

RESOLUTION 69 (Rev. Baku, 2025)

Facilitating the creation and enhancement of national computer incident response teams, particularly for developing countries, and cooperation among them

The World Telecommunication Development Conference (Baku, 2025),

recalling

- a)* Resolutions 101, 102 and 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, which stress the need for collaboration;
- b)* Resolution 58 (Rev. New Delhi, 2024) of the World Telecommunication Standardization Assembly (WTSA), on encouraging the creation and enhancement of national computer incident response teams (CIRTs), particularly for developing countries¹;
- c)* Resolution 50 (Rev. New Delhi, 2024) of WTSA, on cybersecurity;
- d)* Resolution 214 (Bucharest, 2022) of the Plenipotentiary Conference, on artificial intelligence (AI) technologies and telecommunications/information and communication technologies (ICTs), which establishes the scope through which the Director of the Telecommunication Development Bureau (BDT) can support the work of ITU Telecommunication Development Sector (ITU-D) in addressing the challenges and opportunities that AI gives rise to as a new and emerging technology, as it applies to national CIRTs in responding to cybersecurity incidents,

recognizing

- a)* the increasing level of computer use and computer dependency in ICTs in developing countries;

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

- b)* the exposure of developing countries to cybersecurity threats and attacks targeting ICT networks, and that they could be better prepared for such cybersecurity incidents and for the increasing level of fraudulent activities by these means;
- c)* the need to improve cooperation and capacity to respond to cybersecurity challenges;
- d)* the results of work carried out to date under study Question 3/2 by ITU-D Study Group 2 and its reports on this subject, which include support for the creation and coordination of CIRTs and establishing public-private partnerships;
- e)* the work carried out to date by BDT, to bring together Member States and other stakeholders to assist countries in building national incident management capabilities, such as CIRTs;
- f)* the importance of having an appropriate level of cybersecurity emergency preparedness in all countries, particularly developing countries, by establishing CIRTs on a national basis, and the importance of coordination within and among the regions and of taking advantage of regional and international initiatives in this regard, including ITU cooperation with regional and global projects and organizations, such as the Forum of Incident Response and Security Teams (FIRST), the Organization of American States and the Asia-Pacific Computer Emergency Response Team, among others;
- g)* that emerging telecommunications/ICTs are being applied as part of technical measures against cybersecurity attacks and threats;
- h)* the relevant work of Study Group 17 of the ITU Telecommunication Standardization Sector (ITU-T), including cybersecurity information-sharing techniques;
- i)* that countries may benefit from coordination between national sectoral CIRTs, where present, to enhance incident management during major cybersecurity incidents with domestic cross-sectoral impact;
- j)* the outcomes of ITU-D efforts on national CIRT assessment, design, establishment, enhancement and collaboration,

noting

- a) that there is an improved, but still low, level of cybersecurity emergency preparedness within developing countries;
- b) that the high level of interconnectivity of telecommunication/ICT networks could be affected by cybersecurity attacks and threats from networks of less-prepared nations, which are mostly developing countries;
- c) countries may face significant new challenges and opportunities in responding to cybersecurity incidents, as new and emerging telecommunication/ICTs services and technologies continue to develop;
- d) *considering i)* of Resolution 130 (Rev. Bucharest, 2022), which states 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 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;
- e) that the establishment and enhancement of CIRTs requires ongoing and appropriate resourcing in order to be successful and sustainable;
- f) the work of ITU-T Study Group 17 in the area of national CIRTs, particularly for developing countries, and cooperation between them, as contained in the outputs of that study group;
- g) the need for the establishment of CIRTs on a national basis, as appropriate, including CIRTs responsible for government-to-government cooperation, and the importance of coordination among all relevant organizations;
- h) the ITU Global Cybersecurity Agenda (GCA) and the guidelines for utilization of the GCA as approved by the ITU Council;

