DRAFT 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 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]

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 Global Cybersecurity Agenda.[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]

1.4 Pursuant to these instructions, these 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) and the involvement of Member States, for consideration and approval by Council[4]. 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.

Background

1.5 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).

1.6 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*",[5] in response to which ITU launched the GCA in 2007 as a framework for international cooperation in this area.

---

[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

[4] For more information on the process, and for inputs received from Member States, please visit: https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx

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

1.7 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.

1.8 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.).

1.9 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 on August 2008 (HLEG Report 2008).[6] The Chairman of the HLEG, while submitting this Report of the Group, 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.*

1.10 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.

Context

1.11 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, except for a few specific aspects that could be considered dated or have been superseded by other events.

1.12 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;

---

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

[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*.

- 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 user privacy, security and trust, algorithms, and tools;
- 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.

1.13 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. Facebook has more than 2.5 billion monthly active users (December 2019)[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]

1.14 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.

1.15 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.

1.16 The COVID-19 pandemic in 2020 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.

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

1.18 As of 2019, more than 125 countries have signed and/or ratified different cybersecurity and cybercrime conventions, declarations, guidelines or agreements. The Council of Europe Convention on Cybercrime of 2001 has been ratified by 65 States (March 2020), and negotiations on a 2nd

---

[8] Number of monthly active Facebook users worldwide as of 4th quarter 2019, 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

Additional Protocol to the Convention on Cybercrime have commenced in 2017[10]. The Tallinn Manual 2.0 was also published in 2017, expanding the coverage of the international law governing cyber warfare to peacetime legal regimes. Within the UNGA First Committee, a Group of Governmental Experts (GGE) continues to study the threats posed by the use of ICTs in the context of international security, with a focus also on how these threats should be addressed[11].

1.19 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.

1.20 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), and India's Cybercrime Coordination 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, and others.

1.21 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

1.22 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.

1.23 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

[10] Council of Europe, Protocol Negotiations, available at https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

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

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]

1.24 In order to help the ITU in strengthening its efforts towards utilizing the GCA, further guidance is offered in the subsequent sections. 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

Introduction

2.1 The legal dimension of cybersecurity is key to ensuring that people from all nations retain 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 recommended relevant regional initiatives as references, including but not limited to the Council of Europe's Convention on Cybercrime of 2001.

Evolution of the legal landscape since 2008

2.3 Regional organizations have developed numerous conventions, declarations, agreements, and guidelines after 2008 on cybersecurity (See Annex 1). As mentioned above, more than 125 countries have signed and/or ratified different cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, which has, to some extent, resulted in fragmentation and diversity at the international level.

2.4 There have been suggestions for a more globally coordinated and structured response to address the wide range of challenges relating to global cybersecurity, and also for any guidelines on legal measures to include principles for harmonizing laws on several global issues[13]. Additionally, some have suggested to develop principles for formulating an international framework for cyberspace for the purpose of global coordination[14].

---

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

- ITU's annual activities report to ITU Council on building confidence and security in the use of ICTs, available at https://www.itu.int/en/council/2020/Pages/default.aspx

- The report to Council 2020 on ITU's utilization of the GCA, which will be available at https://www.itu.int/md/S20-CL-C/en in May 2020

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

[14] Brad Smith, *The need for a Digital Geneva Convention*, February 14, 2017, available at *https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/*

Legal measures and new technologies

2.5 The Council of Europe Convention on Cybercrime is based on cyber conducts[15] in the late 1990s. Some experts have suggested that new technology and methods of conducts in cyberspace with criminal intent should be covered by criminal law.[16] Many countries have adopted or are preparing for new laws covering some of those conducts. Some examples of recent and emerging technologies and trends which could potentially impact legal measures are set out below:

a. Global cyberattacks

Global cyberattacks against critical communications and information infrastructures are emerging as a national security threat. Governments, international organizations, and private institutions have all been targets of global cyberattacks. Some experts suggest, therefore, that global efforts to harmonize legal measures in various areas should include cybersecurity related aspects.[17]

b. Criminal conducts in social networks

There are calls for measures for countering illegal conducts, 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.[18] In 2016, in one of the biggest web attacks ever, web infrastructure across the world was attacked by a botnet of hacked connected devices, ranging from webcams to routers. In 2017, the FBI emphasized the various opportunities available to cybercriminals for accessing IoT and other devices as well as the information attached to these networks.[19] With the advent of new technologies such as 5G, and ubiquitous interconnected devices having become a reality, there are likely to be increased risks.[20]

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.

