|  |  |
| --- | --- |
| **Council 2022 Geneva, 21-31 March 2022** |  |
|  |  |
|  |  |
| **Agenda item: PL 1.4** | **Document C22/18-E** |
| **18 February 2022** |
| **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 2021 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** this 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)*,* [*C20/18*](https://www.itu.int/md/S20-CL-C-0018/en)*,* [*C21/18*](https://www.itu.int/md/S21-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 two meetings in April and August/September 2021 where SG17 established 22 [new standardization work items](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17) and two e-plenary sessions in Januarys of 2021 and 2022. SG17 approved 30+ new or revised Recommendations on ICT security, namely: X.1011, X.1046, X. 1047, X.1054 (revised),X.1060,X.1061, X.1080.2, X.1217, X.1233, X.1234, X.1235, X.1252, X.1333, X.1369**,** X.1376**,** X.1405**,** X.1406, X.1407, X.1408, X.1453**,** X.1470, X.1643, X.1712, X.1752**,** X.1770**,** X.1811**,** and X.Suppl.36.

3.3 SG17 also agreed on Technical Report “Framework for Security Standardization for Virtualized Services”.

3.4 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.1102](https://www.itu.int/rec/T-REC-D.1102) on Customer redress and consumer protection mechanisms for OTTs.

3.5 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-USSD “Low resource requirement, quantum resistant, encryption of USSD messages for use in financial services” and Q.Suppl.75 related to combating counterfeit and stolen telecommunication/ICT devices.

3.6 ITU-T SG9 approved revised [ITU-T J.1026](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14868), [J.1027](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14869), [J.1028](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14870), and [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357). SG9 also approved J.1205 and continued updating of Implementers’ Guide of ITU-T [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13573) and two 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) and [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287).

3.7 ITU-T SG13 approved the following Recommendations: ITU-T Y.3056 andY.3057 on trust-based personal data management and ITU-T Y.3805 and Y.3806, on quantum key distribution networks.

3.8 ITU-T SG15 agreed ITU-T G.Suppl.OTNsec “Optical transport network security”

3.9 ITU-T SG16 approved Recommendation ITU-T F.747.10 “Requirements of distributed ledger systems (DLS) for secure human factor services” (under publication), which provides general requirements and functional capabilities for distributed ledger systems (DLS) for secure human factor services.

3.10 ITU-T SG20 developed the following security related Recommendations: [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381), Y.4810, and Y.4811.

3.11 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 Testbeds Federations for IMT-2020 and beyond (FG-TBFxG)*](https://www.itu.int/en/ITU-T/focusgroups/tbfxg/Pages/default.aspx) (2) [*ITU-T Focus Group on "Artificial Intelligence (AI) and Internet of Things (IoT) for Digital Agriculture" (FG-AI4A)*](https://www.itu.int/en/ITU-T/focusgroups/ai4a/Pages/default.aspx) (3) [*ITU-T Focus Group on AI for Natural Disaster Management (FG-AI4NDM)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx)(4) [*ITU-T Focus Group on Autonomous Networks (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/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 "Environmental Efficiency for Artificial Intelligence and other Emerging Technologies" (FG-AI4EE)](https://www.itu.int/en/ITU-T/focusgroups/ai4ee/Pages/default.aspx) (7) [*ITU-T Focus Group on Artificial Intelligence for Health (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h), and (8) [*ITU-T Focus Group on Vehicular Multimedia (FG VM*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)*).*

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). 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 In 2021, 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. Direct engagement in establishment and/or enhancement of 17 National CIRTs have been completed by 2021, three (3) projects were completed in 2021, CIRT assessment have been conducted for Guinea Bissau, Bahamas, Mongolia, and Guyana, CIRT design was reviewed for Eswatini, and currently there are four ongoing CIRT implementation projects. ITU has also assisted Mali and Malawi in designing National PKI frameworks for each of the countries.

4.2 Till date, ITU has organized 34 [CyberDrills](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) involving more than 120 countries. Within the period of September-December 2021, ITU has organized and executed the ITU 2021 [Global CyberDrill](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberdrills-2021.aspx) through several online events consisting of regional dialogues, technical and policy webinars, and tools use and skills development trainings, as well as two sub-regional CyberDrills for ECOWAS and SADC countries and one national CyberDrill for India. Also, two publications “Operational framework and guidelines for the planning and execution of ITU regional CyberDrills” and “ITU cybersecurity programme: CIRT framework” weredeveloped in 2021.

