

RESOLUTION 45 (Rev. Baku, 2025)

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

The World Telecommunication Development Conference (Baku, 2025),

recalling

- a)* Resolution 130 (Rev. Bucharest, 2022) 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. Bucharest, 2022) 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 50 (Rev. New Delhi, 2024) of the World Telecommunication Standardization Assembly (WTSA), on cybersecurity;
- f)* Resolution 52 (Rev. New Delhi, 2024) of WTSA, on countering and combating spam;
- g)* Resolution 58 (Rev. New Delhi, 2024) of WTSA, on encouraging the creation and enhancement of national computer incident response teams (CIRTs), particularly for developing countries¹;
- h)* Resolution 69 (Rev. Baku, 2025) of this conference, on facilitating the creation of CIRTs, particularly for developing countries, and cooperation among them;
- i)* Resolution 67 (Rev. Baku, 2025) of this conference, on the role of the ITU Telecommunication Development Sector (ITU-D) in child online protection;

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

- j)* Resolution 214 (Bucharest, 2022) of the Plenipotentiary Conference, on artificial intelligence (AI) technologies and telecommunications/ICTs, which establishes the scope through which the Director of the Telecommunication Development Bureau (BDT) can support the work of ITU-D in addressing the challenges and opportunities that AI gives rise to as a new and emerging technology, as it applies to cybersecurity and combating spam;
- k)* the relevant opinions of the sixth World Telecommunication Policy Forum 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 thematic priorities set out in the strategic plan for the Union in force;
- p)* the WSIS Geneva Declaration of Principles, which states in § 37: "Spam is a significant and growing problem for users, networks and the Internet as a whole. Spam and cybersecurity should be dealt with at appropriate national and international levels";
- q)* ITU-D study Question 3/2, on securing information and communication networks: best practices for developing a culture of cybersecurity;
- r)* the report of the Chair of the High-Level Group of Experts of the Global Cybersecurity Agenda (GCA), established by the ITU Secretary-General pursuant to the requirements of WSIS Action Line C5, on building confidence and security in the use of ICTs, and in accordance with Resolution 140 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on the role of ITU as lead facilitator for Action Line C5, and Resolution 58 (Rev. New Delhi, 2024), on encouraging the creation and enhancement of national CIRTs, particularly for developing countries;

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

t) 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;

u) the Global Digital Compact, adopted in Annex I to Resolution 79/1 of the United Nations General Assembly (UNGA), which set out objectives, principles, commitments and actions related to digital transformation²,

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) the existence of a cryptographically relevant quantum computer would pose a threat to some deployed cryptography used in telecommunication/ICT networks;

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

² Noting that some Member States have not endorsed the Global Digital Compact.

- e) the need for Member States to develop national cybersecurity programmes centred around a national plan, private-public partnerships, a sound legal foundation, an incident management, watch, warning, response and recovery capability, and a culture of awareness, using as a guide the several resources developed and/or made available by ITU and its membership and partners, where desirable or applicable;
- f) 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 cybersecurity 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;
- g) that the considerable and increasing losses which users of telecommunication/ICT systems have incurred from the growing problem of cybersecurity incidents, including those that are linked to the misuse of telecommunications/ICTs for malicious purposes worldwide, alarm all developed and developing nations of the world without exception;
- h) the reasons behind the adoption of Resolution 37 (Rev. Baku, 2025) 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;
- i) the outcomes of several ITU activities related to cybersecurity, especially, but not limited to, the ones coordinated by BDT, in order to fulfil ITU's mandate as facilitator for the implementation of Action Line C5;
- j) that various organizations from all sectors of society work in collaboration to enhance cybersecurity of, and build confidence in, telecommunication/ICT services and technologies;
- k) that all relevant stakeholders can play a valuable role in promoting awareness of cybersecurity issues, in particular among women, children, persons with disabilities, persons with specific needs and persons with age-related disabilities;

l) 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;

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

n) that the development of human skills and capacity building are key to enhancing cybersecurity, including the need to raise awareness and promote basic security measures for cyber hygiene that everyone, including women, children, persons with disabilities, persons with specific needs and persons with age-related disabilities, should take to protect themselves from cybersecurity risks;

o) 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;

