|  |  |
| --- | --- |
| **Council 2021Virtual consultation of councillors, 8-18 June 2021** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.4** | **Document C21/18-E** |
| **22 February 2021** |
| **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 in 2020 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). The 2020 version of this report (C20/18) was prepared for submission to 2020 session of the Council but was not reviewed.Action requiredThe Council is invited to **note** this report as well as document C20/18.\_\_\_\_\_\_\_\_\_\_\_\_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)*,* [*C20/18*](https://www.itu.int/md/S20-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 2.2 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 relevant organizations that provide assistance to Member States.

**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 one meeting in September 2020 where SG17 established [15 new standardization work items](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17) and an e-plenary session on 7 January 2021. SG17 approved 40+ new or revised Recommendations on ICT security, namely: [X.510 | ISO/IEC 9594-11](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14320); [X.680-690-series](https://www.itu.int/rec/T-REC-x/en); [X.1046](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1046); [X.1052 (revised)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14044) and [X.1054 (revised, under approval)](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1054); [X.1148](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14249); [X.1149](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14250); [X.1216](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14259), [X.1217](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1217)and[X.1218](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14444); [X.1254 (revised)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14260), [X.1279](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14261), [D.1140/X.1261](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1261), [X.1451](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14252) and [X.1452](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14451); [X.1363](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14087), [X.1364](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14088), [X.1365](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14089), [X.1366](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14262), [X.1367](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14263), and [X.1368](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1368)**;** [X.1371](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14090), [X.1374](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14446), [X.1375](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14447) and [X.1376](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1376), [X.1400](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14449), [X.1401](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14092), [X.1402](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14251), [X.1403](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14264) and [X.1404](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14450), [X.1606](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14265); [X.1710](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14452) and [X.1714](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14453); [X.1750](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14266) and [X.1751](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14267), andX.1811 (under approval)**.**

3.3 SG17 also agreed on the following Technical Reports: “Security framework for quantum key distribution in telecom network”, “Problems, requirements and potential solutions for OID resolution”, “Security in telecommunications and information technology (7th edition)”, “Successful use of security standards (2nd edition)”, “Description of the incubation mechanism and ways to improve it”, “Strategic approaches to the transformation of security studies”, and “Unified Security Model (USM) - a neutral integrated system approach to Cybersecurity”.

3.4 In preparation for WTSA-20, SG17 agreed to restructure its existing 14 Questions to 12 Questions. Due to the postponement of WTSA-20, this new set of 12 Questions was endorsed by TSAG January 2021 meeting and became effective on 18 January 2021 for the remainder of the study period.

3.5 ITU-T SG3 continues to study economic and policy aspects of big data and digital identity relating to international telecommunication services through its Question 11/3. SG3 recently approved [Recommendation ITU-T D.267/X.1261](https://www.itu.int/rec/T-REC-D.1140-202008-I).

3.6 ITU-T SG11 continues improving the signalling protocols in order to make them more secure, including the development of additional requirements for signalling messages exchange and particular protocols. ITU-T SG11 agreed [Technical Report QSTR-SS7-DFS](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-TUT-PROTO-2019), revised stack of SS7 protocols (Q.731.3-Q.731.6) and approved Recommendation ITU-T [Q.3057](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.3057). Also, ITU-T SG11 continues developing standards ITU-T [Q.5050](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5050), [Q.5051](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5051), [Q.5052](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5052) and [Q.5053](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5053) related to combating counterfeit and stolen telecommunication/ICT devices.

3.7 ITU-T SG9 approved the following security-related Recommendations: ITU-T [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13573), [J.1013](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13574), [J.1014](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13575), [J.1015](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13576), and [J.1015.1](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13837); ITU-T [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357); and [J.1031](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14280), [J.1032](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14355), and [J.1033](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14356). SG9 also agreed on three Supplements to the following J-series Recommendations (ITU‑T J.1012-J.1015.1) namely ([J.Sup7](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14286), [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287) and [J.Sup9](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14288)).

