
CAPACITY BUILDING
Public awareness, Professional training,
National education programmes, R&D programmes,
Incentive mechanisms, Home-grown industry.
COOPERATION
Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.

- ***Legal sub-pillar*:** Legal measures empower a nation state to establish 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 standards of behavior across the board on which further cybersecurity capabilities can be built. Ultimately, the goal is to enable all nation states to have adequate legislation in place in order to harmonize practices at the regional/international level, and facilitate international combat against cybercrime. ***The legal environment is evaluated based on the number of legal institutions and frameworks dealing with cybersecurity and cybercrime.***
- ***Technical sub-pillar*:** Technology is the first line of defense against cyber threats. Without adequate technical capabilities to detect and respond to cyberattacks, nation states remain vulnerable. Effective ICT development and use can only truly prosper in a climate of trust and security. Nation states therefore need to establish accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be accompanied by the creation of a national entity focused on dealing with cyber incidents, a responsible government agency and a national framework for watch, warning and incident response. The ***Technical component is evaluated based on the number of frameworks dealing with cybersecurity by the nation state.***
- ***Organizational sub-pillar:*** Organizational measures are necessary for the proper implementation of any national initiative. A broad strategic objective needs to be set by the nation state, along with a comprehensive plan in implementation, delivery and measurement. National agencies need to be present to implement the strategy and evaluate the results. Without a national strategy, governance model and supervisory body, efforts in different sectors become disparate, thwarting efforts to attain national harmonization in cybersecurity capability development. ***The organizational structures are evaluated based on the existence of institutions and strategies concerning cybersecurity development at the national level.***
- ***Capacity building sub-pillar:*** Capacity building is intrinsic to the first three measures (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 necessary to enhance knowledge and know-how across sectors, to formulate appropriate solutions, and promote the development of competent professionals. ***Capacity building is evaluated based on the number of research and development, education and training programs, and certified professionals and public sector agencies.***
- ***Cooperation sub-pillar:*** Cybercrime is a global problem and is blind to national borders or sectoral distinctions. As such, tackling cybercrime requires a multi-stakeholder approach with inputs from all sectors and disciplines. 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.***

4 METHODOLOGY

The questionnaire was elaborated on the basis of these sub-pillars. The value for the 25 indicators were therefore constructed through 50 binary, pre-coded and open ended questions. This was done in order to achieve the required level of granularity and ensure accuracy and quality on the answers.

The GCI includes 25 indicators (50 questions) with sub-questions more defined in a pre-coded answers and accurate. A detailed definition of each indicator is provided in Annex A.

