|  |  |
| --- | --- |
| **Council 2020Geneva, 9-19 June 2020** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.4** | **Document C20/18-E** |
| **30 March 2020** |
| **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 2019 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 requiredThe 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);* [*ITRs*](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), Recent Council Documents* [*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)*,* [*C19/18*](https://www.itu.int/md/S19-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.

**2. Legal Measures**

2.1 As part of Objective 2/outcome 2.2 of the Buenos Action Plan, and taking into account ITU-D SG2 Question 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 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 one meeting in September 2019 where SG17 established [25 new standardization work items](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). SG17 approved 30+ new or revised ITU-T Recommendations on ICT security, namely: 9th edition of the cornerstone standards for cybersecurity X.500-series Recommendations on public key infrastructure, X.1044 “Security requirements of network virtualization”, X.1045 ”Security service chain architecture for networks and applications”, X.1059 “Implementation guidance for telecommunications organizations on risk management of their assets globally accessible in IP-based networks”, X.1702 “Quantum noise random number generator architecture”, X.1232 “Technical framework for countering advertising spam in user generated information”, X.677 “Identification mechanism for unmanned aerial vehicles using object identifiers”, X.1402 “Security threats to distributed ledger technology”, X.1197 Amendment 1 “Revised guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection”, X.694 Cor.1 and X.893 Cor.1 on ASN.1, revised Z.100-series on SDL and revised Z.160-series on Testing and Test Control Notation Version 3 (TTCN-3). SG17 also approved a new Supplement on use cases of Entity Authentication Assurance (EAA) framework and revised Z-series implementor’s guide.

3.3 SG17 organized a one-day [ITU workshop on Fintech Security](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx) on 26 August 2019 which came out with suggestions on SG17 follow-up activities in collaboration with other identified Fintech security-related SDOs, i.e., FG-DLT, FG-DFC, ISO TC 307, W3C on DLT. SG17 also organized a [mini workshop on cybersecurity challenges in automated driving](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx) on 26 August 2019 in cooperation with ITU Collaboration on ITS (CITS) and UNECE WP29.

3.4 Due to the worldwide outbreak of coronavirus, SG17 meeting on 17-26 March 2020 became the first fully virtual ITU-T study group meeting. Also SG17 had to postpone its [joint ITU-T SG17/ISO TC 307 Workshop on “DLT security, identity management and privacy”](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200316/Pages/default.aspx) planned on 16 March 2020.

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

3.6 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.

3.7 ITU-T SG13 approved Recommendation ITU-T Y.3053 (2018) Amendment 1 “Framework of trustworthy networking with trust-centric network domains: Amendment 1 - Trustworthy networking deployment architecture and procedures”. Y.3514 Cor.1 “Cloud computing - Trusted inter-cloud computing framework and requirements” and Y.3517 “Cloud computing - Overview of inter-cloud trust management”.

3.8 ITU-T SG15 is working on Supplement (G.Sup.otnsec) which describes language and a common data infrastructure in existing Optical Transport Network (OTN) protocol layers that is needed to use independently proposed cryptographic protocols for creating secure transport solutions on selected OTN layers.

3.9 ITU-T SG20 approved Rec. ITU-T Y.4807 “Agility by design for Telecommunications/ICT Systems Security used in the Internet of Things”.

3.10 Several ITU-T Focus Groups are exploring trust aspect of various emerging technologies as part of their work. These include (1) The [*ITU-T Focus Group on Machine Learning for Future Networks including 5G (FG ML5G)*](https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx) (2) [*ITU-T Focus Group on Technologies for Network 2030 (FG NET-2030)*](https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx) (3) [*ITU-T Focus Group on Artificial Intelligence for Health (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h) (4) [*ITU-T Focus Group on Vehicular Multimedia (FG VM*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)*)* (5) [*ITU-T Focus Group on “AI for autonomous and assisted driving”*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx) (FG-AI4AD) (6) [*ITU-T Focus Group on "Quantum Information Technology for Networks" (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx)*.*

3.11 ITU in joint collaboration with the Bill & Melinda Gates Foundation, the World Bank Group, and the Bank for International Settlements, organized a [workshop on Security, Infrastructure and Trust for Digital Financial Services](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Pages/default.aspx) which took place from 4-5 December 2019 at ITU Headquarters, Geneva, Switzerland.

3.12 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 76 countries and is taking the necessary follow-up actions. Direct engagement in 14 such activities have been completed. Through the implementation of CIRT services and related capabilities project, the State of Palestine was assisted in building and deploying the technical capabilities and related trainings for CIRT operations. Kiribati and Solomon Islands received assistance to develop their national cybersecurity strategies. Capacity development on CIRT was provided to Papua New Guinea and Vanuatu through the [ITU-Department Communications and the Arts, Australia (DoCA) project](https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9RAS18061). CIRT readiness assessment workshops were conducted in Chad and Liberia. The national CIRT stakeholders of Gambia were trained on CIRT operations. 4 CIRT projects were initiated and implementation is still ongoing in Botswana, Burundi, Gambia, and Malawi. In Kenya, the existing CIRT enhancement is ongoing (to be completed in 2020).

