INFORMATION DOCUMENT FOR GUIDELINES FOR UTILIZATION OF THE GLOBAL CYBERSECURITY AGENDA

Contents

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 draft Guidelines (Open Consultation). Over 160 participants attended the meetings and provided feedback section by section on the draft 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 (Draft 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 C21/VCC-1 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 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] 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

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

(a) the Guidelines for utilization of the GCA (C22/32) developed for consideration and approval of Council 2022; and

(b) this Information Document presenting the background, evolving landscape and context for development of these Guidelines.

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. Council 2022 approved these documents for transmission to the 2022 ITU Plenipotentiary Conference.

Background

1.6 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).

1.7 At WSIS, Heads of States and world leaders entrusted ITU to be the Facilitator of Action Line C5 in 2005, "*Building confidence and security in the use of ICTs*",[4] in response to which ITU launched the GCA in 2007 as a framework for international cooperation in this area.

1.8 The GCA is comprised of five Pillars or Work Areas: legal measures; technical and procedural measures; organizational structures; capacity building, and international cooperation. It is designed for multi-stakeholder cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts.

1.9 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. It was chaired by Judge Stein Schjolberg, Chief Judge (Ret.).

1.10 The HLEG comprised of an independent global multi-stakeholder expert group of almost 100 individuals from around the world. The Group delivered their advice to the Secretary-General on all the five Pillars in a Report from the Chairman in August 2008 (HLEG Report 2008).[5] In the Report, the Chairman of the HLEG emphasized that:

> *The costs associated with cyberattacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages. The future growth and potential of the online information society are in danger from growing cyberthreats. Furthermore, cyberspace is borderless: cyberattacks can inflict immeasurable damage in different countries in a matter of minutes. Cyberthreats are a global problem and they need a global solution, involving all stakeholders.*

1.11 In 2008, the work on the five Pillars of the GCA was a major innovation in the global approach related to cybersecurity issues. Over a decade has 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.

---

[4] WSIS Outcome Documents, 2005, available at https://www.itu.int/net/wsis/outcome/booklet.pdf

[5] Judge Stein Schjolberg: Report from the Chairman of HLEG, 2008, available at https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Context

1.12 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. It continues to offer a broad framework for international cooperation on cybersecurity within the framework of the WSIS outcome documents, particularly the principles outlined under Action Line C5. The related recommendations included in the HLEG Report 2008 continue to be relevant today[6], except for a few specific aspects that could be considered dated or have been superseded by other events.

1.13 The ICT landscape has, of course, changed drastically since 2008, with ICTs now underpinning every sector of society, and the bulk of critical infrastructure[7]. The world is witnessing the emergence and adoption of new technologies at a rapid pace, examples of which include:

- the wider adoption of the Internet of Things with tens, if not hundreds, of billions of new interconnected devices which opens up a significant number of new potential vulnerabilities;
- the growth of Artificial Intelligence as a tool to leverage data, especially Big Data, that allows humans to make more informed decisions as well as enables machines to make autonomous and so-called intelligent decisions without human intervention, bringing up challenges of security and trust as well as safeguarding human rights;
- new communication technologies and standards, such as 5G, that allow communication at a speed exponentially greater than what is currently feasible;
- quantum computing that offers computing speeds way beyond current capabilities, offering great opportunities but also putting at risk, *inter alia,* current cryptographic algorithms; and
- new security technologies, such as Distributed Ledger Technologies (blockchains being a popular implementation), that offer significantly better means of safeguarding systems and associated data. More and more countries around the world are also now increasingly moving towards adoption of digital identity systems.

1.14 Additionally, the global ICT ecosystem has also been significantly shaped since 2008 with the global wide-scale adoption of social networks. Some social networks have more users than the population of many countries combined - e.g. as of 2020 Facebook has nearly 2.8 billion monthly active users[8]. Social media has played a pivotal role in connecting people across the world, blurring geographical boundaries, and providing easy access to information and opportunities at a scale and speed that did not exist earlier. It has also brought forth significant trust concerns - regarding privacy and security of users and the data they generate, authenticity and trustworthiness of the information available on social networks, dissemination of hateful content etc.[9]

---

[6] The recommendations in the HLEG Report 2008 are presented with an annotated summary of the views and discussions during the meeting relating to each Recommendation. Although HLEG members did not achieve full consensus on every recommendation most of the HLEG experts were nevertheless in broad agreement on many recommendations.

[7] The Directive of the European Parliament and the Council of European Union of August 12, 2013 on attacks against information systems replaced the Council Framework Decision (2005) has a definition of critical infrastructure as follows: *An asset, system or part thereof located in Member States which is essential for instances for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*.

[8] Number of monthly active Facebook users worldwide as of 4th quarter 2020, available at https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[9] Mark Zuckerberg: *The Internet needs new rules. Let's start in these four areas,* Washington Post, March 30, 2019, available at https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

1.15 Moreover, other factors, such as the emergence of the dark web, have continued to raise growing concerns worldwide about criminal activity in cyberspace, particularly on aspects such as access to malicious tools, services and content.