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

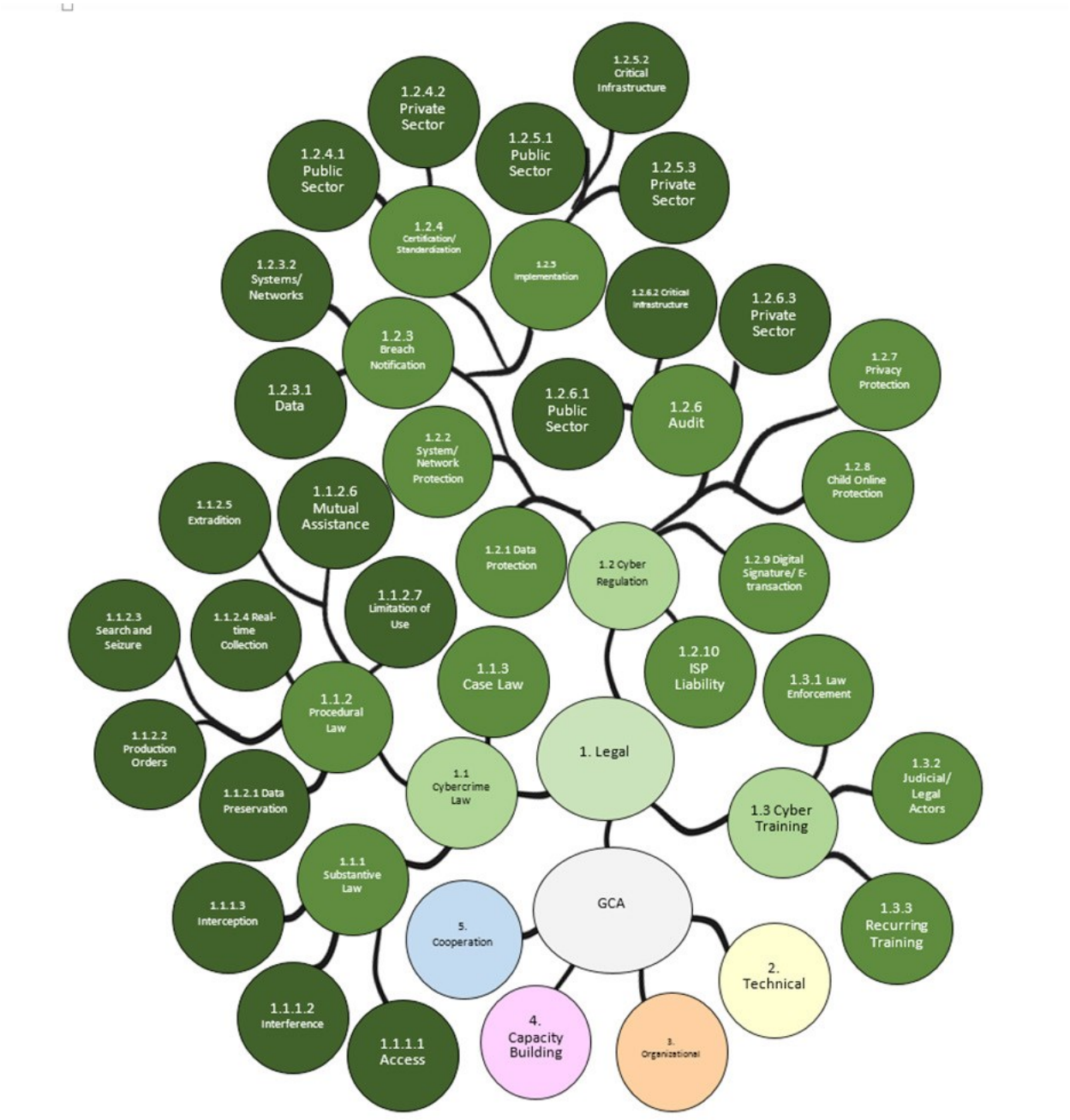
- relevance to the five GCA pillars and for contributing towards the main GCI objectives and conceptual framework

- data availability and quality
- possibility of cross verification through secondary data

The concept of the GCI is based on a cybersecurity development tree map with pre-coded and binary answers possibility. The tree map concept, which is illustrated below, is to provide an answer that define possible paths which countries might be take into account order to enhance their cybersecurity commitment. Each of the five pillars have a specific color.

The depth of the path indicates a higher development level of commitment.

Below is an example of the Legal pillar only for the sake of clarity and given the space constraint in having the complete picture.



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

The rationale behind using binary answer possibilities is an elimination of opinion based evaluation and any possible bias towards certain types of answers. The pre-coded answers would save time and would allow a more accurate data analysis.

Moreover, that simple binary concept will allow quicker and more complex evaluation as it will not require lengthy answers from countries which is assumed to accelerate and streamline the process of providing answers and further evaluation. The idea is that the respondent will only confirm presence or lack of certain pre-identified cybersecurity solutions. An online survey mechanism, which is used for gathering answers and uploading of all relevant materials, will enable the extraction of good practices, and a set of thematic qualitative evaluations by a panel of experts.

The key difference in methodology from the previous versions is that the structure has been modified to questions with pre-defined answers including free text and open-ended questions in every section of the questionnaires. A multiple choice (Multiple answers) has been included to allow Member States to simply tick the boxes that apply to them.

The pre-coded answer simply require a box to be ticked, pre-coded questions are suited to save the respondent time writing in the answers. The option to add further details on the specific subject has been also provided in order for Member States to complement specific information that might have not been captured in the pre-defined answers.

Furthermore, partial answers have been included, to capture "work in progress" material (such as approved drafts of documents, or advanced stage of development of capabilities), in order to ensure that countries are properly positioned in their accurate ranks.

A feature of uploading supporting documents and URLs has also been added as a way to provide more information and prove accuracy 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 improve precision and refine the depth of research.

The detailed computation of the sub-indices and for the main index will be elaborated with the support of a panel of experts that will define weights for each question, to be then aggregated and used to calculate the ranking (See structure in Annex B. to be filled with the weights).

Apart from building the index, open ended questions have been included in the questionnaire to cater for additional requirements from ITU-D Study 2 Question 3 which do not fit within GCI computation.

The questionnaire, is made available through an on line survey for a specific period of time to allow member State to reply and provide their answers.

