Council 2014
Geneva, 6-15 May 2014

Agenda item: PL 1.1

Document C14/23-E
10 February 2014
Original: English

Report by the Secretary-General

ITU ACTIVITIES ON STRENGTHENING THE ROLE OF ITU IN BUILDING CONFIDENCE AND SECURITY IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Summary

This Report summarizes ITU's activities and initiatives since Council 2013 in relation to Resolution 130 (Rev. Guadalajara, 2010), ITU's role as sole facilitator for WSIS Action Line C5, and other decisions by the membership on strengthening the role of ITU in building confidence and security in the use of information and communication technologies (ICTs).

Action required

The Council is invited **to note** the activities described below.

_____

References

Resolution 71 (Rev. Guadalajara, 2010), *Resolution 130 (Rev. Guadalajara, 2010)*, *Resolution 174 (Guadalajara, 2010)*, *Resolution 181 (Guadalajara, 2010)*, *Resolution 140 (Rev. Guadalajara, 2010)*, *Resolution 179 (Guadalajara, 2010)*, *International Telecommunication Regulations (rev. Dubai, 2012)*, Council *Resolution 1282 (2007)*, *Resolution 1306 (2009)*, WTDC-10 Res. 2 and *45*, WTDC-10/HAP *Programme 2*, WTSA-12 *Res. 50*, *52* and *75*, ITU-T *Rec. X. 500*, ITU-T *Rec. X.509*, ITU-T Rec. X.1000 series, ITU-T X.8xx series Recs, ITU-T *Recs X.1121*, *X.1205*, *X.1231*, *X.1240*, *X.1241*, Recs. ITU-R *M.1078*, *M.1223*, *M.1457*, *M.1645*, *M.2012*, *S.1250*, *S.1711*, Council Documents *C05/32*, *C05/EP/10*, *C06/4*, *C07/21*, *C08/33*, *C09/50*, *C10/12*, *C11/54*, *C12/29*, *C13/23*

1. Cybersecurity and Countering Spam Activities

1.1 This report, organized around the five pillars of the Global Cybersecurity Agenda (GCA), shows the complementary nature of existing ITU work programmes and facilitates the implementation of BDT, TSB and BR activities in this domain.

2. Legal Measures

2.1 As part of Programme 2 of the Hyderabad Action Plan, and taking into account ITU-D Q22/1, ITU is assisting Member States in understanding the legal aspects of cybersecurity through its ITU Cybercrime Legislation Resources, in order to help harmonize their legal frameworks.

2.2 Within the framework of the European Commission project (Support for the Establishment of Harmonized Policies for the ICT Market in the African, Caribbean and Pacific islands (ACP) regions), and in close collaboration with work under Programme 2, BDT has undertaken activities aimed at facilitating the harmonization of cybersecurity-related legislation at the regional level. Completed in September 2013, the three sub-projects covered around 60 countries in the ACP regions.

2.3 BDT has developed a publically available database with individual country profiles on the current status of cybersecurity frameworks and policies at the national level, including information on cybersecurity laws, national strategies, and establishment of Computer Incident Response Teams (CIRTs).

3. Technical and Procedural Measures

3.1 ITU-T Study Group 17 (SG-17), the lead study group on security and identity management (IdM), continues to be instrumental in study and standardization in the areas of cybersecurity, anti-spam, IdM, X.509 certificates, information security management, ubiquitous sensors networks, telebiometrics, IPTV security, virtualization security towards cloud computing security, and security architecture and application security, often in cooperation with external Standards Developing Organizations and Consortia.

3.2 SG-17 approved seven Recommendations on cybersecurity: ITU-T X.1208 "A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies", X.1210 "Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks", revised X.1520 "Common vulnerabilities and exposures", revised X.1526 "Language for the open definition of vulnerabilities and for the assessment of a system state", X.1544 "Common attack pattern enumeration and classification", X.1546 "Malware attribute enumeration and characterization", X.1582 "Transport protocols supporting cybersecurity information exchange", and X.1601 "Security framework for cloud computing". Draft Rec. ITU-T X.1211 "Guideline on techniques to prevent web-based attacks" was determined, and draft Rec. ITU-T X.1303bis "Common alerting protocol (CAP 1.2)" was consented to.