---

[15] Council of Europe action against Cybercrime, available at https://www.coe.int/en/web/portal/coe-action-against-cybercrime

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

[17] *Ibid*

[18] 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.)

[19] FBI Tech Tuesday, *Building a Digital Defence Against the Internet of Things (IOT)*, 12 December 2017, available at https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday---building-a-digital-defense-against-the-internet-of-things-iot

[20] The Government of Japan organized a conference titled Cyber3 Conference on Okinawa, November 7-8, 2015 which, among other things, also focused on human factors and the moral dimension of IoT.

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.[21]

e. Online child sexual abuse

The United Nations Convention on the Rights of the Child 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 sexual abuse. 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.[22] 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.

Procedural laws - General principles

2.6 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 cybersecurity and cybercrime. 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.[23] It is important that procedural elements include measures that preserve fundamental rights to privacy and human rights, consistent with obligations under international human rights law.

Guidelines to utilize Pillar 1 - Legal Measures

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

2.8 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. 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.

2.9 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 are set out below:

[21] 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

[22] 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.

[23] *Id* at 16

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

b. ITU should continue to work with partners to develop and maintain resources, such as the Cybercrime Legislation Resources, to help Member States understand the legal aspects of cybersecurity, while also exploring opportunities to work with Member States to support development of frameworks on the subject, including legislation, if so requested.

c. Member States are urged to design and develop any appropriate legal measures in accordance with their fundamental human rights obligations.

d. Member States are encouraged to cooperate as well as work together with other stakeholders to search for a global common ground on legal measures on cybersecurity, while noting and modeling existing frameworks such as the Council of Europe Convention on Cybercrime of 2001.

e. Member States are encouraged to continue taking 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.

f. Appropriate legal measures also need to be taken by Member States to implement effective programmes to prevent or prohibit the dissemination of online materials relating to child abuse, including taking preventive actions to detect, disrupt, and dismantle networks, organisations, or structures used for the production and/or distribution of online materials relating to child abuse, and to put in place mechanisms to detect and prosecute offenders while identifying and protecting victims. In this regard, 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, and outcomes on all aspects including legal measures that can facilitate and support country action on this critical issue.

g. ITU, in collaboration with appropriate partners, should promote a better understanding of the cybersecurity-related challenges and risks posed by emerging technologies on existing legal measures, and facilitate the exchange of case studies and good practices at the national, regional, and international level.

h. Noting that the principle of state sovereignty applies in cyberspace, Member States are encouraged to explore mechanisms that protect the fundamental rights and safety of citizens while also facilitating lawful access to the content of communications where end-to-end encryption has been implemented.

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 consistent 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. Mastering cyber risk through technological and procedural measures continues to be of prime importance, especially in the context of critical infrastructures. Given the long-standing role played by 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, standardization activities are fundamental. ITU, with its multi-stakeholder membership, offers a unique platform for global ICT standardization.

3.5 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, privacy technologies such as data de-identification and assurance, 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[24] 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.

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*

[24] ITU Standards Landscape, available at

https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance

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"[25].

3.9 Further, as specified in Recommendation 2.2 of the HLEG Report 2008, ITU is identified as "*the global centre of excellence*"[26] to deal with international standardization process, norms, and standards related to technical and procedural measures. In order to achieve this, more technologically advanced countries, and 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, 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*"[27]. 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 throughout its lifecycle after deployment.