1.16 Given these developments, there has been growing recognition among all stakeholders, including governments, on the diversity of urgent actions that need to be taken to advance cybersecurity, ranging from protection of critical infrastructure to safeguarding user privacy. As an issue that could pose a national security threat to all countries, cybersecurity has reached the agendas of the highest political levels of governments, who are increasingly investing in governance and administrative measures to drive a whole-of-government response for the purpose of strengthening their national cyber resilience.

1.17 The COVID-19 pandemic has only further highlighted the centrality of ICTs to health and safety, and towards keeping our economy and society moving forward. From teleworking and e-commerce to telemedicine and remote learning, ICT services and infrastructure are providing continued access to critical needs. The COVID-19 crisis has also heightened the need to address the rapidly evolving and critical cybersecurity challenges that are posed by society's high degree of dependence on ICTs.

1.18 Within the framework of the GCA, each of the five Pillars has evolved in its own specific way over the past decade.

1.19 As of 2020, more than 125 countries have signed and/or ratified different cybersecurity and cybercrime conventions, declarations, guidelines or agreements such as the Council of Europe Convention on Cybercrime of 2001 (Budapest Convention), the Agreement among the Governments of the Shanghai Cooperation Organization Member States on Cooperation in the Field of Ensuring International Information Security (2009) and the African Union Convention on Cyber Security and Personal Data Protection (2014).

1.20 Pursuant to UNGA Resolutions, a Group of Governmental Experts (GGE)[10] and Open-ended Working Group (OEWG)[11] have studied several issues related to the use of ICTs in the context of international security, including, *inter alia*, advancing responsible state behavior in cyberspace, applicability of international law to cyberspace, capacity building, and the need to implement and further develop confidence-building measures in cyberspace.

1.21 Innovative ICT technologies, such as cloud computing, software-defined networking (SDN), network function virtualization (NFV), 5G, Big Data, AI etc., blur market and geographic boundaries, making the cybersecurity ecosystem increasingly dynamic and complex. New technologies and commercial actors can cause exposure to new vulnerabilities and threats, particularly as the private sector's focus on performance, market share, and costs is often prioritized over investments in security in the design stage. There are a number of issues that pose significant challenges when dealing with such technologies, such as finding a way to reduce and master the number of vulnerabilities by ensuring security by design (as products continue to be vulnerable right from the design phase itself), enhancing confidence in products and services through their lifecycles by accreditation schemes, protocols and standards, and legitimate use of user generated data while protecting user privacy. Standardization and periodic certification/accreditation processes could help reduce the number and impact of vulnerabilities by contributing towards developing a culture of security by design, in turn building trust and confidence in such technologies. However, security standardization, i.e. developing technical and procedural measures for security, remains a moving target because this necessitates tech-advanced industry, tech-savvy regulators and capable enforcement bodies, where applicable.

1.22 A number of national, regional and international organizations have been set up to tackle the issue of cybersecurity. Some examples of national and regional initiatives include AFRIPOL, AMERIPOL, GCCPOL, Oceania Cyber Security Centre (OCSC), Australian Cyber Security Centre (ACSC), European Cybercrime Center (EC3), Russian National Coordination Center on Computer Incidents, and India's Cybercrime Coordination

---

[10] Group of Governmental Experts, available at https://www.un.org/disarmament/group-of-governmental-experts/.

[11] Open-ended Working Group, available at https://www.un.org/disarmament/open-ended-working-group/

Centre (I4C). In terms of international entities, recent efforts include the Global Cyber Security Capacity Centre (GCSCC), the Global Forum on Cyber Expertise (GFCE), the INTERPOL Global Complex for Innovation (IGCI), WEF Global Centre for Cybersecurity, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS), Economic Community of West African States (ECOWAS), Southern African Development Community (SADC) and others.

1.23 Further, lack of skill and expertise in technical, legal, organisational and human dimensions of cybersecurity can also adversely affect vital national infrastructures. It is likely that many ICT end-users currently either may not fully understand cybersecurity issues or have the necessary skills or tools to best protect their data, privacy, and assets, with the more vulnerable users, including women and children, being particularly at risk. To build skills, competences, and measures that will contribute to achieving an effective cybersecurity culture remains a crucial challenge.

Continued Relevance and Applicability of the GCA as a Global Framework for Action

1.24 Activities implemented utilizing the GCA framework have been evolving, taking into account the changing ICT landscape, including those undertaken by ITU within its mandate and pursuant to its role as the facilitator for WSIS Action Line C5.

