|  |  |
| --- | --- |
| **Council 2018Geneva, 17-27 April 2018** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.5** | **Document C18/18-E** |
| **8 February 2018** |
| **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 |

|  |
| --- |
| SummaryThis report summarizes ITU’s activities since Council 2017 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 requiredThe 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* [*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf) *(Rev. Dubai, 2014),* [2, 67, 69 *(Rev. Buenos Aires, 2017)*](https://www.itu.int/md/D14-WTDC17-C-0115/en)*; ITU-D Objective 2/Outcome 2.2 (*[Buenos Aires Action Plan](https://www.itu.int/md/D14-WTDC17-C-0115/en)*)*; *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) *,*[*C16/18*](https://www.itu.int/md/S16-CL-C-0018/en), and [*C17/18*](https://www.itu.int/md/S17-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 2.2 of the Buenos 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, mobile security, virtualization security towards cloud computing security, personally identifiable information protection and security architecture and application security, often in cooperation with external Standards Developing Organizations and Consortia.

3.2 At its [29 August- 6 September 2017 meeting](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx), ITU-T SG17 agreed to establish a new Question 14/17 on “Security Aspects of Distributed Ledger Technologies” and approved new Recommendations: X.1040 “Security reference architecture for lifecycle management of e-commerce business data”, X.1053 “Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations”, X.1146 “Security protection guidelines for value-added services provided by telecommunication operators”, X.1213 “Security Capability Requirements for Countering Smartphone-based Botnets”, X.1248 “Technical Requirements for Countering Instant Messaging Spam (SPIM)” and revised X.1541 “Incident Object Description Exchange Format (version 2)”.

3.3 ITU-T SG17 approved three Supplements to ITU-T X-series Recommendations: X.Suppl 29 “Supplement to ITU-T X.1242 –Guidelines on countermeasures against short message service (SMS) phishing and smishing attacks”; X.Suppl 30 “Supplement to ITU-T X.805: Security Guideline for Mobile Virtual Network Operator (MVNO)” and X.Suppl 31 “Supplement to ITU-T X.660 –Guidelines for using object identifiers for the Internet of things”.

3.4 In the next SG17 meeting in March 2018 three draft new Recommendations are planned for TAP approval. Other ongoing work items on “Technical framework for countering mobile in-application advertising spam”, “Security framework for Internet of Things”, “Security framework for voice-over-long-term-evolution (VoLTE) network operation”, “Trust Elevation Protocol- Authentication Step-Up Protocol and Metadata Version 1.0” are planned to be finalized and enter into approval too.

3.5 An [ITU Workshop on Security Aspects of Blockchain](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Pages/default.aspx) was held on 21 March 2017, in Geneva, Switzerland to examine Blockchain’s potential in enhancing trust in the use of ICTs. An expert roundtable brought together industry associations and standardization bodies to identify how the work of ITU-T SG17 could contribute to standards collaboration in support of Blockchain.

3.6 ITU SG17 organized an [ITU Workshop on Security Aspects of Intelligent Transport Systems](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Pages/default.aspx) on 28 August 2017, in Geneva, Switzerland to discuss the security requirements of all actors in the value chain underlying intelligent transport systems (ITS) and to further collaboration among the relevant bodies.

3.7 The [ITU SG17 Regional Group for Arab Region](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/sg17rgarb/Pages/default.aspx) held its first meeting on 10 December 2017, Muscat, Oman.

3.8 ITU SG17 plans to organize an [ITU workshop on 5G Security](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx) on 19 March 2018, prior to the next SG17 meeting taking place on 20-29 March 2018 in Geneva, Switzerland.

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

3.10 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, Cyprus, Gambia, Palestine, and Zimbabwe after the successful completion of related activities in 13 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. Following a project funded by the Australian Government (DOCA), ITU will execute CIRT assessments in Samoa, Tonga, Vanuatu, and Papua New Guinea, followed by Cybersecurity Capacity Reviews.

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. So far, ITU has conducted 19 Cyber Drills involving more than 100 countries. In the current reporting period, international Cyber Drills were held: a) on 3-7 July 2017 in [Paramaribo, Suriname](https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2017/20287.aspx) for the Caribbean, b) on 13-17 November 2017 in [Dar Es Salaam, Tanzania](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Tanzania_cyberdrill_2017.aspx), for both the Africa and Arab Regions, and c) on 21-23 November 2017, in [Chisinau, Moldova](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Moldova_cyberdrill_2017.aspx) for both the Europe and CIS Regions.

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 in 2016 and a follow-up meeting was held in Washington DC, United States on 25-26 February 2018. The product is currently under finalization.

**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 BDT programmes and activities as well as an operational platform for cooperation at the regional and international level.

5.2Following WTDC 2017, 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)) will continue its work during study period 2018-2021.

5.3 ITU, together with the AfricaCERT, organized a five-day capacity-building workshop on [“Threat intelligence for CIRTS”](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Threat-intelligence-training-Benin-2017.aspx) on 11-15 December 2017 in Cotonou, Benin in collaboration with l’Agence Nationale de la Sécurité des systèmes d'information (ANSSI FRANCE).

5.4 Following the launch of the first [Global Cybersecurity Index](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx) (GCI) results in 2014 and its inclusion in Resolution 130 (Rev. Busan, 2014), work was completed on the second version of the [Global Cybersecurity Index (GCI) (2017](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx)) based on responses from 134 countries, and with the assistance of international partners.

5.5 A webinar was organized on 18 December 2017 on the [“Report on Global Cybersecurity Index (GCI) for the Europe Region”](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2017/GCI/Webinar-on-New-Report-on-Global-Cybersecurity-Index-%28GCI%29-for-the-Europe-Region.aspx). The aim of the webinar was to launch the GCI 2017 Europe report which provides a focused and deeper insight into the findings on Cybersecurity in the 43 countries of ITU Europe region including illustrative practices in Europe.

5.6 An [ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/EVENTS/2018/04_Odessa/04_Odessa.aspx) is planned for 4-6 April 2018 in Odessa, Ukraine.

**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 2017](https://www.itu.int/net4/wsis/forum/2017/) that facilitated experience sharing among all stakeholder groups in their global efforts towards building confidence and security in the use of ICTs. Several high-level events are planned for WSIS Forum 2018, taking into consideration the 10-year anniversary of the GCA and the Child Online Protection initiative.

6.3 ITU participated in the [International Multistakeholder Conference “Vienna Cyber Security Week 2018 - Protecting Critical Energy Infrastructure”](https://www.energypact.org/energypact-foundation-events18/) organized by the Austrian government, EnergyPact Foundation, and the Austrian Institute of Technology, supported by IEC, OSCE and ITU from 29 January to 2 February 2018 in Vienna, Austria.

**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 [C18/15](https://www.itu.int/md/S18-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. In June 2017 ITU and UNICEF organized a thematic workshop titled From Child Online Safety to Digital Inclusion: The Role of Global Multistakeholder Partnerships. The session discussed child participation in the decision making deliberations and the importance to use a commonly agreed terminology to identify gaps and action measures.

7.4. ITU participated in the seventh Regional Consultation and Third Policy Dialogue of Child Helplines in Europe. The need to have a regional and harmonized number for child helplines was expressed by several members and more action from policy-makers and regional institutions was encouraged.

7.5. ITU participated in the Aqdar World Summit hosted in Abu Dhabi, UAE, on 21-23 November 2017. The meeting discussed several issues related to the role of moral education in academic institutions regionally and internationally to combat global challenges. ITU presented the work of the CWG-COP and the need to educate young children to use technologies in a safe and responsible manner.

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