Guidelines to utilize Pillar 2 - Technical & Procedural Measures

3.12 In light of the above, the following guidelines are proposed for Pillar 2:

a. All recommendations made in the HLEG Report 2008 (Recommendations 2.1 – 2.16) are still valid. All Member States are encouraged to commit to a shared global cybersecurity vision, to continue to implement these recommendations (2.1 – 2.16), and to support ITU in becoming "the global centre of excellence" for developing Recommendations on technical and procedural measures for cybersecurity in areas within its mandate (as referenced in the HLEG Report 2008).

b. ITU study groups should focus on emerging security technologies in order to study and formulate guidelines for the use of related technologies, and guide Member States on applying these in a timely manner in order to counter changing and escalating cyber threats.

c. A mechanism for close cooperation should be established among the various ITU-T study groups regarding the study of security-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.

d. 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.

e. ITU should continue to collect global ICT security standards. Other standardization

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

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

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

organizations and industry groups are encouraged to submit their standards on technical and procedural measures to ITU-T for adoption as ITU-T Recommendations.

f. Member States are encouraged to participate in mutual certification arrangements towards a global cybersecurity management framework based on harmonized standards.

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 in order to quickly react to cyber incidents. This distinction can be helpful when comparing and contrasting the different organizational structures around the world.

4.2 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 the lack of national capacities pose challenges in adequately and effectively responding to cyber-attacks. National Computer Incident Response Teams (CIRTs) play an important role in the solution.

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 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), 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) and Saudi Arabia's National Cybersecurity Authority (NCA).

4.5 Despite the growing investment in CIRTs by Member States, and the independent regional and international outreach of national CERTs, there are still 85 countries without a national CIRT – a situation of significant concern given the global nature of cyber threats.[28]

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, nearly 80 CIRT readiness assessments have been conducted by ITU to help countries assess their national cybersecurity preparedness and incident response capabilities.[29] ITU has provided support for the

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

[29] *Ibid*

establishment/enhancement of 14 national CIRTs for respective ITU Member States.[30] 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 NATO Cooperative Cyber Defence Centre of Excellence (CCDCE), launched in Tallinn in 2008, provides its research results on cyber defence measures and promotes cybersecurity through exercises targeting technical experts, military staff and decision-making member nations.
- 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.

Guidelines to utilize Pillar 3 – Organizational Structures

4.8 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 in the implementation of National CIRTs and other related technical units/organizations.

b. ITU should prioritize countries where proper cybersecurity organizational structures have not yet been implemented.

c. ITU should promote more open and inclusive collaboration as well as coordination among various national, regional or international organizations engaged in the effort to establish sustainable national organizational structures, in order to ensure effective support and avoid duplicative efforts.

[30] *Ibid*

d. ITU should increase its efforts to measure institutional commitments of Member States to promote cybersecurity as a crosscutting enabler of their digital transformation.

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

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:

- Implement strategic and operational cybersecurity measures;
- Control risks;
- Manage crises related to the occurrence of security incidents (cyber-attacks);
- Strengthen the robustness and resilience of infrastructures; and
- Develop consistent behaviours 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 security 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 and designing a cybersecurity culture, one of the main challenges is to correctly identify what the global and international issues are and what the specific local needs are. International standards can only contribute to identifying the key global and generic issues related to a cybersecurity culture, as cultures mainly rely on local and temporal factors that respond to the multitude of end-user backgrounds, points of views and needs for this purpose.

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[31]. Everything that can be connected could be hacked. 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.

[31] 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.*

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 prepared to face the challenge of building an inclusive 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 strategy, 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 position on cybersecurity by sharing good practices for effective cybersecurity implementations. The GCI has proven to be an invaluable tool in awareness building and should continue to be leveraged and strengthened.

Guidelines to utilize Pillar 4 – Capacity Building

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.[32]

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. Reportedly, there will be up to 3.5 million cybersecurity related job openings by 2021[33]. 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.[34]

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 key players in the growing digital economy by fostering their trust in the use of ICTs (including broadband and the Internet), and reducing vulnerability to attacks.

