Telecommunication
Development Sector
CYBERSECURITY
INTERNATIONAL TELECOMMUNICATION UNION

2015/16

Reference Model

The Global Cyber Security Index measures the cybersecurity commitment of Member States. The second iteration for 2015/2016 strives to bring in a unique value addition to the sphere of existing Cybersecurity indices through a multi-stakeholder collaborative platform.

I Introduction

The Global Cybersecurity Index (GCI) is a composite index combining 24 indicators into one benchmark measure to monitor and compare the level of Member States' cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the Global Cybersecurity Agenda (GCA). These pillars form the five sub-indices of GCI. First developed by ITU in partnership with ABI Research in 2013, and with results presented in November 2014, the GCI is included under Resolution 130 (Rev. Busan, 2014). It is being enhanced in response to ITU Member States' request to develop a cybersecurity index and publish updates regularly.

The main objectives of the GCI are to measure:

- the type, level, and evolution of comparative cybersecurity commitment in countries over time;
- 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 to motivate them to take action to improve their relative GCI ranking, thus helping raise the overall level of cybersecurity worldwide. Through the information collected, the GCI aims to illustrate the practices of other countries so that Member States can implement selected aspects suitable to their national environments, with the added benefit of helping to promote and spread best practices and foster a global culture of cybersecurity.

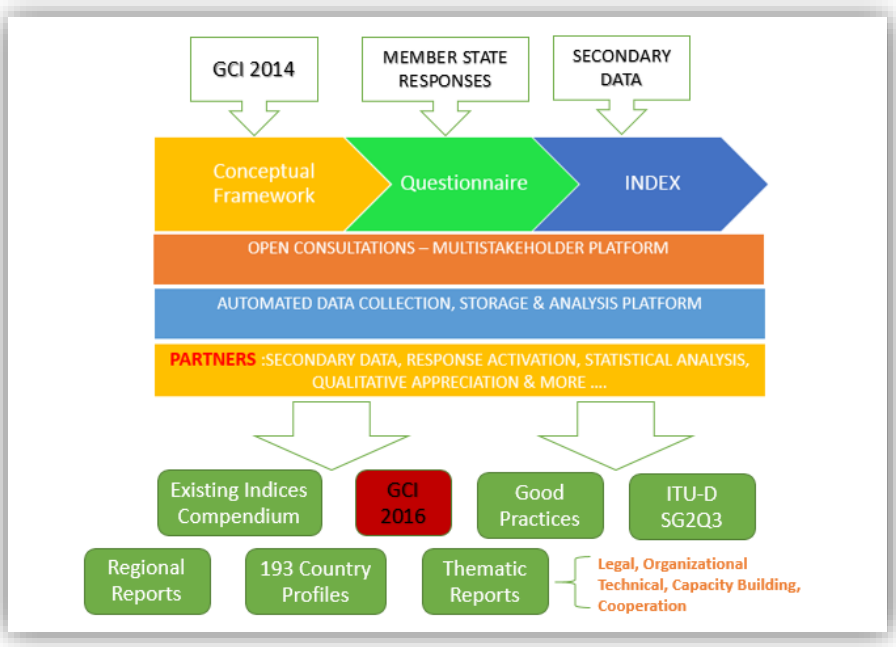
II Background

The GCI is included in the 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".

A first iteration of the GCI was conducted in 2013/2014 in partnership with ABI Research, and the final results have been published (see http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx). A total of 105 countries out of 193 ITU Member States responded. Secondary data was used to build the index for non-respondents and the research outcomes were sent to them for verification/endorsement.

