RESOLUTION 45 (Rev. Kigali, 2022)

Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam

The World Telecommunication Development Conference (Kigali, 2022),

recalling

a) Resolution 130 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of information and communication technologies (ICTs);

b) 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;

c) Resolution 179 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on ITU's role in child online protection;

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

e) Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC);

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

g) Resolution 52 (Rev. Hammamet, 2016) of WTSA, on countering and combating spam;

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

i) Resolution 69 (Rev. Kigali, 2022) of this conference, on facilitating the creation of 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.

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

k) the relevant opinions of the sixth World Telecommunication Policy Forum (WTPF-21) that fall under the mandate of ITU-D;

l) the noble principles, aims and objectives embodied in the Charter of the United Nations and the Universal Declaration of Human Rights;

m) that ITU is the lead facilitator for Action Line C5 in the Tunis Agenda for the Information Society (Building confidence and security in the use of ICTs) of the World Summit on the Information Society (WSIS);

n) the cybersecurity-related provisions of the WSIS Tunis Commitment and the Tunis Agenda;

o) the goals set out in the strategic plan for the Union in force;

p) ITU-D study Question on ''Securing information and communication networks: Best practices for developing a culture of cybersecurity'', under which in the previous cycle many members collaborated to produce reports, including course materials for use in developing countries, such as a compendium of national experiences, best practices for public-private partnerships (PPPs), best practices for building a CIRT with accompanying course material, and best practices for a CIRT management framework;

q) the report of the Chairman of the High-Level Group of Experts of the Global Cybersecurity Agenda (GCA), established by the ITU Secretary-General pursuant to the requirements of Action Line C5 on building confidence and security in the use of ICTs and in accordance with Resolution 140 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on the role of ITU as sole facilitator for WSIS Action Line C5, and Resolution 58 (Rev. Geneva, 2022), on encouraging the creation of national CIRTs, particularly for developing countries;

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

s) that ITU and the United Nations Office on Drugs and Crime have signed a memorandum of understanding (MoU) in order to strengthen security in the use of ICTs,

considering

a) the role of telecommunications/ICTs as effective tools to promote peace, economic development, security and stability and to enhance democracy, social cohesion, good governance and the rule of law, and the need to confront the escalating challenges and threats resulting from the abuse of this technology, including for criminal and terrorist purposes, while respecting human rights (see also § 15 of the Tunis Commitment);

b) the need to build confidence and security in the use of telecommunications/ICTs by strengthening the trust framework (§ 39 of the Tunis Agenda), and the need for governments, in cooperation with other stakeholders within their respective roles, to develop necessary legislation for the investigation and prosecution of cybercrime at national levels, and cooperate at regional and international levels having regard to existing frameworks;

c) that United Nations General Assembly (UNGA) Resolution 64/211 invites Member States to use, if and when they deem appropriate, the voluntary self-assessment tool that is annexed to the resolution for national efforts;

d) the need for Member States to develop national cybersecurity programmes centred around a national plan, PPPs, a sound legal foundation, an incident management, watch, warning, response and recovery capability, and a culture of awareness, using as a guide the reports on best practices for a national approach to cybersecurity: building blocks for organizing national cybersecurity efforts;

e) that the considerable and increasing losses which users of telecommunication/ICT systems have incurred from the growing problem of cybercrime and deliberate sabotage worldwide alarm all developed and developing nations of the world without exception;

f) the reasons behind the adoption of Resolution 37 (Rev. Kigali, 2022) of this conference, on bridging the digital divide, having regard to the importance of multistakeholder implementation at the international level and to the action lines referenced in § 108 of the Tunis Agenda, including building confidence and security in the use of ICTs;

g) the outcomes of several ITU activities related to cybersecurity, especially, but not limited to, the ones coordinated by the Telecommunication Development Bureau, in order to fulfil ITU's mandate as facilitator for the implementation of Action Line C5 (Building confidence and security in the use of ICTs);

h) that various organizations from all sectors of society work in collaboration to enhance cybersecurity of telecommunications/ICTs;

i) that the fact, among others, that critical telecommunication/ICT infrastructures are interconnected at global level means that low infrastructure security in one country could result in greater vulnerability and risks in others;

j) that various information, materials, best practices and financial resources, as appropriate, are available to Member States from national, regional and other relevant international organizations, according to their respective roles;