1.25 The GCA has well served ITU's efforts in building confidence and security in the use of ICTs. As a framework, it is applicable across the global, regional and national levels, and should continue to be implemented as such. Within its mandate, guided by the GCA framework, ITU has been working to bring different stakeholders together to collaborate on a number of initiatives, including assisting Member States with: defining their national cybersecurity strategy, fortifying their infrastructure by developing and implementing international security standards, setting up computer incident response teams, deploying initiatives to protect children online, and building the necessary human capacity and skills. Various multi-stakeholder initiatives, such as the one on Child Online Protection, have been launched under the GCA framework.[12]

1.26 While recognizing the mutual inter-dependence of the five Pillars, each of the sections below addresses a specific GCA pillar and provides some background and context to present an overview of the evolution of the landscape in this respect.

Section 2 Pillar 1: Legal Measures

Introduction

2.1 The legal dimension of cybersecurity is one of the key factors for facilitating trust in the use of ICTs.

2.2 The HLEG Report 2008 stated that Pillar 1 of the GCA sought to promote cooperation and provide strategic advice to the ITU Secretary-General on legislative responses to address evolving legal issues in cybersecurity, including how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner. The discussions noted that ITU could elaborate strategies for the development of model cybercrime legislation as guidelines. The Report also recommended relevant regional initiatives as references.

---

[12] For more information, please refer to the following:

- ITU's annual activities report to the ITU Council on building confidence and security in the use of ICTs, available at https://www.itu.int/en/council/2021/Pages/default.aspx
- The report to Council 2021 on ITU's utilization of the GCA, available at https://www.itu.int/md/S21-CL-C-0036/en.

Evolution of the Legal Landscape since 2008

2.3 Regional organizations have developed numerous conventions, declarations, agreements, and guidelines after 2008 on cybersecurity. As mentioned above, many countries have signed and/or ratified different cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, which has resulted in fragmentation and diversity at the international level.

2.4 Within the UN system, as mentioned previously in Section 1, the UN General Assembly also established two processes to discuss the issue of security in the use of ICTs - the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG). Since 2004, the UN General Assembly has established six GGEs to study the threats posed by the use of ICTs in the context of international security and how these threats should be addressed, with the latest being the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 2019/2021 (Resolution 73/266). In its findings, the 2014/2015 GGE agreed that existing obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms. In 2018, the OEWG on developments in the field of information and telecommunications in the context of international security was established (Resolution 73/27), involving 'all interested States', to discuss existing and potential threats in the sphere of information security and possible cooperative measures to address them; further development of rules, norms and principles of responsible behaviour of States; how international law applies to the use of ICTs by States; confidence-building measures; capacity-building; and the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations. The 2019-2021 OEWG adopted its Final Substantive Report by consensus in March 2021, which reaffirmed that international law, and in particular the Charter of the UN, is applicable in cyberspace and further recommended that States support capacity building efforts in the area of international law, national legislation, and policy because this will enable all States to contribute to building common understandings of how international law applies to the use of ICTs by States. The OEWG is expected to continue its work as Resolution 75/240 established an Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025.

2.5 There have also been several initiatives and processes initiated within the UN system to help identify and address the legal challenges posed by cybersecurity globally. For instance, a number of UN General Assembly resolutions have been passed in this regard, such as the United Nations General Assembly Resolution of 27 December 2019 on *Countering the use of information and communications technologies for criminal purposes* (Resolution 74/247) which decided to establish an open-ended ad hoc intergovernmental committee of experts, representing all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

2.6 In light of the above, there is an ongoing discussion among States in these various forums that further cooperation is needed between them and with other stakeholders to search for a global common ground on understanding, interpreting and upholding international law in the context of cyberspace, in particular by facilitating greater exchange of information and best practices.

Legal Measures and New Technologies

2.7 Some experts have suggested that new technology and methods of conducts in cyberspace with criminal intent should be covered by criminal law.[13] Many countries have adopted or are preparing for new laws covering some of those conducts. It is important that any appropriate legal measures developed in this regard are designed in accordance with their human rights obligations. Some examples of recent and emerging technologies and trends which could potentially impact legal measures are set out below:

[13] Stein Schjolberg, The History of Cybercrime (3rd Edition, February 2020)

a. Global Cyberattacks

Global cyberattacks against critical communications and information infrastructures have emerged as an international and national security threat. Governments, international organizations, and private institutions have all been targets of such global cyberattacks necessitating the development of robust national legal frameworks to address this challenge.

b. Criminal Conducts on Social Networks

There are calls for measures for countering illegal conduct, such as hate speech, in social networks. New initiatives have emerged – such as the Global Internet Forum to Counter Terrorism partnership between the UN and technology companies Facebook, Microsoft, Twitter, and YouTube – to address such issues.

c. Internet of Things (IoT)

Smart technology is changing the way that the global population lives, interacts, and works.[14] There have been multiple recent instances of web infrastructure across the world being attacked by a botnet of hacked connected devices, ranging from webcams to routers. With the advent of new technologies such as 5G, and ubiquitous interconnected devices having become a reality, there are likely to be increased risks.