3.3 New work has started on a technical framework for countering mobile messaging spam, on a security capability requirements framework for countering smartphone-based botnets, on information security controls for cloud computing, and on certified mail transport and certified post office protocols.

3.4 ITU-R's work in radiocommunication standardization continues, matching the constant evolution in modern telecommunication networks. ITU-R established clear security principles for IMT (3G and 4G) networks (Recommendations ITU-R M.1078, M.1223, M.1457, M.1645 and M.2012). It has also issued recommendations on security issues in network management architecture for digital satellite systems (Recommendation ITU-R S.1250) and performance enhancements of transmission control protocol over satellite networks (Recommendation ITU-R S.1711).

4. Organizational Structures

4.1 ITU, in partnership with IMPACT, continues to deploy capabilities to build capacity at regional and international levels. ITU–IMPACT has undertaken technical assessments to evaluate the preparedness for the establishment of CIRTs in 50 countries and is continuing with the necessary follow-up actions. CIRT establishment is currently underway in Jamaica, Ghana, Burundi, Tanzania, Côte d'Ivoire, Barbados and Cyprus. Training for Burkina Faso on CIRT operations was carried out in June and July 2013. Technical assistance on CIRT and National strategies were provided to Monaco, Cyprus and Rwanda during the period of September-December 2013.

4.2 In collaboration with IMPACT, ITU conducts Cyber Drills for its partner countries to enhance the communication and incident response capabilities of participating teams, and to strengthen national and international cooperation against cyber threats. So far, ITU–IMPACT has conducted Cyber Drills for more than 50 countries. In the current reporting period, a Cyber Drill was held for the Latin America region in Montevideo, Uruguay, from 26 to 29 August 2013 and for the Arab Region in Muscat, Oman, from 27 to 28 October 2013. Cyber Drills for Europe and the America Region are planned for the first semester of 2014.

4.3 In July 2013, ITU signed a Memorandum of Understanding (MoU) with the Nigerian Communication Commission to set up a Regional Cybersecurity Centre to facilitate collaboration on combating cyber threats at the regional and national levels – with an emphasis on protecting children online.

5. Capacity Building

5.1 ITU regularly organizes regional cybersecurity forums for all ITU regions, using these as a capacity-building vehicle for different ITU-D programmes and activities as well as an operational platform for cooperation at the regional and international level.

5.2 ITU–IMPACT's Training and Skills Development Centre conducts high-level briefings for representatives of Member States, providing invaluable exposure and privileged private sector insight on latest trends, potential threats and emerging technologies. Over 2700 cybersecurity professionals have been trained and 360 scholarships have been provided to over 49 Member States globally.

5.3 BDT launched the LDC Project to enhance the cybersecurity capacity, capability, readiness, skills and knowledge of the 49 UN-designated Least Developed Countries. In its current stage, the project aims to lay the foundation for the execution of the Least Developed Country Infrastructure Protection Program (LDCIPP) by engaging the 49 targeted countries and defining the LDCIPP's framework (stages, strategies, activities, timeframe, and expected outcomes). The secondary objective is to raise funds among interested stakeholders, making available the necessary capital to execute the LDCIPP.

5.4 ITU organized a workshop on countering and combating spam in Durban, South Africa for the African region on 8 July 2013. Ninety participants from governments and industry from 20 countries participated in the workshop, which explored the various dimensions of the problem of spam.

6. International Cooperation

6.1 Further reinforcing efforts in fostering international cooperation, ITU's work and relationship with IMPACT continue to gain momentum. As of today, 149 countries have joined the ITU–IMPACT collaboration.

6.2 ITU is also developing relationships and partnerships with various regional and international organizations and initiatives including the Commonwealth Cybercrime Initiative, the CyberLympics, the European Union Agency for Network and Information Security (ENISA) and the Forum for Incident Response Team (FIRST). ITU signed a cooperation agreement with FIRST in January 2014 which would facilitate the FIRST affiliation of newly established CIRTs.

6.3 ITU signed a cooperation agreement with Trend Micro at ITU Telecom World 2013 under which Trend Micro would provide current and forward looking analysis on cyber threats to be shared with all Member States. ITU also continues its release of Symantec Threat Intelligence Reports, complemented with a technical executive summary, to inform Member States and to increase their understanding and readiness of the latest cyber threats and risks.