---

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

[33] 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

[34] *Ibid*

5.14 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 Development Bureau (BDT):

a. Continue to promote more open and inclusive collaboration, as well as 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 in cybersecurity capacity building efforts, with the support of the national and international cybersecurity capacity building communities.

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

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

e. Continue to evolve its capacity building activities, taking into account the need for new skills to adapt to the security needs of emerging technologies. In this regard, greater collaboration should be fostered with academia.

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

g. Continue to develop and strengthen the GCI as a tool for capacity building.

h. Develop a "Guide on the Implementation of Cybersecurity Education Program" with an aim of providing support to Member States in developing/adopting cybersecurity courses for youth in primary, secondary, university, and adult professional education systems in order to contribute to training more cybersecurity professionals globally.

i. Continue to facilitate identification of cybersecurity-related research activities or dialogues among different stakeholders, especially in emerging technology areas, leveraging ITU's academic membership as has been done, for example, through ITU's annual Artificial Intelligence for Good Global Summit.

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 address security challenges, and build trust and confidence in MSME use of ICTs.

k. Continue to promote a culture of cybersecurity.

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[35]

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, such as the London Process, the Global Commission on the Stability of Cyberspace, groups such as the G20, 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 position in the UN system as the specialized agency for ICTs, can continue to play a leading role, within its mandate, in related developments.

6.6 While a "Global Conference" was suggested in Recommendation 1.15 of the HLEG Report 2008[36], 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 whole-of-government approach with the creation of 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, for example the USA-China High-level

[35] See Annex 1 for more information

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

Joint Dialogues[37] , India-UK Cybersecurity Dialogue[38], Republic of Korea-Australia Cyber Policy Dialogue[39], EU-Japan Cyber Dialogue[40] and so on.

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 with more than 30 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 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 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.

6.13 Even so, different UN agencies need to deliver according to the indications provided by their concerned membership, and more channels for international dialogue can only help contribute towards developing a more comprehensive and common understanding of the issues involved.

6.14 It is 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[41] offers an

[37] More information is available at https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue

[38] More information is available at https://www.gov.uk/government/news/the-4th-uk-india-cyber-dialogue

[39] More information is available at https://www.minister.defence.gov.au/minister/lreynolds/statements/australia-republic-korea-foreign-and-defence-ministers-22-meeting-2019

[40] More information is available at https://www.mofa.go.jp/files/000495346.pdf

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

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.

Guidelines to utilize Pillar 5 - International Cooperation

6.17 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:

a. 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. ITU, 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) should continue to play a leading role, within its mandate, in related developments.

b. Based on the WSIS Process and taking into account the efforts of the UN Secretary-General's High Level Panel on Digital Cooperation – especially Recommendation 4 (Global Commitment on Trust and Security), ITU should help strengthen facilitation efforts in bringing different players together, including the conveners of the various processes. These could be through the mechanisms offered under Action Line C5 related processes through the WSIS Forum, as well as those offered by the IGF, among others.

c. While bilateral and multilateral discussions among key players should continue to be encouraged, given the global nature of cyber threats, it is also important that broader discussions should be facilitated among wider groups, including the private sector and other stakeholders. ITU could play a key facilitating role in this regard – working with partners to help bring together Member States and other stakeholders within the wider global context of the United Nations.

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 co-lead, with other key agencies within the UN family, efforts to harmonize UN's internal efforts 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

7.1 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. In acknowledgment of the urgent challenge posed by cybersecurity at the national and international levels, countries are encouraged to continue elevating the issue of cybersecurity to the highest channels of policy-making and governance within their governments.

b. 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.

c. 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.

d. 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, the deliverables required to meet them, and in accordance with appropriate metrics and measurements that are designed specifically for this purpose.

e. 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 and, where relevant, their potential application to counter cyber threats.

f. 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.