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

q) that cybersecurity and cyber resilience have become fundamental at the national, regional and international levels for sustainable digital 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) the challenges that States, in particular developing countries, face in building confidence and security in the use of telecommunications/ICTs;

b) 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;

c) that UNGA Resolution 75/176, on the right to privacy in the digital age, affirms, *inter alia*, that the same rights that people have offline must also be protected online, including the right to privacy, with special regard given to the protection of children;

d) the need to take appropriate actions and preventive measures, as determined by law, against abusive uses of telecommunications/ICTs, as mentioned under "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 the Internet, and the need to protect the Internet and other 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);

e) the need to effectively address 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 affect the integrity of the infrastructure within States, and to work cooperatively to prevent the misuse of information resources and technologies, while respecting human rights;

f) 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;

g) 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 securely, in order to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Sustainable Development Goals (SDGs);

h) 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;

i) 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 WSIS outcomes has demonstrated;

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

k) that the manipulation of how caller information is presented when a call is received by a user is an important issue for voice spam that can arise from cybersecurity vulnerabilities that may require the application of appropriate measures and continued international cooperation among all stakeholders;

l) the need to deal effectively with the significant problem posed by spam, as called for in § 41 of the Tunis Agenda, as well as cyberattacks and cybersecurity incidents;

m) that comprehensive anti-spam mechanisms are essential to protect ICT/telecommunication users, particularly in developing countries,

noting

a) the need for effective coordination within ITU-D;

- b)* the continuing work of ITU Telecommunication Standardization Sector (ITU-T) Study Group 17 (Security) and other standards-development organizations on various aspects of security of telecommunications/ICTs;
- c)* 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;
- d)* that cooperation and collaboration among Member States, Sector Members and relevant stakeholders contributes to building and maintaining a culture of cybersecurity;
- e)* the continuing work of the private sector, academia, the technical community and all other relevant stakeholders to promote cybersecurity of the telecommunication/ICT sector;
- f)* countries may face significant new challenges and opportunities for cybersecurity and countering spam as new and emerging telecommunications/ICTs services and technologies continue to develop;
- g)* that the cybersecurity aspects of protection of data and personally identifiable information (PII) are an important issue;
- h)* that there is a need to promote the growth and development of a diverse and skilled cybersecurity workforce that is able to address and mitigate cybersecurity risks, and promote the importance of effective qualifications and professional career pathways,

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

3 to invite national and international finance organizations to pay more attention to giving substantial financial support, including through favourable credit arrangements, to national cybersecurity hard-skills programmes and training for those developing countries that lack appropriate cybersecurity hard-skills, prioritizing youth, women and persons with disabilities;

4 to continue promoting partnerships for cybersecurity capacity building, enabling ITU-D to work with other relevant stakeholders and organizations that have the expertise and knowledge in the field;

5 to continue to integrate cybersecurity considerations into all ITU-D digital development initiatives and projects,

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, including countering and combating spam;

3 to continue, in collaboration with relevant organizations and stakeholders, to carry out studies on strengthening the cybersecurity and cyber resilience of developing countries at regional and international levels, 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, and the cybersecurity aspects of protection of data and PII;

- 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 maintain 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 that 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 support Member States in identifying the basic cybersecurity measures for cyber hygiene that everyone should take to protect themselves from cybersecurity risks and spam, and to encourage and support ITU members and other stakeholders to promote those measures to the public;
- 9 to assist Member States, particularly developing countries, by sharing guidance and best practices related to the challenges and opportunities of cybersecurity and countering spam that arise from new and emerging telecommunication/ICT services and technologies;
- 10 to help raise awareness and understanding of the need to prepare for national migration to post-quantum cryptography in telecommunication/ICT networks, within the remit and expertise of ITU, and to encourage members to share good practices and national experiences in this regard;
- 11 to disseminate to developing countries information on guidelines, recommendations, technical reports and best practices related to cybersecurity which have been developed by the ITU-T study groups, particularly ITU-T Study Group 17 as lead study group on security, in collaboration with the Director of TSB;