d. Artificial Intelligence (AI)

Algorithmic transparency, including traceability of actions undertaken, is a very important factor in establishing accountability and liability for decisions made by partially or fully automated systems, and thereby ensuring trust in ICT applications and services. Experts have noted that for several types of AI techniques, such as deep learning, it is difficult to clarify how outcomes are reached. As automated decision-making processes become more prevalent in consumer and business applications and services, the need for greater clarity on legal aspects concerning accountability and liability for the analyses and decisions these processes deliver will become prominent.[15]

e. Online Child Sexual Abuse and Exploitation

The United Nations Convention on the Rights of the Child (CRC) was adopted in 1989. Article 34 of the Convention obliges State Parties to take appropriate measures to protect children from all forms of sexual exploitation and abuse. In 2002, an Optional Protocol to the CRC on the sale of children, child prostitution and child pornography came into force. Online child sexual abuse has spread with the growth of the Internet and social media. Experts have called for a comprehensive approach towards the prevention of such abuses.[16] These include measures to prevent the development of, and access to, websites that contain content related to child sexual abuse, including blocking, filtering, or such other similar technology. In March 2021, the Committee on the Rights of the Child adopted its general comment No. 25 (2021) on children's rights in relation to the digital environment which explains how States parties should implement the CRC in relation to the digital environment and provides guidance on relevant legislative, policy and other measures.

2.8 Procedural Laws - General Principles

---

[14] The European Union Commission launched a programme called Horizon 2020 for developing the potential of the Internet of Things, and the work programme 2016-2017 for supporting experimentation and innovation. Proposals are invited against several topics, also including: IoT security and privacy. Advanced concepts for end-to-end security in highly distributed, heterogeneous and dynamic IoT environments. Approaches must be holistic and include identification and authentication, data protection, and prevention against cyber-attacks at the device and system levels. They should address relevant security and privacy elements such as confidentiality, user data awareness and control, integrity, resilience, and authorisation (See European Commission Decision C (2015) 6776 of October 13, 2015.)

[15] T. Ballell, *Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact*, Uniform Law Review, Volume 24, Issue 2, June 2019, Pages 302–314, available at https://doi.org/10.1093/ulr/unz018

[16] A model legal framework may be the Directive 2011/92/EU of the European Parliament and of the Council of December 13, 2011, on combating the sexual abuse and sexual exploitation of children and child pornography.

Adopting the procedural laws necessary to establish powers and procedures for the prosecution of criminal conducts in cyberspace has been considered an essential legal measure for the global prevention, investigation, and prosecution of cybercrime and to ensure cybersecurity. However, some experts have noted that such powers and procedures could also be necessary for the prosecution of other criminal offences committed by means of a computer system, and regulations could apply to the collection of evidence in electronic form of all criminal offences.[17] All procedural laws should be consistent with obligations and standards set under international human rights law. In this regard, noting that the principle of state sovereignty applies in cyberspace, there have also been requests and discussions on exploring mechanisms that can potentially facilitate lawful access to the content of communications where end-to-end encryption has been implemented, while ensuring that the fundamental rights and safety of citizens are protected[18]. Some stakeholders have cautioned that any such mechanisms would weaken the security of the Internet and place the global economy, the critical services many depend on, and the lives of citizens at greater risk of harm.

2.9 In light of the above sections, it is clear that countries should continue to take appropriate legal measures to protect their critical communication and information infrastructures (and any related asset, system, or part thereof) that are essential for the maintenance of vital societal functions such as the health, safety, security, economic, or social well-being of people, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

2.10 As recognized earlier, the five GCA Pillars are all mutually inter-dependent, with the one on legal measures cutting across them all.

2.11 Since the launch of the GCA, ITU's focus has been on the areas of cybersecurity that are within its core mandate and expertise, notably the technical and development spheres, and not those related to Member States' application of legal or policy principles related to national defence, national security, content, and cybercrime, which are within their sovereign rights. Therefore, with respect to activities under Pillar 1, ITU has primarily focused on facilitating collaborative action, using mechanisms such as MoUs, with other relevant international organizations and stakeholders (such as INTERPOL and UNODC) who may have a lead mandate in this area to deliver assistance to countries. This has included helping Member States understand the legal aspects of cybersecurity, through resources such as the ITU Cybercrime Legislation Resources and the UNODC Cybercrime Repository. Work was also done to assist Member States in the Caribbean, Sub-Saharan Africa, and Pacific Islands in harmonizing ICT regulations and legislations, including cybercrime legal frameworks.

Section 3 Pillar 2: Technical & Procedural Measures

Introduction

3.1 The GCA has guided the development and implementation of various initiatives, contributing to the maturity of the cybersecurity debate at the international, regional, and national levels. The need for effective and efficient cybersecurity measures, should it be at a strategic or operational level, has to be satisfied within a coherent approach, which continues to be a major challenge.