New GCI approach

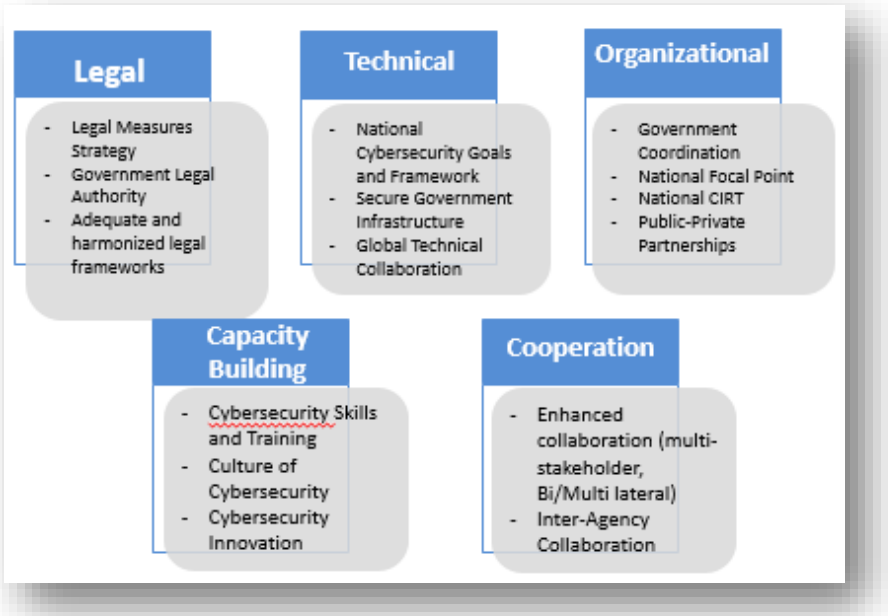
Following feedback received from various communities, a second iteration of the GCI is under preparation. This new version is being formulated around an extended participation from Member States, experts and industry stakeholders as contributing partners. An enhanced reference model has thereby been devised. Whilst GCI score would remain the key outcome, several other deliverables are envisaged including Country Profiles, Best Practices, and Thematic reports including the state of play for cybersecurity norm building. The primary data collection mechanism is an online questionnaire to be completed by Member States.



III Conceptual Framework

The GCA is the ITU framework for international multi-stakeholder cooperation in cybersecurity aimed at building synergies with current and future initiatives.