**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)) continued its work during study period 2018-2021.

5.3 ITU facilitated the process to update [The Guide to Developing a National Cybersecurity Strategy](https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018) (NCS). More than [20 organizations](https://ncsguide.org/partners/) contributed to the second [edition of the Guide which](https://ncsguide.org/the-guide/) was launched in November 2021 through a global webinar which discussed the lifecycle development and implementation of a NCS, highlighted challenges and opportunities and called for more cooperation. Technical assistance activities on NCS have commenced with Bahamas, Rwanda, Morocco and the SADEC region, and there are ongoing discussions with other Member States that need assistance. ITU also finalized and made available the online training “[Lifecycle, principles and good practices of national cybersecurity strategy development and implementation](https://academy.itu.int/training-courses/full-catalogue/lifecycle-principles-and-good-practices-national-cybersecurity-strategy-development-and)” on the ITU Academy platform in three languages (English, French, Spanish. The Russian version of training will be available in March 2021. ITU is partnering with the World Bank Group to organize regional webinars to provide operational insights on how to develop an NCS action plan. ITU is developing an NCS Benchmarking tool to support Member States and cybersecurity practitioners in their NCS efforts. The pilot of the tool was finalized in January and the work to further update will continue in 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 The fourth edition of the [ITU Global Cybersecurity Index](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx)  (GCI) Report was [released on 29 June 2021](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI/GCIv4-Report-Launch.aspx).  This edition of the index covers 193 Member States and the State of Palestine, with 169 countries contributions to the data. The work on an updated questionnaire for the GCI has already started. The new set of documents was virtually presented to ITU-T Study Group 2 Question 3 in October 2021, and a virtual Correspondence Group was created by the Study Group to give input into the revised questionnaire. A new edition of the GCI Questionnaire is expected to be released early 2022.

5.6 To promote the involvement of young people in the field of cybersecurity and to raise awareness on the field’s worldwide workforce shortage, ITU is planning activities and collaborations for and by youth under the umbrella of the Generation Connect Initiative

5.7 ITU has successfully completed the first edition of the Women in Cyber Mentorship Programme targeted at building capacity of women junior professionals wishing to enter or thrive in the field of cybersecurity. A new cohort is set to begin in April of 2022, with target groups residing in Africa, Arab and Asia-Pacific regions.

**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 The 2019 session of Council instructed the Secretary-General to submit to Council appropriate guidelines developed for utilization of the Global Cybersecurity Agenda (GCA) for its consideration and approval. [Document C21/71](https://www.itu.int/md/S21-CL-C-0071/en) was accordingly prepared and submitted by the Secretary-General to the Virtual Consultation of Councillors 2021 (C21/VCC1). Following discussions at C21/VCC-1, Council Member States instructed the secretariat *“to conduct further consultations with Council Member States, taking into account the inputs received and the comments made at this meeting. The secretariat should bring back a revised document 71 for consideration and approval at the next session of the Council"*. Consultations are currently being held with Council Member States and a revised Document will be submitted to Council 2022 for consideration and approval.

6.3 As the lead facilitator for WSIS Action Line C5, ITU organized a dedicated cybersecurity track comprising several sessions at the [WSIS Forum 2021,](https://www.itu.int/net4/wsis/forum/2020/en) including an Action Line C5 facilitator session on “Cybersecurity : Multidimensional cybersecurity measures- Current opportunities and challenges in using indices to understand cybersecurity”, a Second Open Consultation on the draft Guidelines for utilization of the GCA, and a High-Level dialogue on “AI Readiness Check: Policy Impact, Opportunities and Challenges”.

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

7.1 Child online protection was incorporated as one of the key elements into the fourth pillar in the ITU and UNICEF joint project Giga.

7.2 ITU has also signed a collaboration agreement with the SCORT Foundation on COP. ITU has contributed to many discussions such as the Safer Internet Day 2021 and the 15th European Football for Development Conference as well as in a round table discussion with European Football Clubs.

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 started in 2021 with the signature of an ITU internal project document. ITU has started implementing the project focusing on capacity building through the development of online self-paced trainings for all relevant stakeholders and other interactive solutions for children and young people to become responsible digital citizens.

7.4 All ITU regions started implementing activities of the Global Project on ‘Creating a safe and empowering cyber environment for children’. The first implementing country was Albania, followed by Malawi and Morocco.

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 moderated different virtual events, such as among others the Online Safety Moment at the [Girls in ICTs Day Celebration](https://www.itu.int/women-and-girls/girls-in-ict/girlsinict-online-safety-moment/) and the [Session 4: Safe Digital Inclusion - Child Online Protection](https://www.itu.int/en/ITU-D/Conferences/GSR/2021/Pages/global.aspx) at GSR2021.

7.6 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. In five episodes, the [Online Safety Course with Sango](https://www.itu-cop-guidelines.com/children) provides practical advice to children up to 9 years old on risks that they can face online.

7.7 Through the ITU Academy, ITU provided a training session for regulators on the Arab Region on child online protection.

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