k) that the ITU GCA encourages international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of telecommunications/ICTs;

l) that cybersecurity has become a very important issue at the international level for sustainable development, and that ITU-D, within its mandate, can continue to contribute to these efforts towards building confidence and security in the use of ICTs,

recognizing

a) that measures undertaken to ensure the stability and security of telecommunication/ICT networks, to protect against cyberthreats/cybercrime and to counter spam must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights (see also § 42 of the Tunis Agenda) and the International Covenant on Civil and Political Rights;

b) that UNGA Resolution 68/167, on the right to privacy in the digital age, affirms, *inter alia*, that ''the same rights that people have offline must also be protected on line, including the right to privacy'';

c) the need to take appropriate actions and preventive measures, as determined by law, against abusive uses of telecommunications/ICTs, as mentioned in connection with "Ethical dimensions of the information society" in the WSIS Geneva Declaration of Principles and Plan of Action (§ 43 of the Tunis Agenda), the need to counter terrorism in all its forms and manifestations on telecommunication/ICT networks, while respecting human rights and complying with other obligations under international law, as outlined in operative paragraph 81 of UNGA Resolution 60/1 on the 2005 world summit outcome, the importance of the security, continuity and stability of telecommunication/ICT networks and the need to protect telecommunication/ICT networks from threats and vulnerabilities (§ 45 of the Tunis Agenda), while ensuring respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users (§ 46 of the Tunis Agenda);

d) the need to effectively confront challenges and threats resulting from the use of telecommunications/ICTs such as 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, and to work cooperatively to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights;

e) the role of telecommunications/ICTs in the protection of children and in enhancing their development, and the need to strengthen action to protect children and youth from abuse and defend their rights in the context of telecommunications/ICTs, emphasizing that the best interests of the child are a key consideration;

f) the desire and commitment of all concerned to build a people-centred, inclusive and secure development-oriented information society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights, so that people everywhere can create, access, utilize and share information and knowledge in complete security, in order to achieve their full potential and to attain the internationally agreed development goals and objectives, including the United Nations Sustainable Development Goals (SDGs);

g) the provisions of §§ 4, 5 and 55 of the Geneva Declaration of Principles, and that freedom of expression and the free flow of information, ideas and knowledge are beneficial to development;

h) that the Tunis phase of WSIS represented a unique opportunity to raise awareness of the benefits that telecommunications/ICTs can bring to humanity and the manner in which they can transform people's activities, interaction and lives, and thus increase confidence in the future, conditional upon the secure use of telecommunications/ICTs, as the implementation of the Summit outcomes has demonstrated;

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

j) the need to deal effectively with the significant problem posed by spam, as called for in § 41 of the Tunis Agenda, as well as, *inter alia*, spam, cybercrime, viruses, worms and denial-of-service attacks;

k) the need for effective coordination within ITU-D,

noting

a) the continuing work of ITU-T Study Group 17 (Security) and other standards-development organizations on various aspects of security of telecommunications/ICTs;

b) that spam is a significant problem and continues to pose a threat for users, networks and the Internet as a whole, and that the issue of cybersecurity should be addressed at appropriate national, regional and international levels;

c) that cooperation and collaboration among Member States, Sector Members and relevant stakeholders contributes to building and maintaining a culture of cybersecurity,

resolves

1 to continue to recognize cybersecurity as one of ITU's priority activities, taking into account new and emerging telecommunication/ICT services and technologies, and to continue to address, within its area of core competence, the issue of building confidence and security in the use of telecommunications/ICTs, by raising awareness, identifying best practices, providing assistance in implementing technical measures, and developing appropriate tools and training materials in order to promote a culture of cybersecurity;

2 to enhance collaboration and cooperation with, and share information among, all relevant international and regional organizations on cybersecurity, including cyberresilience-related initiatives, within ITU's areas of competence, taking into account the need to assist developing countries,

instructs the Director of the Telecommunication Development Bureau

1 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;

2 to continue to organize, in collaboration with relevant organizations, as appropriate, taking into account member contributions, and in cooperation with the Director of the Telecommunication Standardization Bureau (TSB), meetings of Member States, Sector Members and other relevant stakeholders to discuss ways and means to enhance cybersecurity;

