Buenos Aires Action Plan

STUDY GROUP 2

QUESTION 3/2

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

1 Statement of the situation or problem

The use of telecommunications and information and communication technologies (ICTs) has been invaluable in fostering development and social and economic growth globally. However, despite all the benefits and uses these technologies offer, there are risks and threats to security.

From personal finances to business operations, national infrastructure and public and private services, all transactions are increasingly managed through information and communication networks, making them more vulnerable to some form of attack.

In order to build trust in the use and application of telecommunications/ICTs for applications and content of all kinds, especially those having a major positive impact in economic and social areas where all players exert an effect on the protection of personal data, network security and the actual network user, close collaboration is required between national authorities, foreign authorities, industry, academia and users.

Based on the foregoing, 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 ICT;

b) cybersecurity remains a matter of concern of all, and there is thus a need to assist countries, in particular developing countries[1], 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, 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;

---

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

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 Resolutions 68/167, 69/166 and 71/199, on the right to privacy in the digital age, affirm, *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 implementation and follow-up, to be the lead facilitator/moderator for Action Line C5 (Building confidence and security in the use of ICTs), and relevant resolutions have been adopted by the Plenipotentiary Conference, the World Telecommunication Standardization Assembly (WTSA) and the World Telecommunication Development Conference (WTDC);

l) UNGA Resolution 70/125 adopted the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the WSIS outcomes;

m) the WSIS+10 Statement on the implementation of WSIS outcomes, and the WSIS+10 vision for WSIS beyond 2015, adopted at the ITU-coordinated WSIS+10 high-level event (Geneva, 2014) and endorsed by the Plenipotentiary Conference (Busan, 2014), which were submitted as an input into the UNGA's overall review on the implementation of WSIS outcomes;

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

o) Resolution 130 (Rev. Busan, 2014) of the Plenipotentiary Conference resolves to continue promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at the national, regional and international level;

p) WTSA Resolution 50 (Rev. Hammamet, 2016), highlights the need to harden and defend information and telecommunication systems from cyberthreats and cyberattacks, and continue to promote cooperation among appropriate international and regional organizations in order to enhance exchange of technical information in the field of information and telecommunication network security;

q) the conclusions and recommendations set out in ITU Telecommunication Development Sector (ITU-D) Study Group 2's final report on Question 3/2, to the effect that the activities in the current terms of reference be continued and that evolving and emerging technical threats beyond spam and malware be considered for the next study period;

r) 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 the ITU Telecommunication Standardization Sector (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 under the relevant programme; and, in certain cases, by experts across the globe;

s) 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;

t) 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 are beneficial for all stakeholders;

u) spam and malware continue to be a serious concern, although evolving and emerging threats must also be studied;

v) 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 to foster the confidentiality, integrity and availability of ICT systems.

b) Discuss approaches and best practices for evaluating the impact of spam and malware within a network, as well as evolving and emerging threats, and provide the necessary input for measures and guidelines, including mitigation techniques and legislative and regulatory aspects that countries can use, taking into account existing standards and available tools.

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

d) Continue to gather national experiences from Member States relating to cybersecurity and child online protection and to identify and examine common themes within those experiences, using that information to provide input for guidelines to assist Member States in developing effective mechanisms for security in the digital environment.

e) Analyse the cybersecurity challenges facing emerging technologies such as Internet of Things (IoT) and artificial intelligence (AI), etc., and measures to address those challenges.

f) Share perspectives regarding how cybersecurity supports the protection of personal data.

g) Promote awareness-raising for users and capacity building regarding cybersecurity.

h) 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 d) above.

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

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

k) Foster cooperation between the players involved with a view to holding ad hoc sessions, seminars and workshops to share knowledge, information and best practices concerning effective, efficient and useful measures and activities to enhance cybersecurity, increase confidence and protect data and networks, taking into consideration existing and potential risks for ICTs, using outcomes of the study, to be collocated as far as possible with meetings of ITU-D Study Group 2 or of the rapporteur group for the Question.

l) Work in collaboration with the relevant ITU-T study groups and other standards-development organizations (SDOs), as appropriate, and taking into account information and material available in these entities.

m) Provide guidance on measures to combat spam and malware at national, regional and international level.

n) Collect and share information regarding regulatory policies developed and/or implemented by national competent authorities to build confidence and security in the telecommunication/ICT sector.

3 Expected output

a) Reports to the membership on the issues identified in § 2 a) to n) above. The reports in question will reflect that secure information and communication networks are integral to building the information society and to ensuring the economic and social development of all nations. They will also provide contributions that assist countries in formulating guidelines to address cybersecurity challenges.

Cybersecurity challenges include potential unauthorized access to, destruction of and modification of information transmitted on ICT networks, as well as countering and combating spam and malware. 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 collaboration with other stakeholders.

In addition, a culture of cybersecurity can promote trust and confidence in these networks, stimulate secure usage, ensure protection of data, including personal data, while enhancing access and trade, and enabling nations to achieve the economic and social development benefits of the information society more effectively.

b) Educational materials for use in workshops, seminars, etc.

c) 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 2, Arab States, Inter-American proposal, Japan, and the 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) Global Cybersecurity Index (GCI)

h) Other sources, as appropriate.

7 Target audience

Target audience	Developed countries	Developing countries
Telecom policy-makers	Yes	Yes
Telecom regulators	Yes	Yes
Service providers/operators	Yes	Yes
Manufacturers	Yes	Yes
Academia	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 of cybersecurity issues in Member States and Sector Members 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 is required with ITU-T, in particular ITU-T Study Group 17, which is responsible for building confidence and security in the use of ICTs. Coordination should also include other relevant organizations with expertise in the issue, such as FIRST, APCERT, OAS CICTE, OECD, RIRs, NGOs, M3AAWG, ISOC, GFCE and UCENET. Given the existing level of technical expertise on the issue in these groups, they should be given the opportunity to comment and provide input on all documents (questionnaires, interim reports, draft final reports, etc.) before the documents are submitted to the full ITU-D study group for comment and approval.

10 BDT programme link

The BDT programme under Objective 2 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

–