RESOLUTION 69 (Rev. Buenos Aires, 2017)

Facilitating creation of national computer incident response teams, particularly for developing countries[1], and cooperation between them

The World Telecommunication Development Conference (Buenos Aires, 2017),

recalling

a) Resolutions 101, 102 and 130 (Rev. Busan, 2014) of the Plenipotentiary Conference, which stress the need for collaboration;

b) Resolution 69 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC), and the need to improve coordination and capacity to respond to cybersecurity challenges;

c) Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly (WTSA), on encouraging the creation of national computer incident response teams (CIRTs), particularly in developing countries;

d) Resolution 50 (Rev. Hammamet, 2016) of WTSA, on cybersecurity,

recognizing

a) the highly satisfactory results obtained by the regional approach adopted within the framework of Resolution 69 (Rev. Dubai, 2014);

b) the increasing level of computer use and computer dependency in information and communication technologies (ICT) in developing countries;

---

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

c) the exposure of developing countries to attacks and threats targeting ICT networks, and that they could be better prepared for such attacks and threats and for the increasing level of fraudulent activity by these means;

d) the results of the work carried out to date under Question 3/2 by Study Group 2 of the ITU Telecommunication Development Sector (ITU-D) and its reports and coursework on this subject, which include support for the creation of CIRTs and establishing public-private partnerships;

e) the work carried out to date by the Telecommunication Development Bureau (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 computer 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 (OAS) and the Asia-Pacific Computer Emergency Response Team (APCERT), among others;

g) the work of Study Group 17 of the ITU Telecommunication Standardization Sector (ITU-T) on cybersecurity information exchange (CYBEX) techniques,

noting

a) that there is an improved, but still low, level of computer emergency preparedness within developing countries;

b) that the high level of interconnectivity of telecommunication/ICT networks could be affected by the launch of an attack from networks of the less-prepared nations, which are mostly the developing countries;

c) *considering f)* in Resolution 130 (Rev. Busan, 2014), 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;

d) the importance of having an appropriate level of computer emergency preparedness in all countries;

e) 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;

f) the need for the establishment of CIRTs on a national basis, including CIRTs responsible for government-to-government cooperation, and the importance of coordination among all relevant organizations;

g) the ITU Global Cybersecurity Agenda,

resolves

1 to invite Member States and Sector Members with experience in this area:

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

- to collaborate closely with relevant organizations, and ITU-T, in this regard, taking into consideration Resolution 58 (Rev. Dubai, 2012);

- to facilitate exchanging best practices among their national CIRTs;

2 to instruct the Director of BDT to give the necessary priority to this, by:

- promoting national, regional and international best practices for establishing CIRTs, as identified to date by the relevant ITU study groups, such as ITU-D Study Group 1 under past Question 22-1/1, and by other relevant organizations and experts;

- preparing the training programmes necessary for this purpose and continuing to provide support as required to those developing countries that so wish;

- 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 organizations such as FIRST, OAS and APCERT, among others;

- working to achieve these goals while avoiding duplication of effort with other organizations;

3 to instruct ITU-D Study Group 2, under Question 3/2, within its mandate, to contribute to the implementation of this resolution, also taking into consideration the work carried out by ITU-T on this issue.