3 to continue, in collaboration with relevant organizations and stakeholders, to carry out studies on strengthening the cybersecurity of developing countries at the regional and international level, based on a clear identification of their needs, particularly those relating to telecommunication/ICT use, including countering and combating spam, and new and emerging telecommunication/ICT services and technologies as well as the online protection of children and youth and any vulnerable persons;

4 to consider the results of the Global Cybersecurity Index (GCI) to guide BDT cybersecurity-related initiatives, especially taking into account the gaps identified through the GCI process;

5 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;

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

7 to support Member States' initiatives, especially in developing countries, regarding mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;

8 to disseminate to the developing countries information on guidelines, recommendations, technical reports and best practices related to cybersecurity which have been developed by the ITU-T study groups, in collaboration with the Director of TSB;

9 to assist Member States, particularly developing countries, by providing guidance and best practices to overcome challenges in terms of cybersecurity and spam arising from new and emerging technologies;

10 to assist the developing countries in enhancing their states of preparedness in order to ensure a high and effective level of cybersecurity, including cyberresilience, for their critical telecommunication/ICT infrastructures, including through the holding of workshops and training to promote cyberhygiene;

11 to assist Member States in the establishment of an appropriate framework between developing countries allowing rapid response to major incidents, including promoting voluntary information-sharing between interested administrations, and propose an action plan to increase their protection and strengthen cyberresilience, taking into account mechanisms and partnerships, as appropriate;

12 to collect from Member States and share, in conjunction with the work under Question 3/2 of ITU-D Study Group 2, information regarding regulations, policies and other approaches for building confidence and security in the use of telecommunications/ICTs developed and/or implemented by national telecommunication regulatory authorities and other stakeholder organizations;

13 to facilitate the consideration by relevant ITU-D study groups of cybersecurity-related research, in collaboration with different stakeholders;

14 to encourage all relevant stakeholders to participate in the activities of the ITU Academy training centres to train, educate and raise awareness in relation to cybersecurity issues, within the framework of the GCA;

15 to assist Member States by enhancing sharing of up-to-date information on cybersecurity issues and best practices for consideration by Member States;

16 to assist developing countries with improving their capacity development by holding workshops, seminars or events, within the framework of the GCA pillars, on organizational and technical measures, in collaboration with the Director of TSB;

17 to report the results of the implementation of this resolution to the next WTDC;

18 to continue to consult with the membership on improving the GCI process, including discussion on the methodology, structure, weightage and questions, using the GCI Expert Group, as appropriate, taking into account the financial implications,

invites the Secretary-General, in coordination with the Directors of the Radiocommunication Bureau, the Telecommunication Standardization Bureau and the Telecommunication Development Bureau

1 to report on MoUs between countries, as well as existing forms of cooperation, providing analysis of their status and 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;

2 to support regional and global cybersecurity initiatives and to invite all countries, particularly developing ones, to take part in these activities;

3 to continue to mobilize ITU's development expertise with a view to strengthening national, regional and international cybersecurity in support of the SDGs, 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 remaining mindful of the need to avoid duplicating work between organizations and among the Bureaux and the General Secretariat,

requests the Secretary-General

1 to bring this resolution to the attention of the next plenipotentiary conference for consideration and required action, as appropriate;

2 to report the results of these activities to subsequent Council meetings and to plenipotentiary conferences, as appropriate,

invites Member States, Sector Members, Associates and Academia

1 to provide the necessary support for and engage actively in the implementation of this resolution;

2 to recognize cybersecurity and countering and combating spam as high-priority items, and to take appropriate action and contribute to building confidence and security in the use of telecommunications/ICTs at the national, regional and international level;

3 to encourage service providers to protect themselves from the risks identified, endeavour to ensure the continuity of services provided and notify security infringements;

4 to collaborate at the national level in order to enhance solutions to protect the cybersecurity and resilience of networks;

5 to inform ITU about existing cooperation frameworks between members and with other entities and agencies, regional or international, at the bilateral level,

invites Member States

1 to collaborate closely in order to strengthen regional and international cooperation aimed at addressing current and future issues related to cybersecurity and spam;

2 to establish an appropriate framework allowing rapid response to major incidents, and propose an action plan to prevent, mitigate and recover from such incidents;

3 to establish strategies and capabilities at the national level to ensure protection of national critical infrastructures, including enhancing the resilience of telecommunication/ICT infrastructures;

4 to foster information-sharing on cybersecurity at the national, regional and international levels.