The overall GCI process is implemented as follow:

1. A **Letter of Invitation** is sent by the ITU Secretariat to all Member States, informing them on the initiative and requesting the identification of a country level GCI focal point with whom ITU liaises and who is responsible for collecting all relevant data for completing the online GCI questionnaire.

   During the online survey, the approved focal points chosen by each Member States is officially invited by ITU to answer questionnaire presented to them.

2. **Primary data collection** (for countries who will not respond to the questionnaire):

- ITU Secretariat elaborates an initial draft of the response to the questionnaire using publicly available data and on-line search
- Draft is sent to the concerned Member State for review.
- The focal point identified by the Member State is contacted and provided with indications on how to improve the accuracy of the reviewed responses, and where necessary providing the completed questionnaire with comments.
- After the necessary rounds of iterations and amendments, a pre-final questionnaire is sent to the concerned Member State for final approval.
- Once formal approval is received, the questionnaire is considered validated and used for the analysis, scoring and ranking.
- (NOTE) – Should the Member State not provide a focal point for the GCI, ITU Secretariat will establish contact with the institutional Focal Point as per the ITU Global Directory.[1]

3. **Secondary data collection** (for countries that responds to the questionnaire):
   - ITU carries out verification of the responses provided by the specific Member State to identify possible missing elements (no or missing responses, no or missing supporting documents, no or missing links, etc.).
   - The focal point identified by the concerned Member State is contacted and provided with indications on how to improve the accuracy of the verified responses, where necessary providing the completed questionnaire with comments.
   - After the necessary rounds of iterations and amendments, a pre-final questionnaire is sent to the concerned Member State for final approval.
   - Once formal approval was received, the questionnaire is considered validated and used for the analysis, scoring and ranking.

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

ANNEX A: DEFINITION OF INDICATORS

1. Legal Measures

Legislation is a critical measure for providing a harmonized framework for entities to align themselves to a common regulatory basis, whether on the matter of prohibition of specified criminal conduct or minimum regulatory requirements. Legal measures also allow a nation state to set down the basic response mechanisms to breach: through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. A legislative framework sets the minimum standards of behaviour across the board, applicable to all, and on which further cybersecurity capabilities can be built. Ultimately, the goal is to enable all nation states to have adequate legislation in place in order to harmonize practices supranational and offer a setting for interoperable measures, facilitating international combat against cybercrime.

The legal environment can be measured based on the existence and number of legal institutions and frameworks dealing with cybersecurity and cybercrime. The sub-group is composed of the following performance indicators:

1.1 Cybercriminal Legislation

Cybercrime legislation designates laws on the unauthorized (without right) access, interference, interception of computers, systems and data. This also includes procedural law, and any existing articles on the expedited preservation of stored computer data, production orders, real-time collection of computer data, extradition, mutual assistance, confidentiality and limitation on use; as well as any case law on cybercrime or computer misuse.

1.2 Cybersecurity Regulation

Cybersecurity regulation designates 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.

2. Technical Measures

Technology is the first line of defence against cyber threats and malicious online agents. Without adequate technical measures and the capabilities to detect and respond to cyberattacks, nation states and their respective entities remain vulnerable to cyber threats. The emergence and success of ICTs can only truly prosper in a climate of trust and security. Nation states therefore need to be capable of developing strategies for the establishment of accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be accompanied by the creation of a national entity focused on dealing with cyber incidents at a national level, at the very least with a responsible government agency and with an accompanying national framework for watch, warning and incident response.

Technical measures can be measured based on the existence and number of technical institutions and frameworks dealing with cybersecurity endorsed or created by the nation state. The sub-group is composed of the following performance indicators:

2.1 National CERT/CIRT/CSIRT

The establishment of a CIRT/CERT/CSIRT with national responsibility provides the capabilities to identify, defend, respond and manage cyber threats and enhance cyberspace security in the nation state. This ability needs to be coupled with the gathering of its own intelligence instead of relying on secondary reporting of security incidents whether from the CIRT's constituencies or from other sources.

2.2 Government CERT/CIRT/CSIRT

A government CERT/CIRT/CSIRT is an entity that responds to computer security or cyber security incidents which affects solely governmental institutions. Apart from reactive services, it may also engage in proactive services such as vulnerability analysis and security audits. Unlike the National CERT which services both the private and public sectors, the Government CERT provides its services to constituents from the public sector only.

2.3 Sectoral CERT/CIRT/CSRIT

A Sectoral CERT/CIRT/CSIRT is an entity that responds to computer security or cyber security incidents which affect a specific sector. Sectoral CERTs are usually established for critical sectors such as Healthcare, Public Utilities, Emergency Services and the Financial Sector. Unlike the Government CERT which services the public sector, the Sectoral CERT provides its services to constituents from a single sector only.

