|  |  |
| --- | --- |
| **Council 2017 Geneva, 15-25 May 2017** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.5** | **Document C17/18-E** |
| **14 March 2017** |
| **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 since Council 2016 in relation to Resolution 130 (Rev. Busan, 2014), 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 report.  \_\_\_\_\_\_\_\_\_\_\_\_  References  *Plenipotentiary Resolutions* [*71*](http://www.itu.int/en/council/planning/Documents/PP-14_Res71.pdf)*,* [*130*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf)*,* [*140*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20140.pdf)*,* [*174*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20174.pdf), [*179*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20179.pdf) *(Rev. Busan, 2014),* [*181*](http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf) *(Guadalajara, 2010),* [*International Telecommunication Regulations*](http://www.itu.int/pub/S-CONF-WCIT-2012/en) *(Rev. Dubai, 2012), Council* [*Resolution 1306*](https://www.itu.int/md/S15-CL-C-0109/en)*, WTDC Resolutions* [*2*](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf) *,*[*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf)*,* [*67*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/67revDubai.pdf)*,* [*69*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/69revDubai.pdf) *(Rev. Dubai, 2014), WTDC-14/DAP* [Objective 3](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf)*, WTSA Resolutions* [*50*](https://www.itu.int/pub/T-RES-T.50-2016)*,* [*52*](https://www.itu.int/pub/T-RES-T.52-2016)*,* [*75*](https://www.itu.int/pub/T-RES-T.75-2016) *(Rev. Hammamet, 2016),* [*58*](https://www.itu.int/pub/T-RES-T.58-2016) *(Rev. Dubai, 2012), Council Documents* [*C05/32*](http://www.itu.int/md/S05-CL-C-0032/en)*,* [*C05/INF/10*](https://www.itu.int/md/S05-CL-INF-0010/en)*,* [*C06/4*](http://www.itu.int/md/S06-CL-C-0004/en)*,* [*C07/21*](http://www.itu.int/md/S07-CL-C-0021/en)*,* [*C08/33*](http://www.itu.int/md/S08-CL-C-0033/en)*,* [*C09/50*](http://www.itu.int/md/S09-CL-C-0050/en), [*C10/12*](http://www.itu.int/md/S10-CL-C-0012/en)*,* [*C11/54*](http://www.itu.int/md/S11-CL-C-0054/en)*,* [*C12/29*](http://www.itu.int/md/S12-CL-C-0029/en)*,* [*C13/23*](http://www.itu.int/md/S13-CL-C-0023/en), [*C14/23*](http://www.itu.int/md/S14-CL-C-0023/en), [*C15/18*](http://www.itu.int/md/S15-CL-C-0018/en) *and* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/en) |

## Cybersecurity and Countering Spam Activities

1.1 The development of ICTs, underpinned by security and trust, is recognized as essential for sustainable development. This report, organized around the five pillars of the [Global Cybersecurity Agenda (GCA)](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx), 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 Objective 3 of the Dubai Action Plan, and taking into account ITU-D Q 3/2 (former Q22/1), ITU is assisting Member States in understanding the legal aspects of cybersecurity through its [ITU Cybercrime Legislation Resources](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx) in order to help harmonize their legal frameworks.

2.2 In the area of legal measures, ITU collaborates closely with partners such as UNODC and others that may have expertise in this area.

**3. Technical and Procedural Measures**

3.1 [ITU-T Study Group 17 (SG-17)](http://www.itu.int/ITU-T/studygroups/com17/), 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, ITU-T 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 SG17 approved new cybersecurity Recommendations ITU-T X.1038 “Security requirements and reference architecture for software-defined networking”, X.1039 “Technical security measures for implementation of ITU-T X.805 security dimensions”, X.1085 “Information technology - Security techniques - Telebiometric authentication framework using biometric hardware security module”, X.1087 “Technical and operational countermeasures for telebiometric applications using mobile devices “, X.1258 “Enhanced entity authentication based on aggregated attributes”, X.1542 “Session information message exchange format”, X.1641 “Guidelines for cloud service customer data security”, and important revisions to X.500-series Recommendations on “Information technology – Open Systems Interconnection – The Directory” since ITU Council 2016.