6.4 In its role as the lead facilitator for WSIS Action Line C5, ITU organized several events at the WSIS Forum 2013 that facilitated sharing of experiences among all stakeholder groups in the global effort towards promoting confidence and security in the use of ICTs. Secretariat services were also provided to the Multistakeholder Preparatory Process for the WSIS+10 High-level Event. These included, *inter alia*, the provision of information (including preparation of relevant documents) upon request by the group.

6.6 The Republic of Azerbaijan organized an international conference titled "Global Cybersecurity Cooperation: Challenges and Visions", on 2-3 December 2013 in Baku with the support of ITU in partnership with Interpol, the World Bank and the World Economic Forum. The conference brought together around 200 high-level delegates from different stakeholder groups to discuss global cybersecurity-related issues.

6.7 At the request of the United Nations System Chief Executives Board for Coordination (CEB), ITU, in collaboration with the United Nations Office on Drugs and Crime (UNODC) and some 35 UN agencies, developed a UN-wide framework on Cybersecurity and Cybercrime, which was endorsed by the CEB at its Second Regular Session for 2013 in November 2013. The CEB has requested ITU, UNESCO, UNODC, UNDP, and UNCTAD, in close coordination with HLCP, HLCM and UNDG, to develop a system-wide comprehensive and coherent strategy for addressing the issue, for discussion at CEB's Second Regular Session of 2014.

6.8 ITU is leading the Global Cybersecurity Index (GCI) project to rank the cybersecurity capabilities of nation states. The objective is to publish six regional indices, eventually constituting one global index. The GCI project is a joint effort between the ITU and ABI Research. The Global Cybersecurity Index was launched at ITU Telecom World in November 2013 with the first results from the Arab region.

6.9 Cybersecurity was a key theme of ITU Telecom World 2013. A separate Cybersecurity Pavilion was established with the active participation of governments and major private sector entities. Activities at the pavilion highlighted the critical, wide-ranging and truly global nature of the security issues the world is facing and focused on how the international community can best deal with them.

7. Child Online Protection (COP)

7.1 In July 2013, the First Lady of Nigeria, Dame Patience Jonathan, was formally appointed as Champion for Child Online Protection.

7.2 The COP Initiative is currently in the process of updating the COP Guidelines for Industry. The drafting process involved COP partners from all stakeholder groups, with UNICEF assuming editorial responsibility. Open consultations (online and at IGF 2013) were conducted by ITU and UNICEF with all stakeholders in order to collect views on the draft guidelines (expected to be ready in mid-2014).

7.3 The Joint Coordination Activity on Child Online Protection (JCA-COP) continues its work under SG-17, with three virtual meetings held since the last reporting period. Issues discussed include standards for age verification for enhancing IdM best practices, and approaches of voluntary regulation by Industry.

7.4 In June 2013, ITU, in partnership with the Commonwealth Telecommunication Organization (CTO), organized a workshop in Cameroon to present work on the establishment of COP National Frameworks in six countries – Nigeria, Ghana, Sierra Leone, Gambia, Mauritius and Cameroon.

7.5 Continuing efforts towards establishing efficient and cost-effective methods of fighting against online child sexual abuse content, in June 2013, ITU sponsored a pilot project with the Internet Watch Foundation (IWF) to assess the establishment of a hotline in Uganda.

7.6 In August 2013, ITU established a partnership with the African Child Online Protection Education and Awareness Centre (ACOPEA) and Facebook to run a pilot exercise to train 100 safety ambassadors from government, law enforcement and educators from 25 schools across Addis Ababa. Spot messages promoting online safety for children and young people were developed under the banner ''Click Safe, Click Clever''. An estimated 15,000 children will have seen the safety messages by the end of the pilot in January 2014.

7.7 Under the patronage of the President of Costa Rica, in September 2013, ITU organized the Global Youth Summit: BYND 2015. The purpose of the Summit was to convene young people, both online and offline, to participate in a discussion on how to ensure that technology is used for good, specifically to shape the post-2015 agenda. Child online safety was defined as a priority area by the participants of the BE SAFE & BE SMART track, organized by ITU, along with The Walt Disney Company and UNICEF.

7.8 The proposed Africa Child Online Protection (ACOP) Summit to be held in Kampala, Uganda, has been postponed (revised schedule is currently under discussion).