- i) the increasing use of new and emerging telecommunications/ICTs in all aspects of life, including digitalization of government services, which need to be highly protected;
- j) that CIRTs can help address the urgent need to enhance security and build confidence and trust in the use of ICTs,

resolves

- 1 to facilitate the creation and enhancement of national CIRTs in Member States where support is requested, as appropriate, within existing budgetary resources;
- 2 to encourage ITU-D to continue its work on national CIRT assessment, design, establishment, enhancement and collaboration,

instructs the Director of the Telecommunication Development Bureau

- 1 to promote national, regional and international best practices for establishing and enhancing CIRTs and information sharing and analysis centres (ISACs), as identified to date by the relevant ITU study groups, such as ITU-D Study Group 2 under Question 3/2 and ITU-T Study Group 17, and by other relevant organizations and experts;
- 2 to provide national CIRTs with capacity development, particularly in areas of new and emerging telecommunication/ICT services and technologies, through the ITU regional and area offices, including support for continuous maturity assessments, taking into account the financial resources;
- 3 to support national CIRTs, particularly those in developing countries, by sharing guidance and best practices related to the challenges and opportunities of responding to cybersecurity incidents arising from new and emerging telecommunication/ICT services and technologies;
- 4 to support national CIRTs in enhancing information sharing and collaboration, and in sharing best practices for cybersecurity incident response, aiming to elevate the level of cybersecurity emergency preparedness, particularly in developing countries globally;
- 5 to promote the related operating frameworks of CIRTs in Member States where CIRTs are established, if applicable;

6 to continue to mobilize resources to promote the training programmes necessary in this field, including tiered learning pathways (introductory, intermediate and advanced) to enable progressive capacity building, and continuing to provide support as appropriate to those developing countries that so wish;

7 to promote best practices in establishing a national structure that can coordinate between national sectoral CIRTs, where present, and enhance incident management during significant cybersecurity incidents with domestic cross-sectoral impact;

8 to continue promoting collaboration between and among national CIRTs, including CIRTs responsible for government-to-government cooperation, industry CIRTs and academia CIRTs, in accordance with national legislation, at the regional and global level, by encouraging the participation of developing countries in regional and global projects and in the work of relevant organizations such as FIRST, and regional organizations, among others;

9 to work to achieve these goals while avoiding duplication of effort with other organizations;

10 to continue to develop programmes on awareness-raising campaigns on the importance of creation and enhancement of CIRTs to elevate the level of cybersecurity posture;

11 to continue enhancing existing toolkits which developing countries may utilize to conduct incident response table-top exercises or drills,

invites Member States

1 to establish national CIRTs, including CIRTs responsible for government-to-government cooperation, where needed or currently lacking, as appropriate;

2 to enhance the maturity, capability and resilience of established national CIRTs to address evolving cybersecurity threats effectively;

3 to contribute to the development of an informational resource platform, based on the provisions of Council Decision 630 (C23), that includes and maintains a repository of best practices for creating and operating national CIRTs;

4 to collaborate closely with ITU-D, ITU-T and other relevant organizations, taking into consideration Resolution 58 (Rev. New Delhi, 2024) in this regard, as appropriate;

5 to promote and facilitate the exchange of best practices among their national CIRTs, including participation in relevant CIRT initiatives, such as FIRST;

6 to encourage the use of new and emerging telecommunications/ICTs to enhance technical capabilities of CIRTs;

7 to consider, where appropriate, establishing a national structure for coordination between national sectoral CIRTs, where present, in order to enhance incident management during major cybersecurity incidents with domestic cross-sectoral impact;

8 to encourage, on a voluntary basis, sharing of information on cybersecurity vulnerabilities and threats among Member States, including through existing information-sharing platforms;

9 to raise their needs with the ITU regional and area offices,

invites Sector Members, Associates and Academia, as appropriate

1 to contribute to the creation and enhancement of national CIRTs, particularly for developing countries;

2 to support capacity-building initiatives on new and emerging telecommunication/ICT services and technologies by national CIRTs, particularly for developing countries;

3 to contribute to discussions, information sharing, capacity building and studies on the challenges and opportunities faced by national CIRTs in responding to cybersecurity incidents as AI technologies continue to develop and be used in telecommunications/ICTs to enhance their efficiency and capabilities.