Annex 1 Some regional and global developments since 2008[42]

1. **The Council of Europe Convention on Cybercrime of 2001** is ratified by 65 States, and signed, but not followed by ratification, by 3 States (March 2020) and negotiations on a **2nd Additional Protocol to the Convention on Cybercrime** have commenced in 2017with the aim of concluding in 2020[43]. A statement on an enhanced international cooperation on cybercrime and electronic evidence: *Towards a Protocol to the Budapest Convention*[44] was made on March 19, 2018 as follows: *The matters to be resolved are complex and it may be difficult to reach consensus on the options currently on the table. However, unless solutions are agreed upon, governments may be less and less able to maintain the rule of law to protect individuals and their rights in cyberspace.*

2. **Regional organizations** have developed conventions, declarations, agreements, or guidelines after 2008 on cybersecurity and cybercrime, some of which are as follows:

- Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information (2008)
- The League of Arab States Convention on Combating Information Technology Offences (2010);
- ITU & European Commission - Support for the Establishment of Harmonized Policies for the ICT Market in the ACP States (2012)
- The European Union Directive on attacks against information systems (2013);
- African Union Convention on Cyber Security and Personal Data Protection (2014);
- APEC TEL Strategic Action Plan 2016-2020 (2015);
- The European Union Directive on security of network and information systems (NIS 2016);
- NATO - The Tallinn Manual 2.0: International Law Applicable to Cyber Operations (2017);
- The ASEAN Declaration to Prevent and Combat Cybercrime (2017);
- The European Union General Data Protection Regulation (2018); and
- The Commonwealth Cyber Declaration (2018).

3. **Various organisations** have developed declarations, agreements or guidelines, including:

3.1 The **Paris Peace Forum 2018** included a Declaration launched on November 12, 2018, by President Emmanuel Macron, France, which was titled a *Paris Call for Trust and Security in Cyberspace* included the following statement: *We recognize that the threat of cyber criminality requires more effort to improve the security of the products we use, to strengthen our defences against criminals and to promote cooperation among all stakeholders, within and across national borders, and that the Budapest Convention on Cybercrime is a key tool in this regard.* This high-level declaration was aimed

[42] Information in this Annex has been compiled by Judge Stein Schjolberg, the former chairman of the HLEG, and provided here for information purposes only.

[43] Council of Europe, Protocol Negotiations, available at https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

[44] Council of Europe, *Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention*, available at https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713

at developing common principles for securing cyberspace. 78 countries have signed the *Paris Call for Trust and Security in Cyberspace (*April 2020).[45].

3.2 The Commonwealth Cyber Declaration 2018[46] was unanimously agreed upon by the Commonwealth Heads of Governments Meeting 2018 in London, April 16-20, 2018. Leaders of 53 countries decided in the Declaration to combat cybercrime and promote good cybersecurity, recognising the importance of international cooperation and *recognising the threats to stability in cyberspace and integrity of the critical infrastructure and affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks***.**

3.3 **BRICS Summit Johannesburg Declaration** on July 26, 2018 by Brazil, Russia, India, China and South Africa.

3.4 **The G-20 Summit 2018 (Buenos Aires, Argentina) G-20 Leaders Declaration: Building Consensus for Fair and Sustainable Development** was adopted on December 1, 2018, and reaffirmed the importance of addressing issues of security in the use of ICTs and supported the free flow of information, ideas and knowledge, while respecting applicable legal frameworks, and working to build consumer trust, privacy, data protection and intellectual property rights protection.

3.5. **A Cybersecurity Tech Accord 2018** was launched on April 17, 2018 by global IT companies under the leadership of Microsoft and Facebook. The Cybersecurity Tech Accord is "*a public commitment among more than 30 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace*". Current number of signatories include 143 companies (April 2020)[47].

3.6 The Commonwealth Heads of Governments Meeting 2018 in London on April 16-20. 2018 adopted **A Commonwealth Cyber Declaration**. Leaders of 53 countries decided in the Declaration to combat cybercrime and promote good cybersecurity. It recognizes the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace, and fully abide by the principles and purposes of the Charter of the United Nations.