2.4 Cybersecurity Standards Implementation Framework for Organizations

This indicator measures the 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.

2.5 Cybersecurity Standards and Certification for Professionals

This indicator measures 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), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), (No Suggestions) Certification, Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute, CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc.

2.6 Child Online Protection

This indicator measure 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.

3. Organizational Measures

Organization and procedural measures are necessary for the proper implementation of any type of national initiative. A broad strategic objective needs to be set by the nation state, with a comprehensive plan in implementation, delivery and measurement. Structures such as national agencies need to put in place in order to put the strategy into effect and evaluate the success or failure of the plan. Without a national strategy, governance model and supervisory body, efforts in different sectors and industries become disparate and unconnected, thwarting efforts to reach national harmonization in terms of cybersecurity capability development.

The organizational structures can be measured based on the existence and number of institutions and strategies organizing cybersecurity development at the national level. The creation of effective organizational structures is necessary for promoting cybersecurity, combating cybercrime and promoting the role of watch, warning and

incident response to ensure intra-agency, cross-sector and cross-border coordination between new and existing initiatives. The sub-group is composed of the following performance indicators:

3.1 Strategy

The development of policy to promote cybersecurity is recognized as a top priority. A national strategy for cybersecurity should maintain resilient and reliable information infrastructure and aim to ensure the safety of citizens; protect the material and intellectual assets of citizens, organizations and the State; prevent cyber-attacks against critical infrastructures; and minimize damage and recovery times from cyber-attacks. Policies on National Cybersecurity Strategies or National Plans for the Protection of Information Infrastructures are those officially defined and endorsed by a nation sate, and can include the following commitments: establishing clear responsibility for cybersecurity at all levels of government (local, regional and federal or national), with clearly defined roles and responsibilities; making a clear commitment to cybersecurity, which is public and transparent; encouraging private sector involvement and partnership in government-led initiatives to promote cybersecurity; a roadmap for governance that identifies key stakeholders.

3.2 Responsible Agency

A responsible agency for implementing a national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils or cross-disciplinary centers. Most national agencies will be directly responsible for watch and warning systems and incident response, and for the development of organizational structures needed for coordinating responses to cyber-attacks.

3.3 Cybersecurity Metrics

This indicator measures the 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 rating or evaluating resulting performance for future improvements. For example, based on ISO/IEC 27002-2005, a national cybersecurity standard (NCSec) can help nation states respond to specify cybersecurity requirements. This referential is split into five domains: NCSec Strategy and Policies; NCSec Organizational Structures; NCSec Implementation; National Coordination; Cybersecurity Awareness Activities.

4. Capacity Building

Capacity building is intrinsic to the first three measures (legal, technical and organizational). Understanding the technology, the risk and the implications can help to develop better legislation, better policies and strategies, and better organization as to the various roles and responsibilities. Cybersecurity is a relatively new area, not much older than the internet itself. This area of study is most often tackled from a technological perspective; yet there are numerous socio-economic and political implications that have applicability in this area. Human and institutional capacity building is necessary to enhance knowledge and know-how across sectors, to apply the most appropriate solutions, and promote the development of the most competent professionals.

A capacity building framework for promoting cybersecurity should include awareness-raising and the availability of resources. Capacity building can be measured based on the existence and number of research and development, education and training programs, and certified professionals and public sector agencies. Some data is collected through reliable secondary sources which actually provide certified training worldwide. The sub-group is composed of the following performance indicators:

4.1 Public Awareness Campaigns

Public awareness include efforts to promote widespread publicity campaigns to reach as many people as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centres, computer stores, 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 material and establishing cybersecurity adoption.

4.2 Cybersecurity Training

Cybersecurity training for law enforcement officers, judicial and other legal actors designates 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.

4.3 Cybersecurity Professional Training Courses

This indicator measures the existence of short term national or sector-specific educational and professional training programs for raising awareness with the general public (i.e. national cybersecurity awareness day, week, or month), promoting cybersecurity courses in the workforce (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector.

4.4 National Education Programs and Academic Curriculums

This indicator looks at the existence and the promotion of national education courses and programs to train the younger generation in cybersecurity related skills and professions in schools, colleges, universities and other learning institutes. Cybersecurity related skills include but are not limited to setting strong passwords and not revealing personal information online. Cybersecurity related professions include but are not limited to cryptanalysts, digital forensics experts, incident responders, security architects and penetration testers and general master programmes in cybersecurity.

