|  |  |
| --- | --- |
| **Council 2020Geneva, 9-19 June 2020** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.4** | **Document C20/xx-E** |
| **17 April 2020** |
| **Original: English** |
| Report by the Secretary-General |
| a report explaining how the ITU is currently utilizing the [Global Cybersecurity Agenda](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (GCA) framework |

|  |
| --- |
| SummaryAction requiredThe Council is invited to **note** the Report.\_\_\_\_\_\_\_\_\_\_\_\_References[Global Cybersecurity Agenda (GCA)](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) |

**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)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) *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 Res. 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]](#footnote-1)

**1.3** A Report of the former Chairman of the GCA High-Level Experts Group (HLEG) was submitted to the 2019 session of ITU Council advising that appropriate guidelines may be elaborated for better utilization of the GCA.[[2]](#footnote-2) 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]](#footnote-3)

**1.4** Pursuant to these instructions, the draft guidelines for utilization of the GCA by the ITU have been formulated with the support of Chief Judge (Ret.) Stein Schjolberg (former HLEG Chair), with the involvement of Member States and for consideration and approval by Council[[4]](#footnote-4). In parallel, the Secretary-General has prepared this report explaining how the ITU is currently utilizing the GCA for Council’s consideration.

**2. Background**

**2.1** A fundamental role of ITU, based on the guidance of the World Summit on the Information Society (WSIS) and the ITU Plenipotentiary Conference, is to build confidence and security in the use of Information and Communication Technologies (ICTs).

**2.2** At WSIS, Heads of States and world leaders entrusted ITU to be the facilitator of Action Line C5, "*Building confidence and security in the use of ICTs*", in response to which ITU launched the GCA in 2007 as a framework for international cooperation in this area.

**2.3** The GCA was launched in 2007 - designed for cooperation and efficiency, encouraging collaboration with and between all stakeholders.It comprises of five Pillars or Work Areas: legal measures; technical and procedural measures; organizational structures; capacity building, and international cooperation.

**2.4** Subsequently, the GCA HLEG was established in October 2007 to assist the ITU Secretary-General in developing strategic proposals for Member States on promoting cybersecurity, chaired by Chief Judge (Ret.) Stein Schjolberg.

**2.5** The HLEG comprised of an independent multi-stakeholder global expert group of almost 100 individuals from around the world. The Group delivered their advices to the Secretary-General on all the five Pillars in a Chairman’s Report on August 2008 (HLEG Report 2008).[[5]](#footnote-5)

**2.6** In 2008, the work on the Pillars of the GCA was a major innovation in the global approach related to cybersecurity issues. More than ten years have passed since the HLEG Report 2008 was submitted. Overall, there has been a global recognition of ICTs as a vital tool in achieving the UN Sustainable Development Goals (SDGs), and of the fact that, for ICTs to realize this role, it is important that everyone everywhere has trust and confidence in the use of ICTs. The objective of “*Building Confidence and Security in the Use of ICTs*” is therefore, more than ever, an essential goal to achieve the SDGs.

**2.7** The framework offered by the five Pillars of the GCA has been widely appreciated by ITU membership and has generally withstood the test of time and continues to offer a broad framework for international cooperation on cybersecurity, within the framework of the WSIS outcome documents, especially the principles outlined under Action Line C5. All ITU activities in this area continue to be structured around the five GCA pillars.

**2.8** Since the launch of the GCA, ITU has consistently reported to Council on its activities on building confidence and security in the use of ICTs through an annual report that is organized around the five Pillars, which show the complementary nature of existing ITU work programmes and facilitates the implementation of BDT, TSB, and BR activities in this domain.

**2.9** Detailed information on these activities is available in [C08/33](https://www.itu.int/md/S08-CL-C-0033/en), [C09/50](https://www.itu.int/md/S09-CL-C-0050/en), [C10/12](https://www.itu.int/md/S10-CL-C-0012/en), [C11/54](https://www.itu.int/md/S11-CL-C-0054/en), [C12/29](https://www.itu.int/md/S12-CL-C-0029/en), [C13/23](https://www.itu.int/md/S13-CL-C-0023/en), [C14/23](https://www.itu.int/md/S14-CL-C-0023/en), [C15/18](https://www.itu.int/md/S15-CL-C-0018/en), [C16/18](https://www.itu.int/md/S16-CL-C-0018/en), [C17/18](https://www.itu.int/md/S17-CL-C-0018/en), [C18/18](https://www.itu.int/md/S18-CL-C-0018/en), [C19/18](https://www.itu.int/md/S19-CL-C-0018/en) and [C20/18](https://www.itu.int/md/S20-CL-C-0018/en). The following sections contain some examples of ITU activities under the GCA framework.

**3. Some examples of ITU’s Activities**

**3.1** As the facilitator for Action Line C5, ITU leverages the GCA framework to bring different stakeholders together to help countries address the risks associated with ICTs and works closely in partnership with other organizations, across its sectors and activities, to build trust and confidence in the use of ICTs.