12 to help disseminate technical ITU-T recommendations and relevant information resources developed by other organizations that can help developing countries identify and implement measures that can prevent, detect and mitigate voice spam arising from cybersecurity vulnerabilities and encourage international cooperation among all stakeholders;

13 to assist developing countries in enhancing their states of preparedness in order to ensure a high and effective level of cybersecurity, including cyber resilience, for their critical telecommunication/ICT infrastructures, including through the holding of seminars, workshops and training to promote cyber hygiene and other events, within the framework of the GCA, on organizational, technical and capacity-building measures, in collaboration with the Director of TSB, as appropriate;

14 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 cyber resilience, taking into account mechanisms and partnerships, as appropriate;

15 to collect from Member States and share, in conjunction with the work under study 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;

16 to encourage all relevant stakeholders to participate in and/or contribute to 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;

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

18 to report the results of the implementation of this resolution to the next world telecommunication development conference;

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

20 to continue to support the ITU-D Network of Women (NoW) and other initiatives to encourage active participation of women in ITU-D cybersecurity-related activities and leadership roles;

21 to develop, maintain and promote a repository of best practices on measures that facilitate and encourage people, particularly women and girls, to choose a career in cybersecurity,

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 MoUs 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

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 continue to partner with ITU-D to provide the necessary resources for the implementation of initiatives aiming to support developing countries, paying special attention to the least developed countries, landlocked developing countries and small island developing states, in the development of their cybersecurity capacities, such as through the Cyber for Good project;
- 3 to recognize cybersecurity, including the aspects related to the impact of new and emerging telecommunications/ICTs services and technologies, 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 national, regional and international levels;
- 4 to encourage service providers to protect themselves from the cybersecurity risks identified, minimize exposure to such risks, endeavour to ensure the continuity of services provided and provide notification of cybersecurity infringements, in accordance with their national laws;
- 5 to promote initiatives that encourage more people, particularly women and girls, to enter the cybersecurity profession, including through the development of relevant education and training programmes;
- 6 to contribute and share information on innovative solutions which address cybersecurity threats and counter spam;
- 7 to collaborate closely to help address the challenges and leverage the opportunities arising from new and emerging technologies for the cybersecurity of telecommunication/ICT services and technologies, and to counter spam, including through national, regional and international efforts, as appropriate;
- 8 to collaborate at the national level in order to enhance solutions to protect the cybersecurity and resilience of networks;
- 9 to inform ITU about existing cooperation frameworks between members and with other entities and agencies, regional or international, at the bilateral level;

10 to contribute to work under the relevant ITU-D study Question on cybersecurity and to other ITU-D cybersecurity-related initiatives;

11 to promote the development of educational and training programmes to enhance user awareness of cybersecurity risks, 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 from such risks;

12 to promote the development of tools and materials to enhance the cybersecurity and cyber resilience posture of small and medium enterprises;

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

14 to contribute to discussions, information sharing, capacity building and studies on the challenges and opportunities of cybersecurity and countering spam as AI technologies develop and are used in telecommunications/ICTs to enhance their efficiency and capabilities;

15 to utilize the ITU Academy for capacity building and training on new and emerging telecommunication/ICT services and technologies and related cybersecurity topics,

invites Member States

1 to survey and analyse practices in the use of new and emerging telecommunications/ICTs to counter spam;

2 to encourage all relevant stakeholders to help raise awareness among the public of cybersecurity risks, particularly among women, children, persons with disabilities, persons with specific needs and persons with age-related disabilities;

3 to participate actively in the work of ITU-D on cybersecurity and countering the spread of spam and combating spam, providing technical training sessions and workshop activities for regulators and telecommunication operators;

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

- 5 to establish strategies and capabilities at the national level to ensure protection of national critical infrastructures, including enhancing the resilience of telecommunication/ICT infrastructures;
- 6 to take steps towards developing their national cybersecurity capacities considering the pillars of the GCI, if applicable;
- 7 to foster information-sharing on cybersecurity at national, regional and international levels;
- 8 to contribute to the ITU repository of best practices on measures that facilitate and encourage more people, particularly women and girls, to choose a career in cybersecurity.