3.8 ITU-T SG13 approved the following Recommendations: ITU-T [Y.3055](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14393) on trust-based personal data management and ITU-T [Y.3801](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14258), [Y.3802](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3802), [Y.3803](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3803) and [Y.3804](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14409) on quantum key distribution networks.

3.9 ITU-T SG20 developed the following security related Recommendations: [Y.4560](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14379), [Y.4561](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14380), [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381), and [Y.4907](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14382).

3.10 Several ITU-T Focus Groups are exploring the trust aspect of various emerging technologies as part of their work. These include (1) [*ITU-T Focus Group on Artificial Intelligence for Health (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h) (2) [*ITU-T Focus Group on Vehicular Multimedia (FG VM*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)*)* (3) [*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)*, (4) [*ITU-T Focus Group on "Quantum Information Technology for Networks" (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx)*.* (5) [*ITU-T Focus Group on AI for Natural Disaster Management (FG-AI4NDM)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx)*,* and (6)[*ITU-T Focus Group on Autonomous Networks (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx)*.*

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). Information related to [Futuristic mobile technologies foresee “IMT for 2020 and beyond”](https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx) can be found on the website.

**4. Organizational Structures**

4.1 ITU conducted technical assessments to evaluate the preparedness for the establishment of Computer Incident Response Teams (CIRTs) in more than 80 countries and is taking the necessary follow-up actions to assist the Member States in implementation. In 2020, ITU conducted the CIRT assessments for Guyana and Bermuda, and finalized the assessment report for Liberia. Direct engagement in establishment and/or enhancement of 14 National CIRTs have been completed, and of the 7 projects that are currently ongoing, 3 are in the process of being completed during Q1, 2021. ITU and the Government of the Bahamas have also signed a cooperation agreement for, *inter alia*, the implementation of a National CIRT.

4.2 Till date, ITU has organized 29 [CyberDrills](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) involving more than 100 countries. During September-December 2020, ITU has organized and executed the ITU 2020 [Global CyberDrill](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx) through several online events consisting of regional dialogues, technical and policy webinars, and tools use and skills development trainings, as well as a regional [CyberDrill for the Pacific Islands](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2020/Pacific%20Cyberdrill/Pacific-Cyberdrill21.aspx).

**5. Capacity Building**

5.1 During the [ITU Global Cyberdrill](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), BDT has organized regional cybersecurity forums for all ITU regions to build human and organizational capacity.

5.2 Following 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)) continues its work during study period 2018-2021.

5.3 The process to update [The Guide to Developing a National Cybersecurity Strategy](https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018) (NCS) is underway and expected to end in October 2021. Currently there are more than 20 organizations contributing to the update. ITU also conducted a webinar: “[National Cybersecurity Strategies – Implementation and Monitoring](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-NCS-IM-webinar.aspx)” on 19 October 2020 to discuss the lifecycle development and implementation of a NCS. Technical assistance activities on NCS have commenced with Fiji, Liberia and Chad, and there are ongoing discussions with other Member States that need assistance. A regional workshop for the Asia Pacific region on “[Lifecycle and Development of National Cybersecurity Strategies](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/ITU-regional-workshop-national-cybersecurity-strategies.aspx)” was held in Melbourne, Australia ​ on ​​20 February 2020. ITU is also finalizing the online training materials for NCS Development to be delivered through ITU academy in Q2, 2021.

5.4 Through the [ITU Academy](https://academy.itu.int/training-courses/full-catalogue?search_api_fulltext=&field_taxon_registration=All&field_course_fee=All&field_taxon_region=All&field_taxon_type=All&field_taxon_topics=109&field_taxon_languages=All&date_start=&date_end=&items_per_page=10), the ITU and CoE continue to deliver training activities and workshops in various areas of the cybersecurity domain.

5.5 To address cybersecurity challenges during the COVID-19 pandemic and to [support Member States’ health infrastructure with timely information on cyber threats](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Covid-19-CNI-Solution.aspx), the ITU sector member BitSight provided access to its cybersecurity scoring platform for ITU Member States.