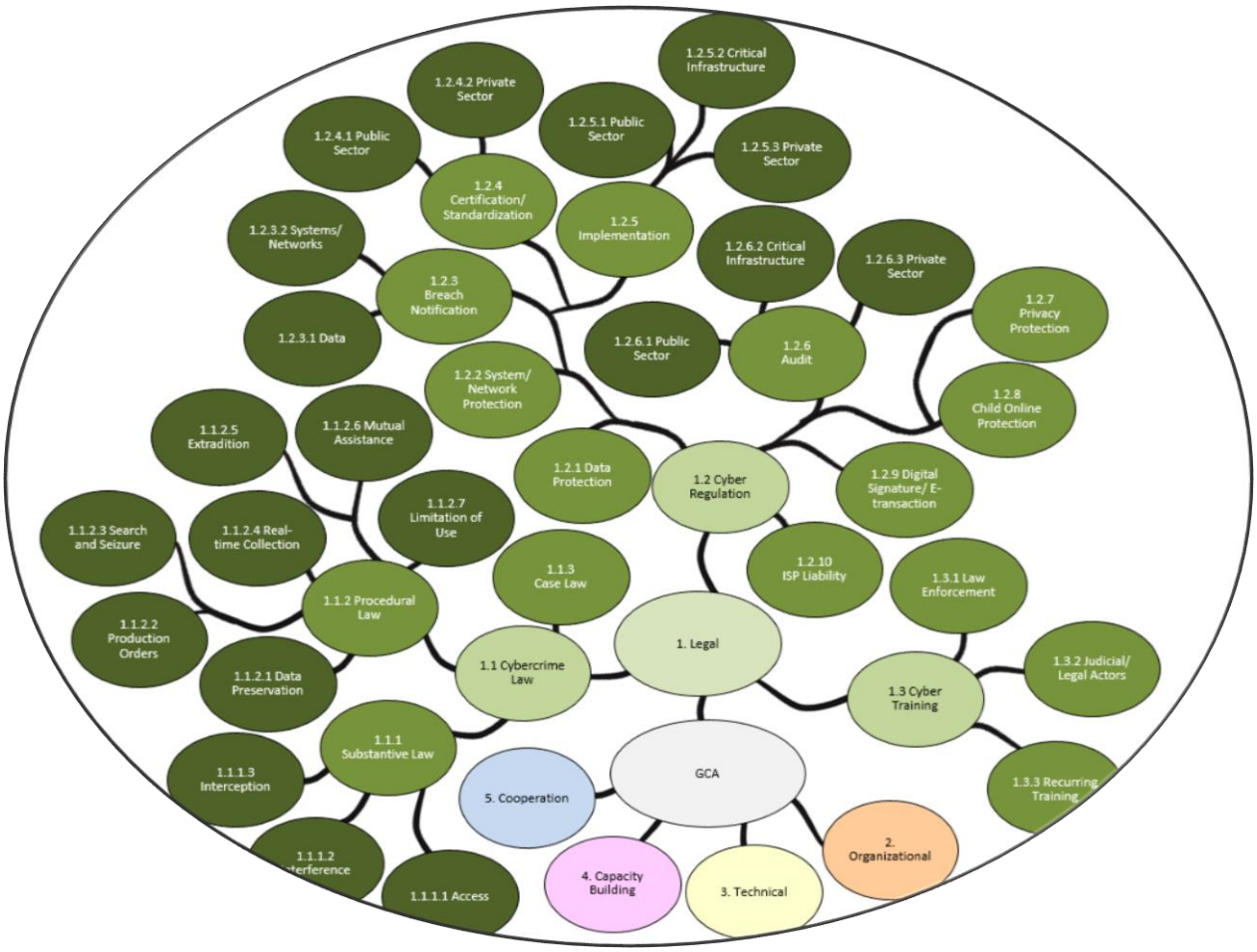
Global cybersecurity agenda



It focuses on the following five pillars: legal, technical, organizational, capacity building and cooperation.

The GCA is the primary reference for establishing the objectives of the GCI initiative and the five GCA pillars form the basis for elaborating the GCI conceptual framework.

The figure below is an illustration of the linkages between the main index, the five sub-indices (different colours) and the GCA. This is in keeping with the cybersecurity development tree map elaborated in the methodology section and its maturity increases as indicated by the deeper tones of colour. The tree has been expanded for a sub-part of the legal pillar only for the sake of clarity and given the space constraint in presenting the complete picture. The tree concept has been expanded for all the five pillars. Each tree level refers to a level in the questionnaire.



Legal sub-index: 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 contributes to establish minimum standards of behaviour across the board as well as to facilitate the development of cybersecurity capabilities at national level, with the objective of ensuring the presence of an adequate domestic framework to address cybercrime In this context, the GCI can be a tool to enable harmonization, promote good practices at the regional/international level, and facilitate international cooperation ***The legal environment is evaluated based on the presence or absence of legal frameworks dealing with cybersecurity and cybercrime.***

Technical sub-index: Technology plays a key role in the defence 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 capabilities and processes to effectively use technology as enabler in addressing cyber threats. This would include 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, as well as national

standards bodies to incorporate international standards and industry best practices into domestic cybersecurity efforts. ***The technical component is evaluated based on the presence or absence of Information Technology related measures, including standardization bodies, dealing with cybersecurity by the nation state.***

Organizational sub-index: 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 or absence of institutions and strategies concerning cybersecurity development at the national level.***

Capacity-building sub-index: 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 programmes, as well as relevant programs run by professionals and public sector agencies.***

Cooperation sub-index: Cybersecurity and Cybercrime are global issues and are 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, scope and type of partnerships, cooperative frameworks, and information sharing networks.***

IV Methodology

The GCI includes 24 indicators (157 questions). 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 in contributing towards the main GCI objectives and conceptual framework;
- data availability and quality;
- possibility of cross verification through secondary data.

The whole concept of a new iteration of the GCI is based on a cybersecurity development tree map and binary answer possibilities. The tree map concept, which is illustrated below, is an answer to different possible paths that might be taken by countries in order to enhance their cybersecurity commitment. Each of the five pillars is associated with a specific colour (the same code as that used in the Cyberwellness country profiles). The deeper the path taken, indicating a more developed level of commitment, the deeper the colour depicting it becomes.

The levels of efforts undertaken on cybersecurity among countries, as well as the different cybersecurity needs reflected by a country's overall ICT development status, were taken into consideration.

The concept is based on an assumption that the more commitment the country has shown on cybersecurity, the more presence of cybersecurity related capabilities and expertise observed will be. Therefore, the further a country goes along the tree map by confirming the presence of pre-identified capabilities, the more mature and sophisticated the cybersecurity development is within that country, allowing it to obtain a higher GCI score.

The rationale behind using binary answer possibilities is the elimination of opinion-based evaluation and of any possible bias towards certain types of answers. Moreover, the simple binary concept will allow quicker and more direct evaluation as it will not require lengthy answers from countries. This, in turn, is assumed to accelerate and streamline the process of providing answers and further evaluation. The idea is that the respondent will only confirm the presence or lack of certain pre-identified cybersecurity capabilities.

An online survey mechanism, which will be used for gathering answers and uploading all relevant materials, will enable the extraction of good practices, information for Cyberwellness profiles and a set of thematic qualitative evaluations by a panel of experts.