3.2 Today, it may seem that the dimensions identified by the GCA Pillars 1, 3, 4, and 5 are becoming increasingly important in the field of cyber diplomacy and international dialogue, and often prevail over Pillar 2. However, technical issues can often be at the root of all the other Pillars. Managing cyber risk through technological and procedural (e.g., administrative, operational, or managerial) measures continues to be of prime importance, especially in the context of critical infrastructures. Given the long-standing role played by

---

[17] Judge Stein Schjolberg, 2018 & Judge Stein Schjolberg, 2019, available at https://www.cybercrimelaw.net/Cybercrimelaw.html

[18] For instance, https://www.justice.gov/olp/lawful-access

ITU, as a UN specialized agency and a global Standards Development Organization (SDO), it is well positioned to advance the field of security related standards and technical measures.

Evolution of the Technical & Procedural Measures Landscape Since 2008

3.3 Technologies (current and emerging), and the digital practices that result from them, are constantly evolving. This dynamic technical dimension is somewhat independent of the other GCA Pillars, and largely evolves by itself, taking into limited consideration the needs and implications on the subject matter of the other four Pillars.

3.4 In order for all infrastructure, applications, and services to function, the development and implementation of standards is fundamental. Moreover, it is important that in the development of standards, relevant human rights obligations must also be taken into consideration.

3.5 ITU, with its multi-stakeholder membership, offers a unique global platform to develop global ICT standards for voluntary adoption in ITU Member States. Within ITU, ITU-T SG17 is the lead study group for security standards – having published over 200 standards focused on security. It is currently working on a variety of emerging technology areas, including FinTech security, IoT security (including industrial internet security), Intelligent Transportation System security, Distributed Ledger Technology, Quantum Key Distribution, Machine Learning for Countering Spam, Security of 5G, Edge Computing, Protection of Personally Identifiable Information, multi-party computing, and guidelines for the creation, operation and automation of cyber defence centers, among several others. In implementing the recommendations of the HLEG Report 2008 on "collaboration" (e.g., 2.1, 2.6, 2.7, 2.10, 2.12, 2.16), SG17 collects and maintains an ICT Security Standards Database[19] for public access, which includes 2600 existing and ongoing ICT Security Standards from 13 key SDOs, including 3GPP, ATIS, ETSI, IEEE, IETF, ISO/IEC JTC 1, ITU, OASIS, OneM2M, etc.

3.6 While ITU-T SG17 continues to be the main study group for security standards, most—if not all—other study groups also address security-related aspects within their respective areas of study, e.g. SG20 on IoT and its applications (including smart cities and communities), SG13 on next generation networks, or SG16 on multimedia coding, systems, and application, among others. The various focus groups on emerging technologies, such as AI and Health, Machine Learning and 5G, Digital Ledger Technologies, Quantum Information Technology for Network and others, also address security related challenges. It is important that close cooperation is developed among the various groups, 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 the development cycle of ICT products/services.

The Proliferation of Standardization Initiatives and the Need for Greater Cooperation

3.7 International cybersecurity standardization is challenging due to the range of technologies and emergence of diverse players across sectors, and especially difficult for developing countries that may lack operational cybersecurity capability and technical skills.

3.8 In this regard, Recommendation 2.1 of the HLEG Report 2008 continues to hold true now more than ever: "*With regards to opportunities to enhance collaboration with existing cybersecurity work outside of ITU, the ITU should work with existing external centres of expertise to identify, promote and foster adoption of enhanced security procedures and technical measures*"[20].

3.9 Further, as specified in Recommendation 2.2 of the HLEG Report 2008, ITU is identified as "*the global centre of excellence*"[21] to deal with the international standardization process and standards related to technical and procedural measures. In order to achieve this, more technologically advanced countries, and

---

[19] ITU Standards Landscape, available at https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance

[20] HLEG Report 2008, Para 2.1, Page 9, *id* at 6

[21] HLEG Report 2008, Para 2.2, Page 9, *id at 6*

their private sectors, should be incentivized to participate in ITU activities, and to collaborate to develop technical and procedural standards, including security-related ones.

3.10 It is important to continue to strengthen coordination and collaboration with the other SDOs, on the basis of reciprocity, so that end-to-end security, security by design, risk assessment, and interoperability throughout the lifecycle of the product are ensured.

3.11 The HLEG Report 2008 has highlighted the importance of "*key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards*"[22]. In this regard, ITU should continue to adapt its work, taking into account new technologies and requirements. For each of these technologies/domains, the following requirements should be taken into consideration:

- Need for security by design/security by default in every element and interface in a heterogeneous ICT ecosystem in the design stage;
- Need for appropriate metrics to identify the level of security in the implementation stage; and
- Need for periodical evaluation and certification process(es) to certify the level of security of a dataset/product/system/service throughout its lifecycle after deployment.

