|  |  |
| --- | --- |
| **Council 2021 Virtual consultation of councillors, 8-18 June 2021** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.04** | **Document C21/82-E** |
| **25 May 2021** |
| **Original: English** |
| Note by the Secretary-General  Contribution from Australia, Canada, Czech Republic, France, Romania, United Kingdom of Great Britain and Northern Ireland | |
| GUIDELINES FOR UTILIZATION OF THE GLOBAL CYBERSECURITY AGENDA | |

I have the honour to transmit to the Member States of the Council a contribution submitted by **Australia, Canada, Czech Republic, France, Romania, United Kingdom of Great Britain and Northern Ireland**.

Houlin ZHAO  
 Secretary-General

**Contribution from Australia, Canada, Czech Republic, France, Romania, United Kingdom of Great Britain and Northern Ireland**

GUIDELINES FOR UTILIZATION OF THE GLOBAL CYBERSECURITY AGENDA

|  |
| --- |
| Summary  It is our view that the Guidelines for utilization of the Global Cybersecurity Agenda (GCA) should be a short and very focussed reference document that takes into consideration the existing work by the ITU on cybersecurity related matters, reflected inter alia by Plenipotentiary Resolution 130, WTSA Resolution 50, WTDC Resolution 45, the work of ITU-T SG-17, and several other initiatives and programs undertaken by the Development Sector.  Action required  This document **is submitted** for Council’s consideration.  **References**  [*https://www.itu.int/en/action/cybersecurity/Pages/default.aspx*](https://www.itu.int/en/action/cybersecurity/Pages/default.aspx)  *[Document C21/36](https://www.itu.int/md/S21-CL-C-0036/en)* |

1. **Introduction**

We appreciate the opportunity to submit further comments on the draft Guidelines for utilization of the GCA, and recognize that substantial efforts have gone in preparing the current draft Guidelines submitted by the Secretary-General for Council’s consideration.

We recognize that the GCA is an important framework comprised of five Pillars: legal measures; technical and procedural measures; organizational structures; capacity building, and international cooperation, in essence a reference document for multi-stakeholder cooperation and collaboration with and between all relevant stakeholders, building on existing initiatives to avoid duplicating efforts.

Furthermore, we wish to highlight that the ITU is already utilizing the GCA in an effective and efficient manner - to the benefit of all ITU membership - as reflected by the Secretary-General’s contribution to the Council.

Recognizing the Union’s mandate and ongoing cybersecurity activities and programs, and the need for ITU and its members to have a clear understanding of the purpose, intended audience and focus of the Guidelines, we are pleased to propose that the Guidelines be a very focused and concise document limited to the following streamlined activities for each of the GCA pillars.

**Pillar 1: Legal Measures**

a. ITU should continue its efforts within its mandate to facilitate multi-stakeholder discussions and collaboration on 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, within its mandate, to develop and maintain cybersecurity legislation resources to help Member States understand the legal aspects of cybersecurity, 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 stakeholders, should work towards a clear and common understanding of the term “emerging technologies”, the opportunities and challenges posed by such technologies, and facilitate an exchange of case studies and good practices on any legal measures that could be applicable 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, activities, including measures that can facilitate and support country action on this critical issue.

**Pillar 2: Technical & Procedural Measures**

a. Within their specific mandates and core competencies, ITU study groups should place an emphasis on further clarifying what is meant by emerging technologies, in order to study and suggest appropriate cybersecurity guidelines for the use of such technologies and recommend Member States to voluntarily apply these in a timely manner.

b. A mechanism for close coordination should be established among the various ITU-T study groups regarding the study of cybersecurity related matters, with SG17 in a coordinating/leading role.

c. Close coordination and collaboration between ITU and private sector led 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 its efforts towards developing voluntary recommendations on technical 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 private sector led SDOs.

## Pillar 3: Organizational Structures

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 among various national, regional or international organizations engaged in the effort to establish sustainable national organizational structures.

c. ITU should maintain its efforts to measure institutional commitments of Member States, leveraging tools such as the Global Cybersecurity Index (GCI).

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.

**Pillar 4: Capacity Building**

a. Continue to promote 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.

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.

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 use the Global Cybersecurity Index (GCI) as a tool for capacity building and awareness creation.

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

i. 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.

# Pillar 5: International Cooperation

a. The ITU should continue to play a leading role in areas within its mandate to foster cooperation, dialogue, and coordination among all nations, as well as with the private sector and other stakeholders on global cybersecurity matters.

b. While bilateral and multilateral discussions among key players should continue to be encouraged, given the global nature of cybersecurity, it is also necessary that broader discussions be facilitated among wider groups, including the private sector, academia, civil society and other stakeholders.

c. 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.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_