3.7 Launched in spring 2018, **the Geneva Dialogue on Responsible Behaviour in Cyberspace** aims to map the roles and responsibilities of actors in contributing to greater security and stability in cyberspace in the context of international peace and security. Currently in its second phase, the dialogue will focus on the roles and responsibilities of the business sector. The project aims to: convene global business sector actors to discuss responsible behaviour in cyberspace; assist the business sector to develop its capacities to understand, follow, and meaningfully contribute to international policy and diplomatic processes; and, facilitate dialogue among global businesses towards shaping principles and an action plan contributing to the global efforts at the UN and elsewhere.

3.8 The European Union and its Member States, through the **Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace,** underlined their commitment to continue to promote responsible behaviour in cyberspace through the application of international law, norms of responsible state behaviour, regional confidence building measures and through the EU's framework for a joint diplomatic response to malicious cyber activities.

4. Developments in the UN:

---

[45] More information is available at https://pariscall.international/en/

[46] Commonwealth Cyber Declaration, available at

http://www.thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf

[47] More information is available at https://cybertechaccord.org/accord/

4.1 **United Nations General Assembly Resolution of November 2, 2018** was titled: *Countering the Use of Information and Communication Technologies for Criminal Purposes*. 85 States voted for the adoption, 55 States voted against and 29 States abstained. The Resolution requests the Secretary-General to seek the views of Member States on the challenges they face in countering the use of information and communications technologies for criminal purposes and to present a report based on those views for consideration by the General Assembly at its seventy-fourth session.

4.2 **The UN General Assembly** adopted two resolutions:[48]

a) "**Advancing Responsible State Behaviour in Cyberspace in the Context of International Security**" (document A/C.1/73/L.37) (adopted by 139 in favour to 11 against, with 18 abstentions). By this text, the Assembly would request the Secretary-General, with the assistance of a group of governmental experts to be established in 2019, to continue to study possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States.

b) "**Developments in the field of information and telecommunications in the context of international security**" (document A/C.1/73/L.27.Rev.1) (adopted by a vote of 109 in favour to 45 against, with 16 abstentions). By the text, the Assembly would decide to convene in 2019 an open-ended working group acting on a consensus basis to further develop the rules, norms and principles of responsible behaviour of States.

4.3 **The United Nations General Assembly Resolution of 27 December 2019**: *Countering the use of information and communications technologies for criminal purposes* (Third Committee). The Assembly 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. In so doing, the Assembly would take into full consideration the existing global instruments and efforts to combat the use of information and communications technologies for criminal purposes — including, in particular, the work of the open-ended intergovernmental expert group to conduct a comprehensive study on cybercrime. By a recorded vote of 79 in favour to 60 against, with 30 abstentions, the Assembly adopted the resolution.[49]

4.4 Within the UNGA First Committee, a Group of Governmental Experts on Advancing Responsible State behavior in cyberspace in the context of international security (GGE) continues to study the threats posed by the use of ICTs in the context of international security and how these threats should be addressed[50].

5. Some examples of statements and calls by Heads of State and Senior Ministers

5.1 In the aftermath of the terrorist attack on the French newspaper Charlie Hebdo on 7 January 2015, at the invitation of **Bernard Cazeneuve, the Minister of the Interior of the French Republic, the**

---

[48] UN, *First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct*, available at https://www.un.org/press/en/2018/gadis3619.doc.htm

[49] **EU Statement of January 15, 2020 did not support the UN General Assembly Resolution:** *The EU notes the need for further technologically neutral and capacity building measures to effectively combat this type of crime. However, there is no consensus on the need for a new international treaty negotiated in the UN framework and the solution cannot be an instrument which could lower the standards for protecting human rights and fundamental freedoms, increase the digital divide and endorse state control of the Internet. The EU reaffirms its support for the high standards already laid down in the Council of Europe Convention on Cybercrime. It invites all States who have not done so to join these Conventions as soon as possible*.