**3.2** While recognizing the mutual inter-dependence of the five Pillars, examples of ITU’s activities on each of the Pillars are highlighted in the sections below. These are intended to offer snapshots of some of the activities, with greater details available in the individual annual reports submitted to Council since 2008 (see para 2.9 above).

**3.3** A separate section has been included on the [Child Online Protection initiative](https://www.itu.int/en/cop/Pages/default.aspx)  as an example of a cross-cutting initiative that spans all the five GCA pillars.

**3.4** **GCA Pillar 1: Legal Measures**

a. An integral component of any national cybersecurity strategy is the adoption of appropriate legislation against the misuse of ICTs for criminal purposes and harmonized with regional and international policy and practices.

b. In the area of Legal Measures, ITU collaborates closely with partners such as UNODC and other experts. ITU also continues to assist Member States in understanding the legal aspects of cybersecurity through its [ITU Cybercrime Legislation Resources](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx) which aims to help harmonize their legal frameworks.

**3.5 GCA Pillar 2: Technical and Procedural Measures**

a. [ITU study groups](https://www.itu.int/en/mediacentre/backgrounders/Pages/itu-study-groups.aspx) provide a neutral, global platform for ITU’s membership to come together and work on security-related standardization on a variety of topics: security architectures and frameworks; security of applications of and services for current and emerging technologies such as Distributed Ledger technologies (of which Blockchain is an implementation), Cloud Computing, Big Data, Artificial Intelligence and Machine Learning, Software Defined Networking, 5G, Internet of Things, Intelligent Transport System and Smart Grids; security foundations like PKI, identity management and authentication; and cybersecurity (including cyber threat information exchange .

b. [ITU-T Study Group 17](https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx) is responsible for building confidence and security in the use of ICTs. This includes study of several technologies with regards to cybersecurity. It is the lead study group on security and identity management (IdM), and continues to be instrumental in the study and standardization of cybersecurity, anti-spam, IdM, public key infrastructure (ITU-T X.509 certificates), information security management, ubiquitous sensors networks, telebiometrics, mobile security, virtualization security towards cloud computing security, personally identifiable information protection and security architecture and application security, together with external Standards Developing Organizations. To date, the group has developed more than 200 standards. Among other things, the Study Group is now working on quantum-based security and have developed Recommendations X.1701 specifications of “Quantum Noise Random Number Generator Architecture”.

c. Other study groups, such as SG9, SG13, SG15 and SG20 (IoT) are working on security-related standards as well.

d. Security and trust have also formed an integral component of the discussions in many of the current and previous [ITU-T Focus Groups](https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx), including (1) The [*ITU-T Focus Group on Machine Learning for Future Networks including 5G (FG ML5G)*](https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx)  (2) [*ITU-T Focus Group on Technologies for Network 2030 (FG NET-2030)*](https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx) (3) [*ITU-T Focus Group on Artificial Intelligence for Health (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h) (4) [*ITU-T Focus Group on Vehicular Multimedia (FG VM*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)*)* (5) [*ITU-T Focus Group on “AI for autonomous and assisted driving”*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx) (FG-AI4AD) (6) [*ITU-T Focus Group on "Quantum Information Technology for Networks" (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx)*.*

e. ITU-R’s work in radiocommunication standardization continues, matching the constant evolution in modern telecommunication networks. ITU-R established clear security principles for IMT (3G, 4G and 5G) networks (Rec. ITU-R M.1078, M.1223, M.1457, M.1645, M.2012 and M.2083). It has also issued Recommendations on security issues in network management architecture for digital satellite systems (Rec. ITU-R S.1250) and performance enhancements of transmission control protocol over satellite networks (Rec. ITU-R S.1711).

**3.6 GCA Pillar 3: Organizational Structures**

a. Effective mechanisms and institutional structures at the national level are necessary to reliably deal with cyber threats and incidents. The absence of such institutions and lack of national capacities poses a genuine problem in adequately and effectively responding to cyber attacks. National Computer Incident Response Teams (CIRT) play an important role in the solution.

b. ITU is working with Member States to build capacity at national and regional levels, deploy capabilities, and assist in establishing and enhancing National CIRTs. ​ITU has conducted technical assessments to evaluate the preparedness for the establishment of CIRTs in 76 countries and is engaging in 20 CIRT establishment projects**,** 14 of them successfully concluded with that national capability fully operational. More are ongoing or planned.

c. ITU has been conducting regular regional and national exercises of [Cyber Drills](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) to enhance countries’ ability to respond to threats, thereby strengthening national and international cooperation among ITU Member States against cyber-threats and cyber-attacks. So far, ITU has conducted 28 Cyber Drills involving more than 100 countries.