The key difference in methodology between GCI Version 1 and GCI Version 2 is the use of a binary system at source instead of a three-level system. The binary system evaluates the existence or absence of a specific activity, department, or measure. The facility for respondents to upload supporting documents and URLs is a way of providing more information to substantiate the binary response. Furthermore, a number of new questions have been added in each of the five pillars in order to refine the depth of research.

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

Computation details

The statistical model used by GCI will be based on a Multi-Criteria Analysis (MCA). The MCA establishes preferences between options by reference to an explicit set of identified objectives for which there are established measurable criteria to assess the extent to which the objectives have been achieved (see Annex A for the list of indicators). A simple linear additive evaluation model will be 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 will be based on the indicators below. A panel of experts in the field of cybersecurity has weighed each of five sub-indices.

The panel of experts has been appointed with the aim of providing expert, thorough, and unbiased recommendation on the weight to be assigned to each question within the survey questionnaire. The weight of questions that has been recommended by the panel of experts reflects the importance of specific dimensions of the overall cybersecurity commitment of a nation state.

The panel of experts consists of around 10 -15 experts in the field of cybersecurity. Participation in the panel of experts has been open to following:

- One appointee of each partner of the GCI (both strategic and contributing) is proposed. It is up to the Partner to decide on participation.
- Volunteers participating in the ITU D SG2Q3
- Well-recognized and respected experts in the field of cybersecurity not being in any of the above categories.

The composition of the panel of experts reflects regional diversity, diversity of expertise, as well as balance between different stakeholders, including governments, private sector and academia.

The evaluation process requires the experts to provide their recommendations regarding the weight for each question. After all inputs have been received by the ITU, weights have been averaged and presented to the experts for discussion, with particular focus on outliers and any other pattern of disagreement;

0 points are allocated where there are no activities; 1 point is allocated for action. The final scores per indicator will be reduced to total 100 points.

Nb	Indicator	Points
1.	Legal measures	
1.1	Cybercriminal legislation	
1.2	Cybersecurity regulation	
1.3	Cybersecurity training	
2.	Technical measures	
2.1.	National CERT/CIRT/CSIRT	
2.2.	Government CERT/CIRT/CSIRT	
2.3.	Sectoral CERT/CIRT/CSIRT	
2.4.	Cybersecurity standards implementation framework for organizations	
2.5.	Cybersecurity standards and certification for professionals	
2.6.	Child online protection	
3.	Organizational measures	
3.1.	Strategy	
3.2.	Responsible agency	
3.3.	Cybersecurity metrics	
4.	Capacity building	
4.1.	Standardization bodies	
4.2.	Cybersecurity best practices	
4.3.	Cybersecurity research and development programmes	
4.4.	Public awareness campaigns	
4.5.	Cybersecurity professional training courses	
4.6.	National education programmes and academic curricula	
4.7.	Incentive mechanisms	
4.8.	Home-grown cybersecurity industry	
5.	Cooperation	
5.1.	Bilateral agreements	
5.2.	Multilateral agreements	
5.3	International fora participation	
5.4.	Public-private partnerships	
5.5.	Interagency partnerships	
	Total	100

Notation:

x_{qc} value of the individual indicator *q* for country *c*, with *q* = 1,...,Q and *c* = 1,...,M.

I_{qc} normalized value of individual indicator *q* for country *c*

CI_c value of the composite indicator for country *c.*

The benchmark used will be the score of the hypothetical country that maximizes the overall commitment (100) points. The resulting composite index will range between 0 (worst possible readiness) and 1 (the benchmark):

$$CI_c = \frac{I_{qc}}{100}$$

The normalization technique will be based on a ranking method:

$$I_{qc} = Rank\ (x_{qc})$$

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 on minimum regulatory requirements. Legal measures also allow a nation state to set down the basic response mechanisms to breaches, such as 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 in an effort to build consensus around cybersecurity norms and to facilitate international cooperation in combatting 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 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 laws, and any existing articles on the expedited preservation of stored computer data, production orders, real-time collection of computer data, extradition of cyber perpetrators, mutual assistance, confidentiality and limitation on use; as well as any case law on cybercrime or computer misuse.

1.2 Cybersecurity legislation

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.

1.3 Cybersecurity training

Cybersecurity training for law enforcement officers, judicial, and other legal actors designates professional and technical, potentially recurring, training for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession. Training targets are both public and private professionals.

2 Technical measures

Technology is the first line of defence against cyberthreats 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 cyberthreats. 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 that promote the use of technology as enabler in addressing cyber threats.

This includes 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, as well as national standards bodies to incorporate international standards and industry best practices into domestic cybersecurity efforts.

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

2.1 National CERT/CIRT/CSIRT

The establishment of a CIRT/CERT/CSIRT[1] with national responsibility provides the capabilities to identify, defend, respond and manage cyberthreats and enhance cyberspace security in the nation state. This ability should be complemented with the gathering of the nation's own intelligence from secondary reporting of security incidents whether from the CIRT's constituencies and/or from other sources.

2.2 Government CERT/CIRT/CSIRT

A government CERT/CIRT/CSIRT is an entity that responds to computer security or cybersecurity incidents which affect 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 only to the constituents of the public sector.

2.3 Sectoral CERT/CIRT/CSIRT

A sectoral CERT/CIRT/CSIRT 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, emergency services and the financial sector. Unlike the government CERT, which services the public sector, the sectoral CERT provides its services only to the constituents of specific sector.

2.4 Cybersecurity standards implementation framework for organizations

This indicator measures the existence of a government-approved (or endorsed) framework(s) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within 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(s) 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 (ISC²), 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 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.

---

[1] A Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), or Computer Security Incident Response Team (CSIRT) is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches. Source: A step by step approach on how to set up a CSIRT – ENISA

3 Organizational measures

Organization and procedural measures are necessary for the proper implementation of any type of national initiative. A broad strategic objective to address cybersecurity needs to be set by the nation state, with a comprehensive plan in implementation, delivery and measurement. Structures such as national agencies need to be established 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 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 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 state, 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; creating 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 centres. Most national agencies will be directly responsible for watch and warning systems and incident response, and for the development of the organizational structures needed for coordinating responses to cyberattacks.

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. The objective is to measure the readiness of the country in assessing the risks posed by cyberthreats as well as its capacity in evaluating the response, though periodical audits. The indicator does provide a qualitative analysis, but rather aims at emphasizing the importance on the continuous improvement of the efforts deployed.

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, policies, strategies and 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 programmes, 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 indicators:

4.1 Standardization bodies

Standardization is a good indicator of the level of maturity of a technology, and the emergence of new standards in key areas underlines the vital importance of standards. Although cybersecurity has always been an issue for national security and treated differently in different countries, common approaches are supported by commonly recognized standards. 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. This indicator measures the existence of a national cybersecurity standardization body and activities in the development and implementation of cybersecurity standards.

4.2 Cybersecurity good 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.

4.3 Cybersecurity research and development programmes

This indicator measures the investment into national cybersecurity research and development programmes at institutions which could be private, public, academic, non-governmental or international. It also considers the presence of a nationally recognized institutional body overseeing the programme. Cybersecurity research programmes include, but are not limited to, malware analysis, cryptography research and research into system vulnerabilities and security models and concepts. Cybersecurity development programmes 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 coordination among the various institutions and sharing of resources.

4.4 Public awareness campaigns

Public awareness includes 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 adoption of those cybersecurity practises that would reduce exposure of the general public to cyberthreats (e.g. Stop, Think, Connect campaign). The presence or absence of direct consultations will also be measured, such as incentives to develop cybersecurity clinics for underserved stakeholders potentially housed at educational institutions that would have the dual-benefit of increasing the availability of applied cybersecurity training for the next generation of cybersecurity professionals.

4.5 Cybersecurity professional training courses

This indicator measures the existence of national or sector-specific educational and professional training programmes.

4.6 National education programmes and academic curricula

This indicator looks at the 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 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.

4.7 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. Incentives increase the demand for cybersecurity-related services and products, which improves defences against cyberthreats.

4.8 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 an input from all sectors and disciplines, and for this reason needs to be tackled though 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, cyberthreats are global in nature and blind to national borders or sectoral distinctions. Cooperation enables sharing of threat information, attack scenarios and best practices in response, mitigations, 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 indicators:

5.1 Bilateral agreements

Bilateral agreements (one-to-one agreements) refer to any officially recognized or ratified 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 multiparty agreements) refers to any officially recognized or ratified 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). 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 Participation in international fora

A. As part of enhancing collaboration in Cybersecurity, the commitment of governments to participate in Cybersecurity events is hereby measured. Such events include regional and international workshops,

conferences and trainings. The World Summit on Information Society, Regional Cybersecurity forum, Regional Cyberdrills, FIRST annual summit and technical colloquia, the Global Forum on Cyber Expertise (GFCE), the Internet Governance Forum as well as conferences by AfricaCERT, APCERT, OICCERT,GCC,OAS are such examples.

5.4 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.

5.5 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, programmes and other public sector institutions.