|  |  |
| --- | --- |
| **Council 2019 Geneva, 10-20 June 2019** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.5** | **Document C19/18-E** |
| **1 April 2019** |
| **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 2018 in relation to Resolution 130 (Rev. Dubai, 2018), 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*](https://www.itu.int/en/council/Documents/basic-texts/RES-071-E.pdf)*,* [*130*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-E.pdf)*,* [*140*](https://www.itu.int/en/council/Documents/basic-texts/RES-140-E.pdf)*,* [*174*](https://www.itu.int/en/council/Documents/basic-texts/RES-174-E.pdf), [*179*](https://www.itu.int/en/council/Documents/basic-texts/RES-179-E.pdf) *(Rev. Dubai, 2018),* [*181*](https://www.itu.int/en/council/Documents/basic-texts/RES-181-E.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](https://www.itu.int/md/D14-WTDC17-C-0115/en) *(Rev. Buenos Aires, 2017); 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), [*C17/18*](https://www.itu.int/md/S17-CL-C-0018/en)*,* [*C18/18*](https://www.itu.int/md/S18-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), shows the complementary nature of existing ITU work programmes and facilitates the implementation of BDT, TSB, and BR activities in this domain.

1.2 The 2018 ITU Plenipotentiary Conference, held from 29 October to 16 November 2018 in Dubai, UAE, revised its Resolutions 130 and 179.

**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. In the area of Legal Measures, ITU collaborates closely with partners such as UNODC and other experts.

**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 the study and standardization 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, together with external Standards Developing Organizations.

3.2 Since the last report to the Council, SG17 held three meetings in March 2018, August-September 2018 and January 2019. SG17 established [55 new standardization work items](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). SG17 approved 17 new or revised ITU-T Recommendations on ICT security, namely: [Generic applications of ASN.1 Cryptographic Message Syntax](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12848), [Security framework for voice-over-long-term-evolution (VoLTE) network operation](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13603), [Security services using the software-defined networking](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13803), [Security framework and requirements for service function chaining based on software-defined networking](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13872), [Telebiometric access control with smart ID cards](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13725), [Telebiometric authentication using biosignals](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13873), [Security requirements and framework for big data analytics in mobile internet services](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13726), [Security assessment techniques in telecommunication/ICT networks](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13404), [Use Cases for Structured Threat Information Expression (STIX)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13849), [Technical framework for countering mobile in-application advertising spam](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13605), [Authentication Step-Up Protocol and Metadata Version 1.0](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13606), [Universal Authentication Framework (UAF)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13727), [Client To Authenticator Protocol/Universal 2-factor framework](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13728), [Security guidelines for home area network (HAN) devices in smart grid systems](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13405), [Security framework for the Internet of things based on the gateway model](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13607), [Guidelines on hybrid authentication and key management mechanisms in the client-server model](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13729) and agreed [Data security requirements for the monitoring service of cloud computing](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13406).

3.3 SG17 agreed revised [Supplement to ITU-T X.1051: Users’ guide for information security controls in telecommunications organizations](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13730&lang=en)” and five new Supplements to ITU-T X-series Recommendations: [Supplement to ITU-T X.805: Security Guideline for Mobile Virtual Network Operator (MVNO)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13410&lang=en), [Supplement to ITU-T X.660 –Guidelines for using object identifiers for the Internet of things](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13411&lang=en), [Supplement to ITU-T X.1058: Code of practice for personally identifiable information protection based on ITU-T X.1058 for telecommunications organizations](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13593&lang=en), [Supplement to ITU-T X.1231: Technical framework for countering telephone service scam](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13731&lang=en), and [Supplement to ITU-T X.1051 | ISO/IEC 27011 (2016): Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13869&lang=en).

3.4 The [SG17 Regional Group for Arab Region](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/sg17rgarb/Pages/default.aspx) held its 2nd meeting in Kuwait (Oct 2018). SG17’s regional group for Africa and regional group for the Arab Region will meet in Tunis, Tunisia (April 2019).

3.5 SG17 organized an [ITU workshop on 5G Security](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx) (March 2018), ITU Workshop on [Advanced Cybersecurity Attacks and Ransomware](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx) (Aug 2018), ITU Workshop on Artificial Intelligence/Machine Learning and Security (Jan 2019) and a workshop on Secure Quantum Communications (Jan 2019), aimed to identify ways forward for SG17 to undertake related standardization subjects in its future study, including potential new work items.

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

3.7 ITU-T SG9 determined five draft Recommendations ITU-T J.1012 J.1013, J.1014, J.1015, and J.1015.1 on Embedded common interface for exchangeable CA/DRM solutions.

3.8 ITU-T SG13 approved Rec. ITU-T Y.3053 (2018) Amd.1 “Framework of trustworthy networking with trust-centric network domains: Amendment 1 - Trustworthy networking deployment architecture and procedures”.

3.9 ITU-T SG15 approved revised Rec. ITU-T G.9978 “Secure admission in G.hn network”.

3.10 ITU-T SG20 approved Rec. ITU-T Y.4205 “Requirements and reference model of IoT-related crowdsourced systems”.

3.11 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 conducted technical assessments to evaluate the preparedness for the establishment of Computer Incident Response Teams (CIRTs) in 75 countries and is taking the necessary follow-up actions. Direct engagement in 14 such activities have been completed, and more are ongoing or planned for 2019.

4.2 ITU partnered with the Global Cyber Security Capacity Centre (Oxford Martin School) to perform joint Cybersecurity Capacity Reviews in Thailand, Sierra Leone, and Madagascar. Pursuant to funding by the Australian Government (DOCA), ITU will execute CIRT assessments in Samoa, Tonga, Vanuatu, and Papua New Guinea, followed by Cybersecurity Capacity Reviews. Additionally, ITU performed CIRT assessments for Albania, Bosnia and Herzegovina, Malawi, Mauritania and Congo DR.

4.3 ITU has conducted 24 [Cyber Drills](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) involving more than 100 countries. Cyber Drills were held in: [Grand Bassam, Ivory Coast](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/IvoryCoastcyberdrill2018.aspx) (Africa region, Oct 2018); [La Plata City, Argentina](https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2018/20577.aspx) (Americas region, June 2018); [Kuwait City, Kuwait](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx)(Arab Region, Oct 2018); [Limassol, Cyprus](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBDRILL/ITU-ALERT-Cyber-drill.aspx) (Europe region, Nov 2018) and [Baku, Azerbaijan](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/EVENTS/2018/09_Baku/09_Baku.aspx) (CIS region, Sept 2018). A 2019 Cyber Drill for Europe is being organized in [Romania](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberDrill/ITU-Cyber-Drill-for-Europe-Region-.aspx) (May 2019).

4.4 A [Guide to Developing a National Cybersecurity Strategy](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf) (NCS), developed through a multi-stakeholder collaborative process comprising 15 intergovernmental organizations, private sector, academia and civil society and facilitated by ITU, was published in September 2018. The NCS initiative provides a functional toolkit to help governments develop and improve their cybersecurity strategies. ITU is organizing regional and national cybersecurity strategy workshops to support Member States with the development of their NCS. A national workshop was held in Poland in 2018, and a regional one for the Europe region will be organized in June 2019. There are also ongoing discussions to organize similar workshops for SADC countries, Malta, Benin, and Guinea. ITU assisted Mauritania in the development of its NCS and held a validation Workshop (Nouakchott – Dec 2018) to present the interim report of the NCS 2019-2022 in Mauritania. ITU also assisted Kiribati and Bhutan in developing their NCS (Nov 2018).

**5. Capacity Building**

5.1 ITU has organized [regional cybersecurity forums](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) for all ITU regions in order to build capacity for different BDT programmes/activities and provide an operational platform for regional and international cooperation.

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, ICANN and WATRA organized a capacity-building workshop on Cybersecurity, CERT and ICANN Ecosystem (Ouagadougou, Burkina Faso - Oct 2018) hosted by the Regulatory Authority for Electronic Communications and Posts (ARCEP).

5.4 ITU and the ITU Arab Regional Cybersecurity Centre organized the [Regional Cybersecurity week](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx) (Kuwait - Oct 2018) that provided a platform for better cooperation and communication among Arab CIRTs.

5.5 ITU, the Advanced Level Telecom Training Centre and Faculty of Applied Science of Post and Telecommunication (ICT Faculty, I.R. Iran), organized an [ITU ASP CoE Cybersecurity Training](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2018/CybersecurityASPCOE/cybersecurity.aspx) (Tehran, Iran – Dec 2018).

5.6 The third iteration of the [Global Cybersecurity Index](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCIv3), with 155 Member States participating, was launched in March 2019 during the ITU-D study group meeting. GCIv3 captures more details on cybersecurity while expanding the partnership into a multi-stakeholder collaborative platform. ITU has initiated the preparation phase for the GCIv4 process which shall start in April 2019.

5.7 ITU organized the [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) (Odessa, Ukraine – April 2018).

**6. International Cooperation**

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

All activities under ITU’s partnership with IMPACT ended in 2016 after the completion of the remaining pending projects. IMPACT communicated its formal dissolution at the beginning of 2018. Such dissolution implied the termination, with immediate effect, of the MoU and the Cooperation Agreement signed between ITU and IMPACT.

6.2 As the lead facilitator for WSIS Action Line C5, ITU organized several sessions at the [WSIS Forum 2018,](https://www.itu.int/net4/wsis/forum/2018/) giving due consideration to the 10-year anniversary of the GCA and the Child Online Protection initiative. High-level sessions were also held during [WSIS Forum 2019](https://www.itu.int/net4/wsis/forum/2019/) including on Artificial Intelligence and Security.

6.3 In July 2018, a [Global Dialogue on AI, IoT and Cybersecurity Policy and Regulatory Challenges and Opportunities](https://www.itu.int/net4/ITU-D/CDS/GSR/2018/default.asp) was organized in ITU, bringing together regulators from different Member States and organizations.

6.4 ITU partnered with academia in the Arab region (Arab States Research and Education Network and Naïf Arab University for Security Sciences) to strengthen their role in promoting cybersecurity culture and encourage active participation in ITU’s work. Within these partnerships, activities were organized in the Arab region.

6.5 Within the framework of the ITU Regional Initiative for Europe, ITU has been co-organizing a series of cybersecurity events including: [The 6th Central European Cybersecurity Public-Private Dialogue Platform](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBR/Cyber-Security-in-Romania.aspx) (Sibiu, Romania - Sept 2018); International Forum on [“The New Global Challenges in Cyber Security”](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CERT-ROForum/default.aspx) (Bucharest, Romania - Oct 2018); [Western European Cybersecurity Public-Private Dialogue Platform](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBCONGR/Second-Western-European-Cybersecurity-Public-Private-Dialogue-Platform.aspx) (Second Porrentruy, Switzerland - Nov 2018); [Vienna Cyber Security Week - Protecting Critical Infrastructure](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/cybervienna.aspx) (Vienna, Austria (co-organized by IEC, supported by OSCE) - March 2019).

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

7.1 ITU assisted Sudan in the development of its national COP strategy. Additionally, advocacies and competition challenges were organized in several Arab countries to raise awareness on Internet safety among children, educators, and parents in collaboration with relevant stakeholders.

7.2 Within the framework of the ITU Regional Initiative for Europe, ITU assisted Georgia in the development of its national COP strategy. Similar activities are planned in other countries in the upcoming period. Additionally, ITU co-organized a series of events aimed at building human capacity, including: [National Event on Child Online Protection: Awareness Day for Children and Teens](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/NECOP/default.aspxhttps:/www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/NECOP/default.aspx) (Noto, Italy - May 2019); [Digital Youth Forum](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/DYF/default.aspx) (Warsaw, Poland - May 2018); International Conference on ["Keeping Children and Young People Safe Online"](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/COP/default.aspx) (Warsaw, Poland - Sept 2018) and [Safer Internet Day 2019](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/SID/Safer-Internet-Day-2019.aspx) (Tirania, Albania – Feb 2019).  
7.3 In November 2018, ITU assisted Kiribati and Bhutan in conducting assessments on COP. ITU also prepared a Paper on “Improving child online protection measures in ASEAN: Partnering with industry” and [a 3D Multiuser Virtual Learning Environment](https://www.youtube.com/watch?v=SymYlZq5v1k&feature=youtu.be) to increase awareness about online risks for children.

7.4 ITU celebrated Safer INTERNET day 2019 with various activities, including promoting protection of children online.