QUESTION 3/2

Securing information and communication networks: Best practices for developing a culture of cybersecurity

1 Statement of the situation or problem

Securing information and communication networks and developing a culture of cybersecurity have become key in today's world for a number of reasons, including:

a) the explosive growth in the deployment and use of information and communication technology (ICT);

b) cybersecurity remains a concern of all and there is thus a need to assist countries, in particular developing countries, to protect their telecommunication/ICT networks against cyberattacks and threats;

c) the need to endeavour to ensure the security of these globally interconnected infrastructures if the potential of the information society is to be achieved;

d) the growing recognition at the national, regional and international levels of the need to develop and promote best practices, standards, technical guidelines and procedures to reduce vulnerabilities of and threats to ICT networks;

e) the need for national action and regional and international cooperation to build a global culture of cybersecurity that includes national coordination, appropriate national legal infrastructures, and watch, warning and recovery capabilities, government/industry partnerships, and outreach to civil society and consumers;

f) the requirement for a multistakeholder approach to effectively make use of the variety of tools available to build confidence in the use of ICT networks;

g) United Nations General Assembly (UNGA) Resolution 57/239, on creation of a global culture of cybersecurity, invites Member States "to develop throughout their societies a culture of cybersecurity in the application and use of information technology";

h) 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 online, including the right to privacy";

i) best practices in cybersecurity must protect and respect the rights of privacy and freedom of expression as set forth in the relevant parts of the Universal Declaration of Human Rights, the Geneva Declaration of Principles adopted by the World Summit on the Information Society (WSIS) and other relevant international human rights instruments;

j) the Geneva Declaration of Principles indicates that "A global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies", the Geneva Plan of Action encourages sharing best practices and taking appropriate action on spam at national and international levels, and the Tunis Agenda for the Information Society reaffirms the necessity for a global culture of cybersecurity, particularly under Action Line C5 (Building confidence and security in the use of ICTs);

k) ITU was requested by WSIS (Tunis, 2005), in its agenda for the implementation and follow-up, to be the lead facilitator/moderator for Action Line C5 (Building confidence and security in the use of ICTs), and ITU-T, ITU-R, ITU-D and the General Secretariat, based on such responsibility and in response to relevant resolutions adopted by the World Telecommunication Development Conference (WTDC) (Doha, 2006 and Hyderabad, 2010), by the Plenipotentiary Conference (Antalya, 2006 and Guadalajara, 2010), as well as by the

World Telecommunication Standardization Assembly (Johannesburg, 2008 and Dubai, 2012), have carried out many studies in order to improve cybersecurity;

l) WSIS outputs (both phases: Geneva, 2003 and Tunis, 2005) called for building confidence and security in the use of ICTs;

m) WTDC Resolution 45 (Rev. Dubai, 2014) supported the enhancement of cybersecurity among interested Member States;

n) consistent with its mandate, ITU-D should play a role in bringing together Member States, Sector Members and other experts to share experiences and expertise for securing ICT networks;

o) the results of Question 22-1/1 in the past study period, which include numerous reports, and contributions from across the globe;

p) there have been various efforts to facilitate the improvement of network security, including the work of Member States and Sector Members in standards-setting activities in ITU-T and in the development of best-practice reports in ITU-D; by the ITU secretariat in the Global Cybersecurity Agenda (GCA); and by ITU-D in its capacity-building activities in the relevant programme; and, in certain cases, by experts across the globe;

q) governments, service providers and end-users, particularly in least developed countries (LDCs), face unique challenges in developing security policies and approaches appropriate to their circumstances;

r) Member States and infrastructure operators would benefit from additional reports detailing the various resources, strategies and tools available to build confidence in the use of ICT networks and the role of international cooperation in this regard;

s) spam continues to be a serious concern;

t) evolving methodologies on common testing criteria for telecommunication networks;

u) the need for simplified test procedures at basic level for security testing of telecommunication networks to promote a security culture.