[50] Some experts have argued that the GGE has not been effective in terms of implementing its goal of strengthening the security of global information and telecommunications systems. See https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance

Ministers of the Interior and/or Justice of Latvia, Rihards Kozlovskis, President Pro Tempore of the EU Council of Ministers, of Germany, Thomas de Maizière, of Austria, Johanna Mikl-Leitner, of Belgium, Jan Jambon, of Denmark, Mette Frederiksen, of Spain, Jorge Fernandez Diaz, of Italy, Angelino Alfano, of the Netherlands, Ivo Opstelten, of Poland, Theresa Piotrowska, and of the United Kingdom, Theresa May and of Sweden, Anders Ygeman, met on January 11, 2015, in Paris and adopted the following statement in the presence of **European Commissioner for Migration and Home Affairs Dimitris Avramopoulos, Attorney General of the United States Eric H. Holder, Jr., United States Deputy Secretary of Homeland Security Alejandro Mayorkas, Steven Blaney, Minister of Public Safety of Canada, and European Counter-Terrorism Coordinator Gilles de Kerchove[51]:**

> *We are concerned at the increasingly frequent use of the Internet to fuel hatred and violence and signal our determination to ensure that the Internet is not abused to this end, while safeguarding that it remains, in scrupulous observance of fundamental freedoms, a forum for free expression, in full respect of the law.*

5.2 Prime Minister Theresa May, UK, made the following statement[52] on the London Bridge terrorist attack that killed 11 and injured 48 persons on June 3, 2017:

> *We need to work with allied, democratic governments to reach international agreements that regulate cyberspace to prevent the spread of extremism and terrorist planning. And we need to do everything we can at home to reduce the risks of extremism online.*

5.3 The Christchurch Call: Prime Minister Jacinda Ardern, New Zealand, made a statement[53] on the mosque terrorist attack in Christchurch killing 50 persons on March 15, 2019:

> "*We will also look at the role social media played and what steps we can take, including on the international stage, and in unison with our partners. We cannot simply sit back and accept that these platforms just exist and that what is said on them is not the responsibility of the place where they are published. They are the publisher. Not just the postman. There cannot be a case of all profit no responsibility*."

President Emmanuel Macron, France, and Prime Minister Jacinda Ardern invited a group of High Level leaders from 17 countries and IT companies such as Amazon, Facebook, Google and Microsoft to a meeting in Paris on May 15, 2019.[54] This summit aimed to bring together countries and technology companies in an attempt to bring to an end the ability to use social media to organise and promote terrorism and violent extremism. World leaders and technology companies pledged to *"eliminate terrorist and violent extremist content online".* 17 countries originally signed the non-binding agreement with another 31 countries following suit on 23 September the same year. The pledge consists of three sections or commitments: one for governments, one for online service providers and one for the ways in which the two can work together.

5.4 The Lawful Access Summit 2019

[51] More information is available at https://in.ambafrance.org/Charlie-Hebdo-joint-statement-of

[52] More information is available at https://www.gov.uk/government/speeches/pm-statement-following-london-terror-attack-4-june-2017

[53] More information is available at https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/prime-minister-jacinda-arderns-house-statement-on-christchurch-mosques-terror-attack/

[54] More information is available at https://www.christchurchcall.com/

The US Dept. of Justice held the Lawful Access Summit[55] on October 4, 2019 for state and federal law enforcement officials with the theme of the Summit – *Warrant-proof encryption.* The purpose was to discuss that tech companies should open up their encryption schemes to police investigating crimes. A problem was emphasized: *Have encryption schemes turned Internet into a lawless space?*[56]

The Australia Minister for Home Affairs Peter Dutton presented at the Summit the anti-encryption law that was enacted in Australia in December 2018 when Australia adopted *The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.[57] The purpose was also to ensure that agencies can lawfully access intelligible communications content, since it was estimated that by 2020 all electronic communications of investigative value will be encrypted.

On October 4, 2019 the U.S. and UK governments also agreed on a *CLOUD Act Agreement.*[58]

———————————

[55] More information is available at https://www.justice.gov/olp/lawful-access

[56] See also: Open letter from the Home Secretary - alongside US Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton - to Mark Zuckerberg, December 23, 2019, available at https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f

[57] More information is available at https://www.justice.gov/dag/page/file/1153466/download

[58] More information is available at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists