RESOLUTION 130 (REV. BUCHAREST, 2022)

Strengthening the role of ITU in building confidence and security in the use of information and communication technologies

The Plenipotentiary Conference of the International Telecommunication Union (Bucharest, 2022),

recalling

a) United Nations General Assembly (UNGA) Resolution 68/198, on information and communication technologies (ICTs) for development;

b) UNGA Resolution 71/199, on the right to privacy in the digital age;

c) UNGA Resolution 68/243, on developments in the field of information and telecommunications in the context of international security;

d) UNGA Resolution 57/239, on the creation of a global culture of cybersecurity;

e) UNGA Resolution 64/211, on the creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures;

f) the WSIS+10 Statement on the implementation of outcomes of the World Summit on the Information Society (WSIS) and the WSIS+10 Vision for WSIS beyond 2015, which were adopted at the ITU-coordinated WSIS+10 High-Level Event (Geneva, 2014), based on the Multistakeholder Preparatory Platform, together with other United Nations agencies and inclusive of all WSIS stakeholders, were endorsed by the Plenipotentiary Conference (Busan, 2014) and were submitted to the UNGA overall review;

g) UNGA Resolution 70/125, on the outcome document of the UNGA high-level meeting on the overall review of the implementation of the WSIS outcomes;

h) Resolution 174 (Rev. Busan, 2014) of the Plenipotentiary Conference, on ITU's role with regard to international public policy issues relating to the risk of illicit use of ICTs;

i) Resolution 179 (Rev. Bucharest, 2022) of this conference, on ITU's role in child online protection;

j) Resolution 181 (Guadalajara, 2010) of the Plenipotentiary Conference, on definitions and terminology relating to building confidence and security in the use of ICTs;

k) Resolution 196 (Rev. Bucharest, 2022) of this conference, on protecting telecommunication service users/consumers;

l) Resolution 45 (Rev. Kigali, 2022) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;

m) Resolution 140 (Rev. Bucharest, 2022) of this conference, on ITU's role in implementing the WSIS outcomes and the 2030 Agenda for Sustainable Development, as well as in their follow-up and review processes;

n) Resolution 50 (Rev. Geneva, 2022) of the World Telecommunication Standardization Assembly (WTSA), on cybersecurity;

o) Resolution 58 (Rev. Geneva, 2022) of WTSA, on encouraging the creation of national computer incident response teams (CIRTs), particularly for developing countries[1];

p) Resolution 67 (Rev. Kigali, 2022) of WTDC, on the role of the ITU Telecommunication Development Sector (ITU-D) in child online protection;

q) Resolution 69 (Rev. Kigali, 2022) of WTDC, on facilitating the creation of national CIRTs, particularly for developing countries, and cooperation among them;

---

[1] These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition.

r) that ITU Council Resolution 1305, adopted at its 2009 session, identified the security, safety, continuity, sustainability and robustness of the Internet as public policy issues that fall within the scope of ITU,

considering

a) that ITU has played a valuable role during the coronavirus disease (COVID-19) pandemic, providing a platform for ICT regulators, policy-makers and other stakeholders to share information and best practices, for example through the ITU's Global Network Resiliency Platform;

b) that the ITU-coordinated WSIS+10 High-Level Event reaffirmed the importance of building confidence and security in the use of ICTs, as mentioned in relevant paragraphs of the WSIS+10 outcome documents (Geneva, 2014);

c) the crucial importance of information and communication infrastructures and their applications to practically all forms of social and economic activity;

d) the cybersecurity-related provisions of the Tunis Commitment and the Tunis Agenda for the Information Society and the outcome document of the UNGA high-level meeting on the overall review of the implementation of WSIS;

e) that, with the application and development of ICTs, new threats from various sources have emerged that have had an impact on confidence and security in the use of ICTs by all Member States, Sector Members and other stakeholders, including all users of ICTs, and on the preservation of peace and economic and social development of all Member States, and that threats to and vulnerabilities of infrastructures, networks and devices continue to give rise to ever-growing security challenges across national borders for all countries, in particular developing countries, while noting in this context the strengthening of ITU's role in building confidence and security in the use of ICTs and the need to further enhance international cooperation and capacity building and develop appropriate existing national, regional and international mechanisms (for example agreements, best practices, memoranda of understanding (MoU), etc.);

f) that the ITU Secretary-General has been invited to support other global or regional cybersecurity projects, as appropriate, and all countries, particularly developing countries, have been invited to take part in their activities that are relevant to ITU;

g) the ITU Global Cybersecurity Agenda (GCA), which encourages international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of telecommunications/ICTs;

h) that the Council approved, at its 2022 session, guidelines for the utilization of the GCA by ITU in its work;

i) that, in order to protect these infrastructures and address these challenges and threats, coordinated national, regional and international action is required for prevention, preparation, response and recovery from computer security incidents, on the part of government authorities, at the national (including the creation of national CIRTs) and sub-national levels, the private sector and citizens and users, in addition to international and regional cooperation and coordination, and that ITU has a lead role to play within its mandate and competencies in this field;

j) that an iterative, risk-based approach to cybersecurity enables cybersecurity practices to be developed and applied as needed to address constantly evolving threats and vulnerabilities, and that security is a continuous and iterative process which must be built into the development and deployment of technologies and their applications from the beginning and continue throughout their lifetime;

k) the need for continual evolution in new technologies to support the early detection of, and coordinated and timely response to, events or incidents compromising computer security, or computer network security incidents that could compromise the availability, integrity and confidentiality of critical infrastructures in ITU Member States, and for strategies that will minimize the impact of such incidents and mitigate the growing risks and threats to which such platforms are exposed;

l) that UNGA Resolution 70/125, on the outcome document of the UNGA high-level meeting on the overall review of the implementation of the WSIS outcomes, recognized the challenges that States, in particular developing countries, face in building confidence and security in the use of ICTs and called for renewed focus on capacity building, education, knowledge-sharing and regulatory practice, as well as promoting multistakeholder cooperation at all levels and raising awareness among ICT users, particularly the poorest and most vulnerable;

m) that the number of cyberthreats and cyberattacks is growing, as is dependence on the Internet and other networks that are essential for accessing services and information;

n) that the ITU Telecommunication Standardization Sector (ITU-T) has adopted around 300 standards relating to building confidence and security in the use of ICTs;

o) the final report on ITU-D study Question 3/2, on securing information and communication networks: best practices for developing a culture of cybersecurity;

p) that the multidisciplinary nature of the cybersecurity standards landscape calls for shared actions, cooperation and synergies between ITU and other national organizations of Member States and regional, global and sectoral organizations;

q) that many developing countries are elaborating or implementing national cybersecurity strategies;

r) that although progress has been made in some areas, many countries face challenges in developing effective qualifications and career pathways, and this is a significant barrier to promoting confidence and security in ICTs;

s) that cybersecurity has become a very important issue at the international level, and that the role and involvement of the United Nations and its relevant specialized agencies such as ITU in building confidence and security in the use of ICTs is therefore important;

t) the different roles and responsibilities of all stakeholders in ensuring confidence and security in the use of ICTs;

u) that some small and medium enterprises (SMEs) face additional challenges in implementing cybersecurity practices;

v) the need to raise awareness and promote basic security measures for cyberhygiene that everyone should take to protect themselves, including women, children, persons with disabilities, persons with specific needs and persons with age-related disabilities, from cybersecurity risks,

recognizing

a) that cybersecurity is a fundamental element for securing telecommunication/ICT infrastructures and an essential foundation for social and economic development;

b) that the development of ICTs has been and continues to be instrumental for the growth and development of the global economy, including the digital economy, underpinned by security and trust;

c) that WSIS affirmed the importance of building confidence and security in the use of ICTs and the great importance of multistakeholder implementation at the international level, and established Action Line C5 (Building confidence and security in the use of ICTs), with ITU identified in the Tunis Agenda as moderator/facilitator for the action line, and that this task has been carried out by the Union in recent years, for example under the GCA;

d) that the Kigali Declaration adopted by WTDC-22 declares: "In the digital era, universal, secure and affordable broadband connectivity is indispensable and provides opportunities for boosting productivity and efficiency, ending poverty, improving livelihoods and ensuring that sustainable development becomes a reality for all. Continuing to build confidence, trust and security in the use of telecommunications/ICTs remains of vital importance.";

e) that WTDC-22 adopted the Kigali Action Plan and the ITU-D priority on inclusive and secure telecommunications/ICTs for sustainable development, which declares: "The focus of this priority is on providing support for Member States to achieve secure telecommunications/ICTs for digital development for all. The following topics can be considered as the supporting components of this priority: fostering digital literacy and raising awareness of cybersecurity issues and best practice; strengthening the security of users online and promoting consumer protection; assisting Member States to develop national cybersecurity strategies and computer incident response teams (CIRTs); promoting digital skills development and digital training programmes, including training for public authorities; investment in secure infrastructure, particularly in underserved areas.";

f) that WTDC-22 revised Resolution 45 (Rev. Kigali, 2022), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam, as appropriate; WTDC-22 adopted Resolution 69 (Rev. Kigali, 2022), on facilitating the creation of national CIRTs, particularly for developing countries, and cooperation among them; and WTSA-20 adopted Resolution 58 (Rev. Geneva, 2022), on encouraging the creation of national CIRTs, particularly for developing countries;

g) § 15 of the Tunis Commitment, which states: "Recognizing the principles of universal and non-discriminatory access to ICTs for all nations, the need to take into account the level of social and economic development of each country, and respecting the development-oriented aspects of the information society, we underscore that ICTs are effective tools to promote peace, security and stability, to enhance democracy, social cohesion, good governance and the rule of law, at national, regional and international levels. ICTs can be used to promote economic growth and enterprise development. Infrastructure development, human capacity building, information security and network security are critical to achieve these goals. We further recognize the need to effectively confront challenges and threats resulting from use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights", and that the challenges created by such misuse of ICT resources have only continued to increase since WSIS;

h) that the ITU-coordinated WSIS+10 High-Level Event identified several challenges in the implementation of the WSIS action lines that still remain and that will need to be addressed beyond 2015;

i) that Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats at the national, regional and international levels, may require assistance from ITU in establishing technical and procedural measures, aimed at securing national ICT infrastructures, on request from these Member States, while noting that there are a number of regional and international initiatives which may support these countries in elaborating such legal measures;

j) Opinion 4 (Lisbon, 2009) of the World Telecommunication/ICT Policy Forum (WTPF), on collaborative strategies for creating confidence and security in the use of ICTs;

k) the relevant outcomes of WTSA-20, notably:

i) Resolution 50 (Rev. Geneva, 2022), on cybersecurity;

ii) Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam;

l) that secure and trusted networks will build confidence and encourage the exchange and use of information and data;

m) that the development of human skills and capacity building are key to enhancing the protection of information networks;

n) that many Member States face significant skills shortages in their cybersecurity workforce and that this lack of trained cybersecurity professionals is a fundamental barrier to building confidence and security in the use of ICTs, and that it is important to encourage more people to choose a career in cybersecurity;

o) that Member States are making efforts to improve institutional environments;

p) that risk assessment and analysis provide a better understanding of the cybersecurity risks that organizations face and how to mitigate them;

q) that spam is a global problem, with different characteristics in different regions, and a multistakeholder cooperative approach is necessary to counter it,

aware

a) that ITU and other international organizations, through a variety of activities, are examining issues related to building confidence and security in the use of ICTs, including stability and measures to combat spam, malware, etc. and to protect personal data and privacy;

b) that the relevant ITU study groups, in accordance with their mandates, should keep pace with the development of telecommunication/ICT technologies and take into account issues related to cybersecurity;

c) that ITU-T Study Group 17, ITU-D Study Groups 1 and 2 and other relevant ITU study groups continue to work on technical means for the security of information and communication networks, in accordance with WTSA Resolutions 50 (Rev. Geneva, 2022) and 52 (Rev. Hammamet, 2016) and WTDC Resolutions 45 and 69 (Rev. Kigali, 2022);

d) that ITU has a fundamental role to play in building confidence and security in the use of ICTs;

e) that ITU-D Study Group 2 continues to carry out the studies called for in ITU-D study Question 3/2, on securing information and communication networks: best practices for developing a culture of cybersecurity, which has been reflected in UNGA Resolution 64/211;

f) that ITU is also assisting developing countries in building confidence and security in the use of ICTs and supporting the establishment of CIRTs and promoting the related operating framework of CIRTs, including CIRTs responsible for government-to-government cooperation, and the importance of coordination among all relevant organizations;

g) that Council Resolution 1336, adopted at its 2011 session, established the Council Working Group on international Internet-related public policy issues (CWG-Internet), whose terms of reference are to identify, study and develop matters related to international Internet-related public policy issues, including those issues identified in Council Resolution 1305 (2009), such as security, safety, continuity, sustainability and robustness of the Internet;

h) that WTDC-17 adopted Resolution 80 (Rev. Buenos Aires, 2017), on establishing and promoting trusted information frameworks in developing countries to facilitate and encourage electronic exchanges of economic information between economic partners;

i) of Article 6, on security and robustness of networks, and Article 7, on unsolicited bulk electronic communications, of the International Telecommunication Regulations adopted by the World Conference on International Telecommunications (Dubai, 2012),

noting

a) that, as an intergovernmental organization with private-sector participation, ITU is well-positioned to play an important role, together with other relevant international bodies and organizations, in addressing threats and vulnerabilities which affect efforts to build confidence and security in the use of ICTs;

b) §§ 35 and 36 of the Geneva Declaration of Principles and § 39 of the Tunis Agenda, on building confidence and security in the use of ICTs;

c) that although there are no universally agreed upon definitions of spam and other terms in this sphere, spam was characterized by ITU-T Study Group 2, at its June 2006 session, as a term commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging (SMS, MMS), usually with the objective of marketing commercial products or services;

d) the Union's initiative on cooperation with the Forum for Incident Response and Security Teams;

e) the relevant WTPF-21 opinions,

bearing in mind

the work of ITU established by WTSA Resolutions 50 and 58 (Rev. Geneva, 2022) and 52 (Rev. Hammamet, 2016) and WTDC Resolutions 45 and 69 (Rev. Kigali, 2022); the ITU-D priority on inclusive and secure telecommunications/ICTs for sustainable development of the Kigali Action Plan; the relevant ITU-T questions on technical aspects regarding the security of information and communication networks; and ITU-D study Question 3/2,

resolves

1 to continue promoting the ITU's Global Network Resiliency Platform and its work to provide a platform for ICT regulators, policy-makers and other stakeholders to share best practice on building confidence and security in the use of ICTs;

2 to continue to give this work high priority within ITU, taking into account new and emerging telecommunication/ICT services and technologies and in accordance with its competences and expertise, including promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at the national, regional and international levels;

3 that ITU should continue to serve as an information-sharing platform for the various activities, initiatives and projects that are being carried out on different facets of cybersecurity by stakeholders and organizations active in this field to provide an easy point of access for all;

4 to continue to give high priority to the work of ITU described under *bearing in mind* above, in accordance with its competencies and areas of expertise, and to continue to work closely, as appropriate, with other relevant bodies/agencies within the United Nations and other relevant international bodies, taking into account the specific mandates and areas of expertise of the different agencies, while being mindful of the need to avoid duplicating work between organizations and among the Bureaux or the General Secretariat;

5 that ITU shall focus resources and programmes on those national, regional and international areas of cybersecurity that are within its core mandate and expertise, notably the technical and development spheres, and not including areas 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, although this does not however exclude ITU from carrying out its mandate to develop technical recommendations designed to reduce vulnerabilities in the ICT infrastructure, nor from all the assistance that was agreed upon at WTDC-22, including the ITU-D priority on inclusive and secure telecommunications/ICTs for sustainable development;

6 to promote a culture in which security is seen as a continuous and iterative process, built into products from the beginning and continuing throughout their lifetime, and is accessible and understandable for users;

7 to promote greater awareness among ITU members on the activities carried out within ITU and other relevant entities involved in strengthening confidence and security in the use of ICTs, including cybersecurity, cyberresilience and capacity building;

8 to engage actively with other relevant organizations in order to raise their awareness of the particular challenges faced by developing countries in building confidence and security in the use of ICTs;

9 to contribute to further strengthening the trust and security framework, consistent with ITU's role as lead facilitator of WSIS Action Line C5, taking into account Resolution 140 (Rev. Bucharest, 2022);

10 to continue to maintain, in building upon the information base associated with the "ICT Security Standards Roadmap" and "Security Compendium" and ITU-D's efforts on cybersecurity, and with the assistance of other relevant organizations, an inventory of national, regional and international initiatives and activities to promote the development of common approaches in the field of cybersecurity;

11 to promote the growth and development of a diverse and skilled cybersecurity workforce that is able to address and mitigate cyberrisks, and promote the importance of effective qualifications and professional career pathways;

12 to develop case studies on cybersecurity-related institutional arrangements, regulatory approaches, awareness-raising programmes and skills and workforce development in cooperation with the membership and relevant organizations;

13 to consider the specific cybersecurity challenges faced by SMEs and incorporate those considerations into ITU's activities in the area of building confidence and security in the use of ICTs;

14 to take into account the impact of the deployment of emerging technologies on cybersecurity, and incorporate this consideration in ITU's activities in the area of building confidence and security in the use of ICTs;

15 to support the development of infrastructure which underpins the ongoing digital transformation of the global economy by building confidence and security in the use of ICTs, in particular in dealing with existing and future threats, within the mandate of ITU;

16 that all work carried out by ITU to build confidence and security in the use of ICTs should be guided by an assessment of the needs and objectives of its members using tools such as the Global Cybersecurity Index (GCI), with clearly defined deliverables, and in accordance with appropriate metrics and measurements that are designed specifically for this purpose;

17 to take into account the specific challenges faced especially by developing countries in the area of building confidence and security in the use of ICTs;

18 to utilize the GCA framework in order to further guide the work of the Union on efforts to build confidence and security in the use of ICTs, taking into consideration the Guidelines for utilization of the GCA by ITU approved by the Council;

19 to encourage all stakeholders to engage with one another and take action to support capacity building and voluntary information-sharing on cybersecurity issues and best practices,

instructs the Secretary-General and the Directors of the Bureaux

1 to continue to provide a platform for ICT regulators, policy-makers and other stakeholders to share with one another information and best practice on building confidence and security in the use of ICTs, especially during globally shared challenges such as pandemics;

2 to continue to review:

i) the work done so far in the three Sectors, under the GCA and in other relevant organizations and initiatives to address and strengthen protection against existing and future threats in order to build confidence and security in the use of ICTs;

ii) the progress achieved in the implementation of this resolution, with ITU continuing to play a lead facilitating role as the moderator/facilitator for WSIS Action Line C5, with the help of the advisory groups, consistent with the ITU Constitution and ITU Convention;

iii) the results of work done so far to support developing countries in particular to build capacity and skills in cybersecurity in order to ensure that ITU is effectively focusing its resources to address development challenges;

3 to raise awareness on the activities carried out within ITU and other relevant entities involved in strengthening cybersecurity, including on capacity building, and of the particular challenges faced by developing countries in building confidence and security in the use of ICTs, consistent with *resolves* 4 and 5 above;

4 to facilitate access to tools and resources, within the available budget, required for enhancing confidence and security in the use of ICTs for all Member States, consistent with WSIS provisions on universal and non-discriminatory access to ICTs for all nations;

5 to continue knowledge- and information-sharing of existing and future national, regional and international cybersecurity-related initiatives worldwide through the ITU cybersecurity webpage, and encourage all stakeholders to contribute to these activities, taking into account existing portals;

6 to further enhance coordination between the study groups across the Sectors and programmes concerned;

7 to consider the results of the GCI to guide ITU cybersecurity-related initiatives, especially taking into account the gaps identified through the GCI process;

8 to report annually to the Council on the implementation of this resolution, and on the activities of the three Sectors and the General Secretariat to build confidence and security in the use of ICTs in line with WSIS Action Line C5, and to make proposals as appropriate;

9 consistent with Resolution 45 (Rev. Kigali, 2022), to report to the Council on activities within ITU and other relevant organizations and entities aimed at enhancing cooperation and collaboration, regionally and globally, and strengthening building confidence and security in the use of ICTs of Member States, in particular developing countries, taking into account any information provided by Member States, including information on situations within their own jurisdiction that could affect this cooperation;

10 consistent with Resolution 45 (Rev. Kigali, 2022), to report on MoU between countries, as well as existing forms of cooperation, providing analysis of their status, scope and the application of these cooperative mechanisms to strengthen cybersecurity and combat cyberthreats, with a view to enabling Member States to identify whether additional memoranda or mechanisms are required,

instructs the Director of the Telecommunication Standardization Bureau

1 to intensify work within existing ITU-T study groups in order to:

i) address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs, taking into account new and emerging telecommunication/ICT services and technologies based on telecommunication/ICT networks, by developing recommendations, supplements and technical reports, as appropriate, with the goal of implementing WTSA resolutions, particularly Resolutions 50 and 58 (Rev. Geneva, 2022) and 52 (Rev. Hammamet, 2016), allowing work to begin before a question is approved;

ii) seek ways to enhance the exchange of technical information in these fields, promote the adoption of protocols and standards that enhance security, and promote international cooperation among appropriate entities;

iii) to encourage collaboration among the various ITU-T study groups regarding the study of cybersecurity-related matters, throughout their work on standardization;

iv) to facilitate actions deriving from the outcomes of WTSA, in particular:

- Resolution 50 (Rev. Geneva, 2022), on cybersecurity;
- Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam;

2 to consider within ITU-T the promotion of a culture in which security is seen as a continuous and iterative process, and to make proposals to the Council as appropriate;

3 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions and joint coordination activity groups, and, by invitation, through written contributions from relevant organizations;

4 to support the work under ITU-D study Question 3/2;

5 to continue to collaborate with the Director of the Telecommunication Development Bureau in the dissemination to developing countries of information on guidelines, recommendations, technical reports and best practices related to building confidence and security in the use of ICTs which have been developed by the ITU-T study groups,

instructs the Director of the Telecommunication Development Bureau

1 consistent with the results of WTDC-22, and pursuant to Resolutions 45 and 69 (Rev. Kigali, 2022), Resolution 80 (Buenos Aires, 2017) and the ITU-D priority on inclusive and secure telecommunications/ICTs for sustainable development of the Kigali Action Plan, to support ongoing regional and global cybersecurity projects, and to encourage all countries to take part in these activities;

2 upon request, to support ITU Member States in their efforts to build capacity, by facilitating Member States' access to resources developed by other relevant international organizations that are working on national legislation to combat cybercrime; supporting ITU Member States' national and regional efforts to build capacity to protect against cyberthreats/cybercrime, in collaboration with one another; consistent with the national legislation of Member States referred to above, assisting Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats at the national, regional and international levels; establishing technical and procedural measures aimed at securing national ICT infrastructures, taking into account the work of the relevant ITU-T study groups and, as appropriate, other relevant organizations; establishing organizational structures, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level;

3 to provide the necessary financial and administrative support for these projects within existing resources, including those for the continuity of the GCI process, and to seek additional resources (in cash and in kind) for the implementation of these projects through partnership agreements;

4 to ensure coordination of the work of these projects within the context of ITU's overall activities in its role as moderator/facilitator for WSIS Action Line C5, and to eliminate any duplication regarding this important subject with the General Secretariat and ITU-T;

5 to continue to evolve capacity-building activities, through international collaboration, taking into account the need for new skills to adapt to the opportunities and challenges of emerging technologies in the field of cybersecurity; in this regard, greater collaboration should be fostered with Member States, academia, the private sector and relevant United Nations organizations;

6 to coordinate the work of these projects with that of the ITU-D study groups on this topic, and with the relevant programme activities and the General Secretariat;

7 to continue collaboration with relevant organizations with a view to exchanging relevant information on cybersecurity threats and issues, sharing best practices and disseminating information through, for example, joint workshops and training sessions;

8 to identify best practice for the development of qualifications and professional career pathways in cybersecurity for the benefit of the ITU membership;

9 to support the work of ITU-T Study Group 17 and other study groups by promoting and facilitating the implementation of approved security-related ITU-T recommendations by ITU Member States and Sector Members, especially from developing countries;

10 to support ITU Member States in the development of their national and/or regional cybersecurity strategies towards building national capabilities for protecting against and dealing with cyberthreats in accordance with the principles of international cooperation;

11 to support the membership in the development of human skills and capacity building to enhance cybersecurity;

12 to support the membership to address cybersecurity skills shortages by encouraging people to enter the cybersecurity profession and promoting the employment of women in the cybersecurity field;

13 to support the membership in the risk-assessment activities related to cybersecurity;

14 to maintain, develop and promote a repository of best practice on measures that facilitate and encourage people to choose a career in cybersecurity;

15 to change how the results of the GCI are presented so that countries are represented in tiers rather than by individual ranking in order to more accurately reflect the development of cybersecurity in Member States;

16 to create and maintain a repository of best practices on countering and combating spam, to be shared through ITU with all members,

further instructs the Director of the Telecommunication Standardization Bureau and the Director of the Telecommunication Development Bureau, each within the scope of their responsibilities:

1 to implement relevant resolutions of both WTSA-20 and WTDC-22, including the ITU-D priority on inclusive and secure telecommunications/ICTs for sustainable development of the Kigali Action Plan, with particular focus on the needs of developing countries as they undertake efforts to improve cybersecurity and build confidence and security in the use of ICTs;

2 to disseminate to ITU Member States, in particular developing countries, information on guidelines, recommendations, technical reports and best practices related to cybersecurity;

3 to identify and promote the availability of information on building confidence and security in the use of ICTs, including ICT infrastructure, for Member States, Sector Members and relevant organizations;

4 to continue to support relevant ITU study groups to build confidence and security in the use of ICTs;

5 without duplicating the work under ITU-D study Question 3/2, to continue identifying best practices related to Question 3/2, including establishing CIRTs, and promoting the related operating framework of CIRTs to review the reference guide for the Member States and, where appropriate, to contribute to Question 3/2;

6 to cooperate with relevant organizations and other relevant international and national experts, as appropriate, in order to identify best practices in building confidence and security in the use of ICTs, including the establishment of CIRTs;

7 to take action with a view to new questions being examined by the study groups within the Sectors on the establishment of confidence and security in the use of ICTs;

8 to identify, document and promote the adoption of practical steps to support developing countries in building capacity and skills in cybersecurity, taking into account the specific challenges they face;

9 to consider the specific cybersecurity challenges and needs faced by SMEs, incorporating these particular aspects into the activities of ITU to build confidence and security in the use of ICTs;

10 to take into account the challenges faced by all stakeholders, particularly in developing countries, in building confidence and security in the use of ICTs and identifying steps that can help to address them;

11 to support Member States to identify the basic security measures for cyberhygiene that everyone should take to protect themselves from cyberrisks, and to encourage and support ITU members and other stakeholders to promote these to the public;

12 to identify and document practical steps to strengthen security in the use of ICTs internationally, including the concept that security is seen as a continuous and iterative process, based on "security by design" approaches and other widely accepted practices, guidelines and recommendations that Member States and other stakeholders can choose to apply to improve their ability to combat cyberthreats and attacks, including a dynamic and iterative risk-based approach that reflects the evolving nature of threats and vulnerabilities, and to strengthen international cooperation in building confidence and security in the use of ICTs, including promoting voluntary information-sharing among interested Member States, taking into account the GCA and within available financial resources;

13 to support strategy, organization, awareness-raising, cooperation, evaluation and skills development;

14 to provide the necessary technical and financial support, within the constraints of existing budgetary resources;

15 to encourage the engagement of experts in the ITU's activities in the area of building confidence and security in the use of ICTs;

16 to mobilize appropriate extrabudgetary resources, outside the regular budget of the Union, for the implementation of this resolution, to help developing countries;

17 to support and assist developing countries in promoting and facilitating the implementation of security-related ITU-T recommendations;

18 to share experiences and raise awareness on cybersecurity assurance practices and programmes,

instructs the Secretary-General

pursuant to the Secretary-General's initiative on this matter:

1 to continue to mobilize the development and technical expertise of the Union, as a specialized agency for ICTs within the United Nations system and the sole facilitator of WSIS Action Line C5 (Building confidence and security in the use of ICTs), with a view to strengthening national, regional and international cybersecurity in support of the Sustainable Development Goals, working with other relevant bodies/agencies within the United Nations and other relevant international bodies, taking into account the specific mandates and areas of expertise of the different agencies, while being mindful of the need to avoid duplicating work between organizations, and among the Bureaux or with the General Secretariat;

2 to cooperate with relevant international organizations, including through the adoption of MoU, subject to the approval of the Council in this regard, in accordance with Resolution 100 (Minneapolis, 1998) of the Plenipotentiary Conference;

3 to support ITU's regional and global cybersecurity initiatives, and to invite all countries to take part in these activities, such as cyberdrills, among others;

4 to support efforts to promote cybersecurity through bringing different stakeholders together, through the WSIS Forum, *inter alia*, taking into account WSIS Action Line C5,

requests the ITU Council

to include the report of the Secretary-General in the documents sent to Member States in accordance with No. 81 of the Convention,

invites Member States

1 to consider joining appropriate competent international and regional initiatives for enhancing national legislative frameworks relevant to the security of information and communication networks as well as collaboration in building confidence and security in the use of ICTs;

2 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 45 (Rev. Kigali, 2022), with a view to enhancing confidence and security in the use of ICTs, in order to mitigate risks and threats;

3 to support ITU initiatives on cybersecurity, including the GCI, and the Global Network Resiliency Platform, in order to promote national strategies and the sharing of information on efforts across industries and sectors;

4 to inform the Secretary-General of relevant activities related to this resolution regarding confidence and security in the use of ICTs;

5 to benefit from the resources, support and best practices of national, regional and international cybersecurity-related initiatives worldwide through the ITU cybersecurity webpage;

6 to collaborate with relevant organizations, through the exchange of best practices in building confidence and security in the use of ICTs, including the establishment, development and implementation of national CIRTs, especially in developing countries;

7 to encourage their national CIRTs to collaborate with other national and subnational governmental agencies as appropriate, and other CIRTs and stakeholders;

8 to encourage the engagement of experts in ITU's activities in the area of building confidence and security in the use of ICTs;

9 to continue to raise awareness through the dissemination of best practices and policies that have been implemented in order to increase the ability to develop appropriate policies to address the protection of users, so as to enhance trust in the use of telecommunications/ICTs;

10 to identify the basic security measures that their public should take to protect themselves from cyberrisks, and promote them;

11 to encourage information-sharing on cybersecurity issues and best practices, at the national, regional and international levels;

12 to support and engage in efforts that lead to sustainable, secure and stable national telecommunication/ICT infrastructure,

invites Member States, Sector Members and Associates

1 to contribute on this subject to the relevant ITU study groups and to any other activities for which the Union is responsible;

2 to contribute to building confidence and security in the use of ICTs at the national, regional and international levels, by undertaking activities as outlined in the WSIS outcome documents, the WSIS+10 Statement on the implementation of WSIS outcomes and the WSIS+10 Vision for WSIS beyond 2015, and the outcome document of the UNGA high-level meeting on the overall review of the implementation of the WSIS outcomes, and to contribute to the preparation and implementation of those activities;

3 to raise awareness among all stakeholders, including organizations and individual users, of the importance of strengthening cybersecurity, including the implementation of basic safeguards;

4 to promote the development of educational and training programmes to enhance user awareness of cyberrisks, especially for women, children, persons with disabilities, persons with specific needs and persons with age-related disabilities, and the steps that they can take to protect themselves;

5 to incorporate an iterative, risk-based approach towards addressing evolving threats and vulnerabilities, and to promote a culture in which security is seen as a continuous and iterative process which must be built into the development and deployment of technologies and their applications from the beginning and continue throughout their lifetime, in their efforts to build confidence and security in the use of ICTs;

6 to promote initiatives to encourage more people to enter the cybersecurity profession and to provide training opportunities for them;

7 to provide initiatives so that women and girls can have access to studies and careers in cybersecurity;

8 to contribute to ITU's repository of best practices on measures that facilitate and encourage more people to choose a career in cybersecurity;

9 to collaborate on cybersecurity, cyberresilience and capacity-building solutions, as appropriate, in order to address and prevent problems that undermine confidence and security in the use of telecommunications/ICTs;

10 to engage in the improvement of the GCI process, including the discussion on the methodology, structure, weightage and questions, using the GCI expert group;

11 to share best practices and information about digital certificates.

(Marrakesh, 2002) – (Rev. Antalya, 2006) – (Rev. Guadalajara, 2010) – (Rev. Busan, 2014) – (Rev. Dubai, 2018) – (Rev. Bucharest, 2022)