**3.7 GCA Pillar 4: Capacity Building**

a. ITU has organized [regional cybersecurity forums](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) for all ITU regions in order to build capacity for different BDT programmes/activities and provide an operational platform for regional and international cooperation.

b. ITU assists Member States in developing and improving effective national cybersecurity strategies. The [Guide to Developing a National Cybersecurity Strategy](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf) (NCS), developed through a multi-stakeholder collaborative process, constitutes a good practice guide and functional toolkit that has been used by countries in all regions to develop and improve their cybersecurity strategies. Since its launch in September 2018, national and regional workshops have been organized in over twenty countries, with three receiving direct assistance to develop and revise national cybersecurity strategies using the Guide.

c. ITU has launched the [Global Cybersecurity Index](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) which is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue.   Each country’s level of development or engagement is assessed along the five Pillars of the GCA, which [​](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)provides the general foundation and framework for the initiative. Based on a multi‐stakeholder approach and initiative, the GCI leverages the capacity and expertise of different organizations, with the objectives of improving the quality of the survey, fostering international cooperation, and promoting knowledge exchange on this topic. The fourth version of the Global Cybersecurity Index survey is currently underway.

**3.8 GCA Pillar 5: International Cooperation**

a. The GCA is based on international cooperation and strives to engage all relevant stakeholders in a concerted effort to build confidence and security in the use of ICTs.

b. ITU continues to develop and maintain relationships and [partnerships](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) with various regional/international organizations and initiatives, including e.g. the World Economic Forum (WEF), Commonwealth Cybercrime Initiative, ENISA, INTERPOL, ECOWAS, the World Bank, UNODC, FIRST, and regional CSIRT/CERT associations, such as AP CERT, AFRICA CERT, and OIC CERT. These partnerships facilitate multi-stakeholder collaboration on activities that cut across all the Pillars of the GCA.

c. As the facilitator for WSIS Action Line C5, ITU leverages the WSIS Process, including the annual WSIS Forum, to help facilitate multi-stakeholder dialogue. ITU organizes High Level Dialogues, C5 facilitators meetings and targeted workshops on the topic of cybersecurity at the [WSIS Forum](https://www.itu.int/net4/wsis/forum/2019/) every year.

d. Recognizing the importance of working towards building a shared understanding within the UN on the needs and requirements for properly establishing programs and initiatives that would effectively support the efforts undertaken by all stakeholders, a significant first step was taken in 2010 towards enhanced internal coordination among UN agencies in their assistance to Member States with regard to cybersecurity. Upon the request of the UN Chief Executives Board for Coordination (CEB), ITU and UNODC, in collaboration with 33 other UN agencies, led a two-year effort to develop an UN-wide framework on Cybersecurity and Cybercrime, which was endorsed by the CEB in November 2013. Since then ITU has continued to contribute to various related initiatives that are targeted at improving internal coordination and cooperation within the UN system.

**3.9 Child Online Protection Initiative**

a. ITU launched the [Child Online Protection (COP)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) Initiative in November 2008 as a multi-stakeholder effort within the GCA framework. The initiative brings together partners from all sectors of the global community to develop cybersecurity strategies and promote safe online environments for children around the world.

b. The key objectives of COP are to (a) ​identify risks and vulnerabilities to children in cyberspace; (b) create awareness; (c) develop practical tools to help minimize risks; and (d) share knowledge and experience.

c. COP takes a holistic approach to promoting child online safety, developing strategies that span the five Pillars of the GCA:

* **Legal Measures**: ​A comprehensive framework of law is an essential tool for promoting a supportive and safer online environment for children and young people. COP tracks approaches taken in different countries with varying legal systems and produces guidelines designed to help Member States achieve their goals.
* **Technical and Procedural Measures**: COP develops key recommendations and standards to support the protection of children online by all key stakeholders.
* **Organizational Structures**: ​COP promotes a model national framework to assist in the development of a positive online environment for children and young people. COP encourages the creation of COP Units at the national level and is developing a series of indicators to assist with the measurement of progress in implementing online child protection initiatives at global, regional, and national levels.
* **Capacity Building**: COP supports countries in the implementation of COP National Frameworks and organizes strategic events at the regional and global level to support these processes.
* **International Cooperation**: COP promotes a global culture of digital citizenship and encourages the establishment of cooperative arrangements for sharing information in order to eliminate or mitigate risks to children and young people online.

d. A variety of activities have been undertaken under the various GCA Pillars, details of which are available on the [COP website](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) as well as in the annual reports to Council since the launch of the initiative. These include the development of tools and resources such as g​​uidelines for children, parents & educators, industry and policy makers. A multi-stakeholder expert working group, consisting of more than 50 organisations and individual experts, are currently reviewing the [Child Online Protection Guidelines](https://www.itu.int/en/cop/Pages/guidelines.aspx), which were first issued in 2009.

1. Minutes of the Plenipotentiary Seventeenth Plenary Meeting, Dubai, Thursday 15 November 2018 [↑](#footnote-ref-1)
2. Transmission of the Report from the former Chairman of GCA High-Level Experts Group (C19/58), ITU, 8 May 2019, <https://www.itu.int/md/S19-CL-C-0058/en> [↑](#footnote-ref-2)
3. Summary record of the sixth Plenary meeting (C19/117), ITU, 20 June 2019, <https://www.itu.int/md/S19-CL-C-0117/en> [↑](#footnote-ref-3)
4. Posted online for Open Consultation with WSIS Stakeholders. Available at: <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx> [↑](#footnote-ref-4)
5. See Judge Stein Schjolberg: Report from the Chairman of HLEG: <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> [↑](#footnote-ref-5)