GUIDELINES FOR UTILIZATION OF THE GLOBAL CYBERSECURITY AGENDA BY THE ITU

Section 1. Introduction

1.1 The ITU 2018 Plenipotentiary Conference in Dubai adopted Resolution 130: *Strengthening the role of ITU in building confidence and security in the use of information and communication technologies***.** The Resolution resolves, inter alia, *to utilize the Global Cybersecurity Agenda (GCA) framework in order to further guide the work of the Union on efforts to build confidence and security in the use of Information and Communication Technologies (ICTs).*

1.2 During the plenary discussions just prior to the adoption of Resolution 130, the ITU Secretary-General *noted with satisfaction that, during the discussions on the draft resolution, the value of the GCA had been widely recognised. He appealed to the Plenary to accept the retention on resolves 12.1 which would allow ITU to utilize the GCA to guide its work on confidence and security in ICTs. He would seek advice from the Council and from the former chairman of the High-Level Experts Group dealing with the GCA, Judge Stein Schjolberg, in that connection.*[1]

1.3 A Report of the former Chairman of the GCA High-Level Experts Group (HLEG) was submitted to the 2019 session of the ITU Council, advising that appropriate guidelines may be elaborated for better utilization of the Global Cybersecurity Agenda.[2] At this meeting, the Council instructed the Secretary-General, in parallel, to submit to the next Council session (1) a report explaining how the ITU is currently utilizing the GCA framework and (2) with the involvement of Member States, appropriate guidelines developed for utilization of the GCA by the ITU for Council's consideration and approval.[3]

1.4 Pursuant to these instructions, the process for developing the Guidelines was set out in Circular Letter (CL-20/55) and two open consultations were held for all WSIS stakeholders on 23 April 2020 and 1 March 2021 to provide comments on the Guidelines (Open Consultation). Over 160 participants attended the meetings and provided feedback section by section on the Guidelines. All comments received from participants in writing prior or subsequent to the Open Consultations have been published on the GCA website.

1.5 Taking into account the inputs received, the report explaining how the ITU is currently utilizing the GCA framework was developed by the secretariat (Secretariat report) and the guidelines for utilization of the GCA (Guidelines) were formulated with the support of Chief Judge (Ret.) Stein Schjolberg (former HLEG Chair) and with the involvement of Member States, for consideration and approval by Council. The Secretary-General is also grateful for the guidance and contribution of Prof. Solange Ghernaouti (Swiss Cybersecurity Advisory & Research Group, University of Lausanne) on the sections relating to GCA Pillars 2 and 4, and of Mr. Noboru Nakatani (Former Executive Director of the INTERPOL Global Complex for Innovation) on the section relating to GCA Pillar 3. It is important to note that this effort is not meant to, and will not, address matters related to the revision of the GCA.

1.6 Due to the COVID-19 pandemic, the presentation of these documents was postponed to VCC 2021 which took place from 8-18 June 2021. Following VCC 2021, Council Member States noted the secretariat Report and made a decision by correspondence regarding the draft Guidelines "*to instruct the secretariat to*

---

[1] Minutes of the Plenipotentiary Seventeenth Plenary Meeting, Dubai, Thursday 15 November 2018, available at https://www.itu.int/md/S18-PP-C-0174/en

[2] Transmission of the Report from the former Chairman of GCA High-Level Experts Group (C19/58), ITU, 8 May 2019, available at https://www.itu.int/md/S19-CL-C-0058/en

[3] Summary record of the sixth Plenary meeting (C19/117), ITU, 20 June 2019, available at https://www.itu.int/md/S19-CL-C-0117/en

conduct further consultations with Council Member States, taking into account the inputs received and the comments made at this meeting. The secretariat should bring back a revised document 71 for consideration and approval at the next session of the Council".

1.7 Accordingly, further consultations were conducted with Council Member States and, taking into account the inputs received, two documents were prepared:

a) an Information Document (C22/INF/8) presenting the background, evolving landscape and context for development of these Guidelines; and

b) these Guidelines set out below that have been developed for consideration and approval of Council 2022.

In developing these documents, recommendations of the HLEG Report 2008, the activities of ITU since then, developments in the field since 2008, and inputs received from Member States and other stakeholders (pursuant to Circular Letters (CL-20/18 & CL-20/55) have been taken into account. The 2022 session of ITU Council approved these Guidelines for transmission to the 2022 ITU Plenipotentiary Conference.

1.8 While recognizing the mutual inter-dependence of the five Pillars, each section addresses a specific GCA pillar and proposes specific guidelines for its utilization. Section 2 focuses on Legal Measures. Section 3 covers Technical and Procedural Measures. Section 4 addresses Capacity Building. Section 5 is on Organizational Structures and Section 6 covers International Cooperation. Section 7 contains some general cross-cutting guidelines for use of the GCA framework.