4.5 Cybersecurity Research & Development Programs

This indicator measures the investment into national cybersecurity research and development programs at institutions which could be private, public, academic, non-governmental or international. It also considers the presence of a nationally recognised 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 will increase co-ordination among the various institutions and sharing of resources.

4.6 Incentive Mechanisms

This indicator looks at any incentive efforts by 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 cyber security capacity building activities. Incentives increase the demand for cybersecurity related services and products which improves defences against cyber threats.

4.7 Home Grown Cybersecurity Industry

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

5. Cooperation

Cybersecurity requires input from all sectors and disciplines and for this reason needs to be tackled from a multi-stakeholder approach. Cooperation enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application. Information sharing is difficult at best between different disciplines, and within private sector operators. It becomes increasingly so at the international level. However,

the cybercrime problem is one of a global nature and is blind to national borders or sectoral distinctions. Cooperation enables sharing of threat information, attack scenarios and best practices in response and defence. Greater cooperative initiatives 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 can be measured based on the existence and number of partnerships, cooperative frameworks and information sharing networks. The sub-group is composed of the following performance indicators:

5.1 Bilateral Agreements

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, regional entity or an international organization (i.e. the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether the agreement is legally binding or pending ratification. Information sharing refers to the sharing of threat intelligence while assets designate the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.

5.2 Multilateral Agreements

Multilateral agreements (one to multi-party agreements) refers to any officially recognized national or sector-specific programs 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). The indicator also measures whether the agreement is legally binding or pending ratification. Information sharing refers to the sharing of threat intelligence while assets designate the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.

5.3 Public-Private Partnerships

Public-private partnerships (PPP) refer to ventures between the public and private sector. This performance indicator can be measured by the number of officially recognized national or sector-specific PPPs for sharing cybersecurity information (threat intelligence) 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.

5.4 Interagency Partnerships

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, programs and other public sector institutions.

5.5 Cybersecurity Best Practices

This indicator measures the research and publication of best practices and guidelines on cybersecurity technology and its use, management, and application to various scenarios. Best practices are methods or procedures which have a proven track record of success. Adopting best practices will not only reduce the probability of failure but also increase efficiency.

ANNEX B: COMPUTATIONAL DETAILS

The statistical model used is based on a Multi-Criteria Analysis (MCA).

The MCA establishes preferences between options by reference to an explicit set of identified objectives and for which there are established measurable criteria to assess the extent to which the objectives have been achieved (the list of indicators as per Annex A).

A simple linear additive evaluation model is applied. The MCA performance matrix describes the options and each column describes the performance of the options against each criterion. The individual performance assessment is numerical.

The benchmark scoring is based on a set of the indicators. Each of five sub-indices is weighted equally through a normalization technique. 0 points are allocated where there are no activities; 1 point is allocation for action.

Below is an example of how points might be allocated.

NOTE: The below table not the final table that will be used. Such final table will be produced by the group of experts that will agree on the weights to be assigned for each specific question. The below table is provided to clarify the approach.

Nb	**Indicator**	**Points**
1.	Legal Measures	**39**
1.1	Cybercriminal Legislation	14
1.2	Cybersecurity Regulation	21
1.3	Cybersecurity Training	4
2.	Technical Measures	**17**
2.1.	National CERT/CIRT/CSIRT	5
2.2.	Government CERT/CRIT/CSIRT	1
2.3.	Sectoral CERT/CIRT/CSRIT	1
2.4.	Cybersecurity Standards Implementation Framework for Organizations	3
2.5.	Cybersecurity Standards and Certification for Professionals	3
2.6.	Child Online Protection	4
3.	Organizational Measures	**25**
3.1.	Strategy	16
3.2.	Responsible Agency	3
3.3.	Cybersecurity Metrics	6

4.	Capacity Building	**27**
4.1.	Standardization Bodies	2
4.2.	Cybersecurity Best Practices	1
4.3.	Cybersecurity Research & Development Programs	3
4.4.	Public Awareness Campaigns	7
4.5.	Cybersecurity Professional Training Courses	4
4.6.	National Education Programs and Academic Curriculums	4
4.7.	Incentive Mechanisms	2
4.8.	Home Grown Cybersecurity Industry	4
5.	Cooperation	**32**
5.1.	Bilateral Agreements	15
5.2.	Multilateral Agreements	7
5.3.	Public-Private Partnerships	7
5.4.	Interagency Partnerships	3
	Total	**140**