2 Question or issues for study

a) Discuss approaches and best practices for evaluating the impact of spam within a network, and provide the necessary measures, including mitigation techniques, that developing countries can use, taking into account existing standards and available tools.

b) Provide information on current cybersecurity challenges that service providers, regulatory agencies and other relevant parties are facing.

c) Continue to gather national experiences from Member States relating to cybersecurity, and to identify and examine common themes within those experiences.

d) Continue to analyse results of the cybersecurity awareness survey carried out in the last study period, and issue an updated survey so as to measure progress over time.

e) Provide a compendium of relevant, ongoing cybersecurity activities being conducted by Member States, organizations, the private sector and civil society at the national, regional and international levels, in which developing countries and all sectors may participate, including information gathered under c) above.

f) Examine specific needs of persons with disabilities, in coordination with other relevant Questions.

g) Examine ways and means to assist developing countries, with the focus on LDCs, in regard to cybersecurity-related challenges.

h) Continue to gather national experiences and national requirements in the area of child online protection, in coordination with other relevant activities.

i) Hold ad hoc sessions, seminars and workshops to share knowledge, information and best practices concerning effective, efficient and useful measures and activities to enhance cybersecurity, using outcomes of the study, to be collocated as far as possible with meetings of Study Group 1 or of the rapporteur group for the Question.

j) Gather national experience and requirements on common criteria and security testing that would facilitate the development of a framework and guidelines that could speed up the security testing of telecommunication equipment, in collaboration with the relevant ITU-T study groups and other standards-developing organizations (SDOs), as appropriate, and taking into account available information and material in these entities.

3 Expected output

1 Reports to the membership on the issues identified in § 2 a) to j) above. The reports in question will reflect that secure information and communication networks are integral to building of the information society and to the economic and social development of all nations. Cybersecurity challenges include potential unauthorized access to, destruction of and modification of information transmitted on ICT networks, as well as countering and combating spam. However, the consequences of such challenges can be mitigated by increasing awareness of cybersecurity issues, establishing effective public-private partnerships and sharing successful best practices employed by policy-makers and businesses, and through collaborating with other stakeholders. In addition, a culture of cybersecurity can promote trust and confidence in these networks, stimulate secure usage, ensure protection of data and privacy while enhancing access and trade, and enable nations to better achieve the economic and social development benefits of the information society.

2 Educational materials for use in workshops, seminars, etc.

3 Accumulation of knowledge, information and best practices on effective, efficient and useful measures and activities to enhance cybersecurity in developing countries resulting from ad hoc sessions, seminars and workshops.

4 Timing

This study is proposed to last four years, with preliminary status reports to be delivered on progress made after 12, 24 and 36 months.

5 Proposers/sponsors

ITU-D Study Group 1; Arab States; Inter-American proposal; Japan; Islamic Republic of Iran.

6 Sources of input

a) Member States and Sector Members

b) Relevant ITU-T and ITU-R study group work

c) Relevant outputs of international and regional organizations

d) Relevant non-governmental organizations concerned with the promotion of cybersecurity and a culture of security

e) Surveys, online resources

f) Experts in the field of cybersecurity

g) Other sources, as appropriate.

7 Target audience

Target audience	Developed countries	Developing countries[1]
Telecom policy-makers	Yes	Yes
Telecom regulators	Yes	Yes
Service providers/operators	Yes	Yes
Manufacturers	Yes	Yes

a) Target audience

National policy-makers and Sector Members, and other stakeholders involved in or responsible for cybersecurity activities, especially those from developing counties.

b) Proposed methods for implementation of the results

The study programme focuses on gathering information and best practices. It is intended to be informative in nature and can be used to raise awareness for Member States and Sector Members of the issues of cybersecurity and to draw attention to the information, tools and best practices available, the results of which may be used in conjunction with BDT-organized ad hoc sessions, seminars and workshops.

8 Proposed methods of handling the Question or issue

The Question will be addressed within a study group over a four-year study period (with submission of interim results), and will be managed by a rapporteur and vice-rapporteurs. This will enable Member States and Sector Members to contribute their experiences and lessons learned with respect to cybersecurity.

9 Coordination

Coordination with ITU-T, in particular Study Group 17 or its successor, ITU-D Question 7/1 on persons with disabilities, as well as other relevant organizations, including FIRST, IMPACT, APCERT, OAS CICTE, OECD, RIRs, NOGs, M3AAWG and others. Given the existing level of technical expertise on the issue in these groups, all documents (questionnaires, interim reports, draft final reports, etc.) should be sent to them for comment and input prior to being submitted to the full ITU-D study group for comment and approval.

10 BDT programme link

The BDT programme under Output 3.1 of Objective 3 shall facilitate exchange of information and make use of the output, as appropriate, to satisfy programme goals and the needs of Member States.

11 Other relevant information

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