3.3 Seven draft Recommendations are planned for TAP approval in March 2017 on cybersecurity, personally identifiable Information protection, access control, encryption for IoT, end-user perception of trustworthiness indicators, and secure software update capability for intelligent transport system; and eight other draft Recommendations are planned to be finalized to enter AAP approval process on structured cybersecurity information exchange techniques, countering smartphone-based botnets, countering instant messaging spam (SPIM), SMS phishing, mobile phone anti-theft measures, and security of open capabilities of telecommunication services. Work has been initiated on draft Recommendations on countering telephone service scam, smart metering service security in smart grids, de-identification processing, hybrid authentication and key management mechanisms in client-server model, Big Data analytics in mobile Internet services, security of Big-Data-as-a-Service, Communication-as-a-Service and Network-as-a-Service, telebiometric authentication using bio-signals, telebiometric anti-spoofing detection and Cryptographic Message Syntax (CMS) Profile.

3.4 [SG17 regional group for Africa](http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/sg17rgafr/Pages/default.aspx) held its second meeting on 27-28 July 2016 in Khartoum, Republic of Sudan.

3.5 SG17 continued coordination with ITU-T SG20 “IoT and its applications including smart cities and communities (SC&C)” on IoT security.

3.6 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, 4G and 5G) networks (Rec. ITU-R M.1078, M.1223, M.1457, M.1645, M.2012 and M.2083). It has also issued Recommendations on security issues in network management architecture for digital satellite systems (Rec. ITU-R S.1250) and performance enhancements of transmission control protocol over satellite networks (Rec. ITU-R S.1711).

**4. Organizational Structures**

4.1 ITU continues to help build capacity at regional and international levels. ITU has undertaken technical assessments to evaluate the preparedness for the [establishment of Computer Incident Response Teams (CIRTs](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx)) in 68 countries and is continuing with the necessary follow-up actions. National CIRT establishment and improvement is currently underway in Burundi, Gambia, Cyprus, and Kenya after the successful completion of related activities in 12 countries.

4.2 ITU partnered with the Global Cyber Security Capacity Centre at the Oxford Martin School, and jointly performed Cybersecurity Capacity Reviews in Thailand, Sierra Leone, and Madagascar.

4.3 ITU continues to conduct [Cyber Drill](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx)s 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 has conducted 16 Cyber Drills involving more than 100 countries. In the current reporting period, international Cyber Drills were held in Quito, Ecuador for the [Americas Region](http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2016/15551.aspx) (27 June–1 July 2016), in Tunis, Tunisia for the [Arab Region](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Tunisia_cyberdrill_2016.aspx) (23-27 May 2016) and in Mauritius for the [Africa Region](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Mauritius_cyberdrill_2016.aspx) (4-8 April 2016).

4.4 A [National Cybersecurity Strategy](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx) toolkit is under development, as a multistakeholder effort facilitated by ITU. To progress the work, three partner workshops were held on 18-19 February 2016 at the ITU HQs in Geneva, Switzerland, on 6-7 June 2016 at the Saïd Business School of the University of Oxford, United Kingdom, and on 13-14 October 2016 in Washington DC, United States, hosted by the Organization of American States (OAS). The product is under finalization and will be publicly available before the end of 2017.

4.5 ITU assisted Nepal in drafting its National Cybersecurity Policy and in Child Online Protection (4-8 July 2016), enhancing awareness and capacity building for about 100 government, regulatory and private stakeholders, and also demonstrated a successful cybersecurity simulation, and enhanced cooperation with the Nepal Telecommunication Authority (NTA).

4.6 A Survey of Cybersecurity readiness was carried out for countries in the Asia-Pacific region (2015-2016) based on the five pillars of the GCA.

**5. Capacity Building**

5.1 ITU continues to organize [regional cybersecurity forums](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) for all ITU regions, using them 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.

5.2ITU-D Study Group 2 continues its work for the Study Period 2014-2018 on [Question 3/2: Securing information and communication networks: Best practices for developing a culture of cybersecurity](http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2).