Section 2. Pillar 1 - Legal Measures

2. Given the rapid advancements in technology, measures taken by organizations and countries need to evolve to keep pace with the rate of change. This brings new complexities to the challenge of cybersecurity, requiring close examination from a variety of different perspectives. In this context, proposed guidelines for utilization of Pillar 1 by ITU within its mandate are set out below:

a. ITU should continue its efforts to facilitate multi-stakeholder discussions and collaboration for addressing the challenges associated with cybersecurity, and in particular, strengthen its relationship with all stakeholders to deliver assistance to Member States in this regard.

b. ITU should continue to work with relevant partners to foster development and maintenance of resources on cybersecurity and cybercrime legislation to help Member States understand the legal aspects of cybersecurity including existing relevant regional and international frameworks and best practices, while also supporting the exchange of experience and knowledge among Member States to support their efforts in developing frameworks on the subject.

c. ITU, in collaboration with all relevant stakeholders, should promote a better understanding of the cybersecurity-related legal challenges and risks posed by emerging technologies and facilitate the exchange of case studies and good practices at the national, regional, and international level.

d. ITU should continue to strengthen the Child Online Protection programme as a platform to work with partners and stakeholders to promote the exchange of knowledge, information, and activities (including those related to legal measures) that can facilitate and support country action on this critical issue.

Section 3. Pillar 2 - Technical & Procedural Measures

3. Recommendations related to Pillar 2 in the HLEG Report 2008 remain valid. In light of this, the following guidelines are proposed for Pillar 2:

a. ITU study groups should focus on telecommunication/ICT related emerging technologies, in order to study and suggest cybersecurity guidelines and Recommendations in building confidence and security in the use of such technologies and recommend Member States to voluntarily apply these in a timely manner.

b. A mechanism for close cooperation should be established among the various ITU-T study groups regarding the study of cybersecurity related matters, with SG17 in a coordinating/leading role, so that the highest possible degree of end-to-end security is maintained throughout the standardization process of all components and interfaces of ICT products.

c. Close coordination and collaboration, on the basis of reciprocity of ITU with other SDOs, should be encouraged to ensure that the end-to-end product security of diverse applications and services is maintained throughout the product cycle.

d. ITU should continue to disseminate global ICT security standards and also work with other standardization organizations and industry groups to encourage them to submit their standards on technical and procedural measures to ITU-T and ITU-R for approval as ITU-T and ITU-R Recommendations.

e. ITU should continue its efforts towards developing Recommendations on technical and procedural measures for cybersecurity in areas within its mandate, incentivizing its members to increase their participation in related ITU standardization activities and through strategic partnerships and consultation with universities and SDOs**.**

f. ITU should continue to encourage its members to initiate/participate in mutual certification arrangements towards harmonized cybersecurity standards.

Section 4. Guidelines to Utilize Pillar 3 – Organizational Structures

4. While recognizing that the recommendations in the HLEG Report 2008 have served well in guiding ITU efforts under Pillar 3 and continue to remain relevant, the following proposed guidelines, relevant in particular to the work of the ITU Development Bureau (BDT), could help strengthen efforts in this regard:

a. ITU should continue to assist developing countries, least-developed countries and Small Island Developing states (SIDS) in the design and implementation of National CIRTs and other related technical units/organizations.

b. In order to avoid duplicative efforts, ITU should continue to promote an open and inclusive collaboration as well as coordination, within its mandate, among various national, regional or international organizations engaged in the effort to establish sustainable national organizational structures.

c. ITU should increase its efforts to measure institutional commitments of Member States, leveraging tools such as the Global Cybersecurity Index (GCI) to promote cybersecurity as a crosscutting enabler of their digital transformation efforts.

d. For national structures in particular, and at the request of Member States, ITU should assist them with the design of strategies for a whole-of-government coordination framework to improve the coherent and cross-cutting implementation of national cybersecurity efforts.

e. ITU should continue to foster greater collaboration among cybersecurity organizational structures regionally and globally through activities such as cyber drills among others.

Section 5. Guidelines to Utilize Pillar 4 – Capacity Building

5. In light of the above, the GCA and the recommendations contained under this Pillar of the HLEG Report 2008 continue to provide a robust framework that enhances and promotes an interdisciplinary approach to capacity building. Taking this into consideration, it is proposed that ITU, through its Telecommunication Development Bureau (BDT):

a. Continue to promote more open and inclusive collaboration and coordination among various national, regional, or international organizations engaged in building capacity for cybersecurity, in order to ensure impact and avoid duplication of efforts.

b. Continue supporting developing countries least-developed countries and SIDS in cybersecurity capacity building efforts, with the support of the national and international cybersecurity capacity building communities.

c. Continue to assist developing countries, least-developed countries and SIDS in collaboration with interested partners and capacity-development communities, on developing national cybersecurity strategies, plans, policies, and incident response capabilities.