Section 4 Pillar 3: Organizational Structures

Introduction

4.1 Organizational structures at the levels of national, regional, and international coordination can be analyzed based on whether the purpose for their cooperation is strategic or operational. In a strategic structure, organizations place a greater emphasis on establishing a collaborative relationship than carrying out joint operations in case of a cyber-incident. On the other hand, in an operational structure, organizations form close information sharing systems to rapidly exchange information to quickly react to cyber incidents. This distinction can be helpful when comparing different organizational structures around the world.

4.2 Effective mechanisms and institutional structures at the national level are necessary to reliably prepare and respond to cyber threats and incidents. The absence of such institutions and the lack of national capacities pose challenges in adequately and effectively responding to cyber-attacks. National Computer Incident Response Teams (CIRTs) play a vital role in improving preparedness and resilience on the national level.

Evolution of the Organizational Structures Landscape Since 2008

4.3 There has been significant progress in the last decade in terms of Pillar 3. Numerous national, regional and international organizations have been set up to tackle the issue of cybersecurity.

4.4 Examples of national and regional initiatives include AFRIPOL, AMERIPOL, GCCPOL, Oceania Cyber Security Centre (OCSC), Australian Cyber Security Centre (ACSC), European Cybercrime Center (EC3), India's Cybercrime Coordination Centre (I4C) and the Cybercrime Reporting Portal, Japan's National Center of Incident Readiness and Strategy for Cybersecurity and Cybercrime Control Center (JC3), Malaysia's National Cyber Security Agency (NACSA), France's National Cybersecurity Agency of France (ANSSI), Lithuania's National Cyber Security Centre (NCSC), National Cyber security Centre for Switzerland, the UK's National Cyber Security Centre (NCSC), United States' International Cyber Crime Coordination Cell (IC4), Russian National Coordination Center on Computer Incidents, as well as Collective Security Treaty Organization Consultative Coordinating Center for Computer Incident Response (CCC CSTO), OAS' Inter-American Committee against Terrorism (CICTE) and Cyber Security Program, Saudi Arabia's National Cybersecurity Authority (NCA) and Rwanda's National Cybersecurity Authority.

---

[22] HLEG Report 2008, Para 2, Page 9, *id* at 6

4.5 Despite the growing investment in CIRTs by Member States, and the independent regional and international outreach of national CIRTs, there are still 85 countries without a national CIRT – a situation of significant concern given the global nature of cyber threats.[23]

4.6 ITU, through its development bureau, is working with Member States, partners, and regional/international organizations to build capacity at national and regional levels, deploy capabilities, and assist in establishing and enhancing national CIRTs. To date more than 80 CIRT readiness assessments have been conducted by ITU to help countries assess their national cybersecurity preparedness and incident response capabilities.[24] ITU has provided support for the establishment/enhancement of 22 national CIRTs projects for respective ITU Member States.[25] To carry out these assessments of countries, ITU collaborates with partners such as the Forum for Incident Response and Security Team (FIRST), the Global Cyber Security Capacity Centre and others.

4.7 In terms of international organizations, there have been several initiatives, some examples of which are listed here:

- The Global Cyber Security Capacity Centre (GCSCC) is an international centre for research on efficient and effective cybersecurity capacity-building, and collaborated with the ITU in developing the Guide to developing a National Cybersecurity Strategy (NCS), which is currently being used to provide hands-on exercises on NCSs, as well as training on good practices for countries on developing an effective national cybersecurity strategy framework.
- The Global Forum on Cyber Expertise (GFCE), established in 2015, aims to exchange good practices and provide expertise on cyber capacity building for countries, international organizations, and the private sector. GFCE and ITU are co-initiators of the CSIRT Maturity initiative, and have collaborated on cybersecurity activities such as the "Combatting Cybercrime Toolkit".
- The INTERPOL Global Complex for Innovation (IGCI), inaugurated in 2015 in Singapore, provides national law enforcement with specialized operational support and training in response to the changing face of crime. In 2018, ITU and INTERPOL signed a cooperation agreement to establish a formal framework for INTERPOL and ITU to cooperate for their mutual benefit and within the scope of their respective mandates and resources, in building confidence and security in the use of ICTs.
- The WEF launched a new Global Centre for Cybersecurity in 2018 with the aim of establishing a global platform for governments, businesses, experts, and law enforcement agencies to collaborate on cybersecurity challenges. In the same year, ITU and the WEF agreed to cooperate in the promotion of cybersecurity projects and initiatives aiming to mitigate cyber threats, and also to explore further opportunities to cooperate in promoting cybersecurity.

Section 5 Pillar 4: Capacity Building

Introduction

5.1 The development and deployment of appropriate skills, of a cybersecurity culture, and good practices among all stakeholders is a crucial issue.

5.2 All countries and all organizations are faced with the need to have sufficient and necessary human resources and skills to:

---

[23] National CIRTs, ITU, available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[24] *Ibid*

[25] *Ibid*

- Implement strategic and operational cybersecurity measures;
- To perform National Cybersecurity Risk Assessments;
- Manage crises related to the occurrence of cybersecurity incidents;
- Strengthen the robustness and resilience of digital infrastructures and services; and
- Develop consistent processes, skills and practices.