5.3 A workshop on ["Cybersecurity strategy in African countries"](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Pages/default.aspx) was jointly organized by ITU and ATU with the support of TSB and BDT on 24-26 July 2016 at the National Telecommunication Corporation (NTC) headquarters in Khartoum, Republic of Sudan.

5.4 For the first time, ITU formally partnered with the European Network and Security Agency (ENISA) to organize a joint [ITU-ENISA Regional Cybersecurity Forum](http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/RCYBF/Regional-Cybersecurity-Forum.aspx) on 29-30 November 2016 in Sofia, Bulgaria.

5.5 The 4th edition of the [“Central European Cybersecurity Public-Private Dialogue Platform”](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/CYBR/Cyber-Security-in-Romania.aspx) was held from 14 to 16 September 2016 in Sibiu, Romania.

5.6 Following the launch of the first [Global Cybersecurity Index](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx) (GCI) results in 2014, a [new iteration of the GCI](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx) is currently under elaboration with an enhanced index and set of partners. To date 136 countries have responded to the questionnaire and analysis is underway.

5.7 In Myanmar, Vietnam, Lao PDR, and Cambodia, in 2016, ITU helped develop technical skills to assist Incident Responders.

**6. International Cooperation**

6.1 ITU continues to develop relationships and [partnerships](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) with various regional and international organizations and initiatives, including the Commonwealth Cybercrime Initiative, ENISA, INTERPOL, ECOWAS, the World Bank, FIRST, and regional CSIRT/CERT associations, such as AP CERT, AFRICA CERT, and OIC CERT.

6.2 In its role as the lead facilitator for WSIS Action Line C5, ITU organized several events at the [WSIS Forum 2016](https://www.itu.int/net4/wsis/forum/2016/) that facilitated experience sharing among all stakeholder groups in their global efforts towards building confidence and security in the use of ICTs.

6.3 During Telecom Forum 2016, ITU, in collaboration with the EastWest Institute (EWI), organized a panel session on [“ICT trust, innovation and trade”](http://www.itu.int/net4/Telecom/webs/TelecomWorld/session/description/C-00001734).

6.4 ITU participated in the [International Multistakeholder Conference “Cyberspace, Energy & Development-Protecting Critical Energy Infrastructure”](https://www.energypact.org/energypact-foundation_conferences/) organized by the Austrian government, EnergyPact Foundation, and the Austrian Institute of Technology, supported by IEC, UNODC and ITU on 16 February 2017 in Vienna, Austria.

6.5 [195 country profiles](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx) continue to be publicly available on the ITU website. The profiles are factual, non-analytical representations of the cybersecurity wellness of each country based on the [five GCA pillars](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx). The profiles are “living” documents that continue being updated as more data on the countries become available.

**7. Child Online Protection (COP)**

7.1 The [Council Working Group on Child Online Protection](http://www.itu.int/en/council/cwg-cop/Pages/default.aspx) (CWG-COP) held two meetings since its last reporting period, including online open consultations with youth on various topics. More information can be found in Document [C17/15](https://www.itu.int/md/S17-CL-C-0015/en).

7.2 ITU and its partners continue to work closely in order to progress the Sustainable Development Goals, and particularly SDG 16.2 “End abuse, exploitation, trafficking and all forms of violence against and torture of children”.

7.3 During the previous two CWG-COP meetings, Child Helpline International (CHI) presented the outcomes of the ITU-CHI [joint campaign](http://www.itu.int/en/council/cwg-cop/Documents/FinalCampaignPresentation.pptx) on ["Partnering to Protect Children and Youth"](http://www.itu.int/en/cop/Pages/consultation-may2016.aspx). Following the campaign’s launch in May 2016, the final results were presented on 15 November 2016 during ITU Telecom World 2016, and new ways to develop the child helpline services were shared with the participants. The collaboration between ITU members and helplines was emphasized. The CWG-COP members welcomed the campaign and the Chair encouraged the Secretariat to continue this effort, in order to make progress within the context of SDG 16.

7.4 The ITU Regional Offices continue providing assistance to Member States in analysing their Child Online Protection landscape, in order to draft and propose a sustainable framework that can be implemented over a long period.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_