Continue capacity building efforts on bridging the standardisation gap, including by providing technical assistance to countries upon request.

d. Enhance and facilitate the exchange of good practices of Member States in order to help countries lagging in cybersecurity expertise improve their cybersecurity posture and reduce the capacity gap.

e. Continue to evolve its capacity building activities, taking into account the need for new skills to adapt to the opportunities and challenges of emerging technologies in the field of cybersecurity. In this regard, greater collaboration should be fostered with academia, private sector and Member States.

f. Continue to maintain special focus on the needs of the more vulnerable groups—such as women, children, persons with disabilities and persons with specific needs, and persons with age-related disabilities – in capacity building efforts.

g. Continue to develop and strengthen the Global Cybersecurity Index (GCI) as a tool for capacity building and awareness creation.

h. Continue to support Member States with capacity-building programmes for youth in primary, secondary, university, and adult professional education systems in order to contribute to training more cybersecurity professionals globally and to raise cybersecurity awareness

i. Continue to facilitate identification of cybersecurity-related research activities among stakeholders, especially in emerging technology areas, leveraging ITU's private sector and academic membership.

j. Disseminate tools, resources and good practices to Member States, industry, and other stakeholders with an aim to support their efforts in building the capacity of MSMEs to build trust and confidence in the use of ICTs, and continue to promote a culture of cybersecurity.

Section 6. Guidelines to Utilize Pillar 5 - International Cooperation

6. The United Nations has a unique role in fostering cooperation, dialogue, and coordination among all nations, as well as with the private sector and other stakeholders, on global cybersecurity matters. Given the cross-cutting nature of this Pillar, and considering the range of collaborations and partnerships in different sectors of the ITU, it is important for all the sectors of ITU to work closely together and coordinate their efforts, both internally and externally, using effective intersectoral coordination mechanisms and designated focal points. The Recommendations of the HLEG Report 2008 in this regard continue to remain relevant and, based on the information provided in the section above, the following guidelines are further proposed for utilization of Pillar 5 by the ITU in areas within its mandate:

a. Considering its position in the UN system as the specialized agency for ICTs, and sole facilitator of Action Line C5 (Building confidence and security in the use of ICTs), ITU should continue to play a leading role on related developments.

b. Based on the WSIS Process, including those related to Action Line C5, and taking into account the efforts of the UN Secretary-General's High-Level Panel on Digital Cooperation, ITU should help support efforts in bringing different players together, including at the WSIS Forum and IGF, among others.

c. Given the global nature of cybersecurity concerns, broader discussions among key players should continue to be encouraged and facilitated among wider groups that include the private sector, UN bodies, academia, civil society and other stakeholders with an aim to mitigate related challenges. ITU should play an important role in these broader discussions, as appropriate.

d. ITU should continue to explore innovative, flexible, and agile mechanisms for building partnerships, taking into account the rapidly evolving technology sector and the range of new entities that are emerging – especially start-ups and MSMEs.

e. ITU should continue to engage with other key agencies within the UN system to support the UN Secretariat's internal efforts to harmonize and streamline its programs and activities on cybersecurity, in order to be more effective in serving the global community.

Section 7. General Guidelines for the GCA Framework

7. The process of developing guidelines for utilization of the GCA yielded a few broad cross-cutting guidelines that are applicable and relevant across the work of the ITU and the five Pillars of the GCA. Recognizing the strong interlinkages between the Pillars, and the need for ITU and its members to work towards a holistic and comprehensive vision of action on cybersecurity, these general guidelines are proposed below:

a. Given the proliferation of stakeholders, organizations, partnerships, and venues that are working on cybersecurity and driving different aspects of progress, ITU should continue to strengthen and expand its collaborations and engagements to the collective benefit of all such stakeholders, in order to enhance knowledge sharing and exchange of information and expertise while also avoiding duplication of efforts.

b. ITU should serve as a repository of information for the various global activities, initiatives, and projects that are being carried out on different facets of cybersecurity by other stakeholders and organizations active in this field, and who may have the lead mandate, role and/or responsibilities in those specific facets, in order to enable the international community to have an easy point of access to all such resources.

c. All work carried out by ITU pursuant to the GCA should be guided by a clear assessment of the needs and objectives of its members using tools such as the GCI, the deliverables required to meet them, and in accordance with appropriate metrics and measurements that are designed specifically for this purpose.

d. ITU should continue to follow the development and use of new and emerging ICTs in order to guide Member States and stakeholders on the security aspects of these technologies in areas within its mandate and, where relevant, their potential application to counter cyber threats.

e. Given the intrinsically transnational and cross-sectoral impact of cybersecurity, ITU should promote activities, initiatives, and projects that can help Member States foster a whole-of-government approach to tackle the issue.

_____