5.6 The fourth version of the [ITU Global Cybersecurity Index](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) survey (GCI), with an improved questionnaire and methodology, has been launched and is currently ongoing. The GCI survey has concluded on 30 September 2020. In addition to experts from academia and the private sector, all Member States were invited to appoint experts to join and contribute to the [GCI Weightage Expert Group meeting](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) held on 15 October 2020.

5.7 To promote the involvement of young people in the field of cybersecurity and to address the field’s worldwide workforce shortage, ITU will be launching the Youth4Cyber initiative.

5.8 ITU is also finalizing the plan to launch the Women in Cyber Mentorship Programme targeted at building capacity of women junior professionals wishing to enter or thrive in the field of cybersecurity.

**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 Following the instructions of the 2019 session of Council, the Secretary-General will submit for the next 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. As per the process set out by Council 2019 for developing the draft Guidelines, and following the first online open consultation held on 23 April 2020 for all WSIS stakeholders to provide comments on the draft Guidelines, a second online open consultation will be held for all WSIS stakeholders on 1 March 2021.

6.3 As the lead facilitator for WSIS Action Line C5, ITU organized several sessions at the [WSIS Forum 2020,](https://www.itu.int/net4/wsis/forum/2020/en) including an Action Line C5 facilitator session on “Cybersecurity in the era of Quantum Information Technology (QIT): challenges and considerations for ICT networks” and a High-Level dialogue on “Ensuring Trustworthy Healthcare in an AI World”.

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

7.1 A multi-stakeholder expert working group, consisting of more than 50 organisations and individual experts from different sectors, reviewed the four sets of the [Child Online Protection Guidelines](https://www.itu.int/en/cop/Pages/guidelines.aspx) for policy-makers, industry, parents and educators as well as children. The [global launch of the new Guidelines](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-COP-Guidelines-launch-webinar.aspx) was followed by [regional launching events](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/2020/Regional-Launches-COP-2020-Guidelines.aspx) to discuss opportunities for implementation at the regional and national levels.

7.2 In Africa, the first training for policy-makers on COP was held in both English and French prior to the launch of the Guidelines in the region.  In the CIS region, an [Online Safety Course](https://onlinesafety.info/#/home) was developed by ITU Regional Office for CIS jointly with the A.S. Popov Odessa National Academy of Telecommunications. In the Asia-Pacific region, assistance was provided for the development of national COP strategies and related frameworks to six small island and developing countries, building upon the COP Guidelines, in coordination with other partners, through a joint project with the Department of Communications and Arts (DoCA) in Australia. In the Americas, discussions have started with Colombia, Costa Rica, Brazil and Paraguay on the development and implementation of national strategy frameworks. The roll out of the COP Guidelines was advanced significantly in Europe, where numerous activities took place, as part of the regional initiative on enhancing trust and confidence in the use of ICTs.

7.3 The Kingdom of Saudi Arabia and ITU signed an agreement to implement a three-year global programme on ‘Creating a safe and empowering cyber environment for children’, which focuses both on policy assistance for governments and development of digital skills and literacy with end-users. The implementation of the program will start in Q1 2021.

7.4 A report on the ‘[Status of national child online protection ecosystems in South Eastern Europe’](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/FINAL%20REPORT.pdf) was published and followed by numerous events and fora, which were (co-) organised on the issue of protecting children online in Europe.

7.5 ITU celebrated Safer INTERNET day 2021 with various communications, including a [blog](https://www.itu.int/en/myitu/News/2021/02/08/18/38/Sango-Internet-safety-drawing-child-online-protection-COP) post on the application of the COP Mascot in a national drawing competition in Hungary. The COP Mascot furthermore [announced a collaborative project with Eni and Deloitte Italia](https://www.bing.com/videos/search?q=sango+announcing+eni+youtube&docid=13903411089711&mid=271E2ABE304F85C97D50271E2ABE304F85C97D50&view=detail&FORM=VIRE) to raise awareness and build capacity on online safety with children and educators.