5.3 It is important to note also that, given the rapid advancements in ICTs and the already existing issues of access and connectivity, end users—and in particular populations such as women, children, older persons, persons with disabilities and specific needs—can often be more vulnerable to cybersecurity threats and incidents. Cybersecurity related education programmes, in addition to raising awareness about cyber security threats relevant to vulnerable end users could therefore be key to decreasing cybersecurity risks for society as a whole.

Evolution of the Capacity Building Landscape Since 2008

5.4 As cybersecurity has a global dimension and deals with a large range of issues—such as ICT uses or misuses, technical measures, economic, legal, and political issues—it is important to develop a global cybersecurity culture to enhance the level of understanding of each actor in the cybersecurity chain. When developing a culture of cybersecurity, one of the main challenges is to correctly identify what the global and international issues are and what the specific local needs are because cultures mainly rely on local and temporal factors. International technical standards can contribute to identifying the key global and generic issues related to the technical and procedural dimension of a cybersecurity culture.

5.5 A collective response to protect digital infrastructures is important. This is increasingly urgent as technological change is moving towards greater and permanent interconnectivity via ICTs[26]. Everything that can be connected could be compromised. Moreover, the miniaturization of components due to nano-technologies, including various types of intelligent and autonomous chips, has led to these chips being integrated into technologies that touch on all of our activities.

5.6 The GCA has served as an innovative and efficient interdisciplinary framework for capacity building efforts from which global, schedulable, and specific answers can continue to be developed by relevant players in order to be collaborate effectively. The GCA framework is well established to support the challenge of building an inclusive and secure information society.

5.7 The recommendations made in this regard by the HLEG Report 2008 continue to remain relevant today. Taking into account the work done by ITU, in particular since the first publication of "The Cybersecurity Guide for Developing Countries" in 2006, and based on the GCA framework and the HLEG Report 2008, extensive work has taken place across Member States on capacity building - including training, awareness, and education activities at the national, regional, and international level.

5.8 Utilizing the GCA framework, ITU continues to assist countries, particularly with building necessary human capacity and skills, defining their national cybersecurity strategies, helping develop skills to manage computer incident response teams (CIRTs), and developing resources to protect children online.

5.9 For instance, in terms of awareness raising, it is important to recognize the contribution of the Global Cybersecurity Index (GCI). From its first launch in 2015, the GCI - which measures the commitment of Member States to Cybersecurity - has had three successful publications as a result of strong demands from Member States, the private sector, academia, and others. Through its dedication in raising awareness, the GCI continues to provide support to Member States to improve their cybersecurity posture through sharing of

---

[26] Tim Berners-Lee, *30 years on, what's next #ForTheWeb?*, March 12, 2019, (available at https://webfoundation.org/2019/03/web-birthday-30/) at the 30th anniversary of the Web, in an open letter, stated that *while the web has created opportunity, given marginalised groups a voice, and made our daily lives easier, it has also created opportunity for scammers, given a voice to those who spread hatred, and made all kinds of crime easier to commit.*

good practices for effective cybersecurity implementations. The GCI has proven to be an invaluable tool in awareness and capacity building and should continue to be leveraged and strengthened.

5.10 Specific actions should be taken at a national level to build or improve cybersecurity capacities of various stakeholders in order to be able to address national and international cybersecurity issues. As capacity building activities primarily occur at the national level, appropriate resources should be allocated to national actors.[27]

5.11 Further, from a global perspective, empowering human resources requires a general, modular, and flexible cybersecurity educational framework to respond to the needs of increased public awareness, and to provide a tailored educational curricula for specific professionals. Particular attention should be paid to the gender gap in this area. There is a lot of untapped human capital that can be brought to contribute to the cybersecurity field, including women who still represent only 20% of the cybersecurity workforce.[28]

5.12 The quality of formal education at a school or university level and general public awareness raising depends to a certain extent on the quality, maturity, and relevance of research.

5.13 In addition, it is important that attention is paid to building capacity for the Micro, Small, and Medium Enterprises (MSMEs) that are now one of the key players in the growing digital economy by enabling them to identify and manage cyber risks and employ ICT assets to (including broadband and the Internet) in a secure and sustainable way.

Section 6 Pillar 5: International Cooperation

Introduction

6.1 It is clear from the past decade that no single entity or organization alone can address the whole range of current and emerging cybersecurity challenges. These challenges can be addressed through partnerships involving close collaboration and coordination among all stakeholders in order to help build a universally available, open, secure, and trustworthy ICT ecosystem.

6.2 Pillar 5 on International Cooperation therefore is a cross-cutting pillar of the GCA – forming the foundation of every aspect of building trust, confidence, and security in the use of ICTs. In the HLEG Report 2008, this Pillar sought to develop a strategy for international cooperation, dialogue, and coordination in dealing with cyber threats.