4.2 ITU has conducted 28 [Cyber Drills](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) involving more than 100 countries. Cyber Drills were held in: [Uganda](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Africa-Cyberdrill-2019.aspx) (Africa region, November 2019); [Oman](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx)(Arab Region, October 2019); [Malaysia](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/ASP-CIS-Cyberdrill-2019.aspx) (Asia & the Pacific region, September 2019) and Romania (Europe & CIS region, May 2019). Five Cyber Drills are planned to be conducted in 2020.

**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.

5.2 Following WTDC 2017, ITU-D SG2 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)) continues its work during study period 2018-2021.

5.3 The ITU Guide to Developing a National Cybersecurity Strategy (NCS) constitutes a good practice guide that has been used by countries in all regions. The following workshops were organized in 2019: (a) A regional workshop, hosted by the Ministry of Informatics and Cyber Security Agency of Indonesia in Jakarta, on cybersecurity strategies (discussions included general data protection regulations) (b) A regional workshop, hosted by Macedonia, on improving national strategies for five Balkan states (c) A regional workshop, hosted by Tunisia, on improving national strategies of countries from the Africa and Arab States regions. Twenty countries actively participated. Three countries received direct assistance to develop and revise national cybersecurity strategies using the guide.

5.4 Capacity development and technical assistance was provided to Sudan to improve its strategy on critical information infrastructure protection.

5.5 During the Regional Cyber Security Week for the Arab States region the ITU Arab Regional Cyber Security Centre (ITU-ARCC) fostered information sharing and capacity building in the field of cybersecurity. The week provided a platform for senior ICT and cybersecurity officials from the region to meet with relevant stakeholders and discuss threats, evolution, opportunities and cybersecurity challenges.

5.6 The Moldova Cybersecurity Week was held in Chisinau, Moldova, and supported by ITU. The conference offered networking opportunities and a platform to exchange ideas, discuss and collaborate to drive, through innovation, global cybersecurity strategies and solutions.

5.7 The Cyber Shield 2019 was held in Ankara, Turkey, and was supported by ITU. The main objectives were to increase incident response capabilities and readiness levels, to increase mutual understanding of cyber risks and associated impacts, and to ensure a continued collaborative effort among international cybersecurity stakeholders especially national CIRTs in order to mitigate cyber threats. ITU also organized a training session for Kyrgyzstan on how to set up a cybersecurity operations center.

5.8 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 – December 2018).

5.9 The third [ITU Global Cybersecurity Index](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) shows considerable improvement in commitment to cybersecurity worldwide. The fourth version of the Global Cybersecurity Index survey, with an improved questionnaire and methodology, has been launched. In partnership with Deloitte, a cybersecurity landscape review was conducted for Cote d’Ivoire, including on the GCI findings. The review helped the country to identify cybersecurity priority initiatives to improve its cybersecurity posture.

**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.

6.2 ITU is supporting the 2020 G20 Presidency (Saudi Arabia), upon their request, as a knowledge partner on various tracks including the Security in the Digital Economy priority, as part of the multistakeholder effort undertaken by the G20 Secretariat in engaging relevant international organizations.

6.3 As the lead facilitator for WSIS Action Line C5, ITU organized several sessions at the [WSIS Forum 2019,](https://www.itu.int/net4/wsis/forum/2019/) including a High-level session on AI and Trust, as well as a session on the importance of measurement in cybersecurity.

6.4 Following the instructions of the 2019 session of Council, the Secretary-General has submitted to the 2020 session of Council (1) a report explaining how the ITU is currently utilizing the GCA framework and (2) with the involvement of Member States, appropriate guidelines developed for utilization of the GCA by the ITU for Council's consideration and approval.

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

7.1  A multi-stakeholder expert working group, consisting of more than 50 organizations and individual experts, started the review of the [Child Online Protection Guidelines](https://www.itu.int/en/cop/Pages/guidelines.aspx), which were first issued in 2009.

7.2 In Africa, discussions started with Chad, Kenya, Malawi, and Rwanda on the implementation of national strategy frameworks. In particular, the COP Regional Forum held in Ghana brought together a wide range of experts to analyse solutions and possible measures to be undertaken. In the Asia-Pacific region, assistance was provided for the development of the ASEAN Regional Framework on Child Online Protection, building upon the COP Guidelines, in coordination with other partners, including such as TELSOM/TELMIN. Other activities took place in Europe, as part of the regional initiative on enhancing trust and confidence in the use of ICTs.

7.3 ITU serves as the Secretariat of the Broadband Commission for Sustainable Development. The Working Group on Child Online Safety, led by the World Childhood Foundation and Zain, released its comprehensive [report](https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf) in New York in October 2019. The COP Guidelines were included as a reference and taken as the basis to implement the recommendations of the report.

7.4 A regional study on national approaches for keeping young people and children safe online was drafted for review and opened for consultations with the countries. Also, assistance was provided to Georgia and Ukraine in the development of a national strategy on child online protection.

7.5 ITU celebrated Safer INTERNET day 2020 with various activities, including promoting protection of children online. The new COP Mascot was launched on Safer Internet Day 2020. The [story and background](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) was designed and created by children at the beginning of January 2020.

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