Evolution of the International Cooperation Landscape Since 2008

Global High-level Dialogues

6.3 Discussions on various aspects of cybersecurity—including technical aspects, cybercrime, privacy, data protection, and others—are spread across many forums and processes. Some of these have been hosted by various UN agencies, including the ITU or other international organizations, and others have been initiated by other stakeholders as well as various other international and regional forums.

6.4 While all the forums and processes are doing a good job of raising awareness and improving understanding, it is important to identify synergies among these various efforts so that the international community can come together and find solutions.

6.5 The United Nations platform, with its significant convening capacity, is well positioned to foster cooperation, dialogues, and coordination at the international level among stakeholders from all nations on addressing challenges related to cyberspace. As highlighted in the HLEG Report 2008, ITU, considering its

---

[27] S. Ghernaouti, *Cyberpower, Crime, Conflict and Security in Cyberspace,* EPFL Press 2013

[28] Laurence Bradford, *Cybersecurity needs women: Here's why*, 18 October 2018, available at https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#5a7a3cc447e8

position in the UN system as the specialized agency for ICTs, can continue to play an important role, within its mandate, in related fields of developments.

6.6 While a "Global Conference" was suggested in Recommendation 1.15 of the HLEG Report 2008[29], current conferences, forums, and processes that have emerged from the WSIS process and strengthened subsequently—the WSIS Forum for development matters and the IGF for governance matters—could also be better leveraged for the same. The WSIS Forum, the largest annual gathering of the ICT4D community, offers several mechanisms to bring together the global community to discuss and identify concrete solutions for the development challenges concerning building confidence and security in the use of ICTs (Action Line C5), including, among others, the Action Line Facilitator's track, High Level Dialogues, and targeted stakeholder sessions.

6.7 An important development in the past decade has been the recognition of the critical importance of cybersecurity at the highest political levels of national governments. This is reflected in the adoption, by many countries, of a strategy for digital transformation that adopts a whole-of-government approach and creates cross-sectoral central coordination mechanisms that usually report directly to Heads of States or governments.

6.8 Another related development has been the significant number of bilateral discussions taking place among technologically advanced countries and regions.

International Multi-stakeholder Partnerships

6.9 ITU has had various successes in fostering international cooperation through its role as sole facilitator of WSIS Action Line C5.

6.10 ITU has forged a range of multi-stakeholder partnerships, be it through:

- Formal mechanisms such as MoUs or similar arrangements (e.g. with FIRST, Interpol, UNODC, WEF, and others);
- Initiatives such as Child Online Protection, in partnership[30] with more than 80 entities from all stakeholder groups; or
- Mechanisms such as Focus Groups e.g. the FGs on Digital Ledger Technologies, Quantum Technologies, AI and Health, etc., which provide a platform for all stakeholders to discuss trust and confidence issues in emerging technologies.

6.11 Significantly expanding its multi-stakeholder membership in the past decade, especially the range of private sector companies and academic institutions, ITU benefits from a wide membership of 193 Member States and nearly 900 private sector companies, universities, and international and regional organizations, thereby reflecting the rapidly changing nature of today's digital society.

Better Coordination within the UN System

6.12 As mentioned previously in paras 2.4 and 2.5 of this document, there are a number of UN processes that have been established by the UN General Assembly to help address the challenges of ensuring international security in cyberspace. These include the work of the GGE and the OWEG. The 2019-2021 OWEG's Final Substantive Report, has concluded, *inter alia,* that future regular institutional dialogue should not duplicate existing UN mandates, efforts and activities focusing on the digital dimensions of other issues, and that any future mechanism for regular institutional dialogue under the auspices of the United Nations should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results based. Taking this into consideration, it is important that

---

[29] HLEG Report 2008, Para 1.15, Page 9, *id* at 6

[30] More information is available at https://www.itu.int/en/cop/Pages/partners.aspx

ITU's work should be complementary to the work streams that are currently ongoing within the UN system in this regard, in particular the abovementioned UNGA processes.

6.13 The complex articulation of the mandate of the UN system can sometimes impede a pragmatic and effective harmonized approach. It is therefore imperative for the UN family to continue working towards harmonizing its efforts, including streamlining programs and activities on cybersecurity in order to be more effective.

6.14 It is therefore important to work 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 governments, industry, and all other relevant stakeholders.

6.15 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. 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 UN Chief Executives Board for Coordination (CEB) in November 2013.

6.16 While it was a key step, further systemic changes are needed in order to ensure effective coordination. The prioritization of Digital Cooperation by the UN Secretary-General[31] offers an opportunity to address the need for the UN family as a whole to continue improving internal coordination and cooperation by utilizing various interagency mechanisms, including the CEB.

_____

[31] More information is available at https://www.un.org/en/digital-cooperation-panel/