|  |  |
| --- | --- |
| **Agenda item: PL 2** | **Document C24/18-E** |
| **18 April 2024** |
| **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 |
| **Purpose**This report summarizes ITU’s activities in 2023-2024 in relation to Resolution 130 (Rev. Bucharest, 2022), 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 by the Council**The Council is invited to **note** the report.**Relevant link(s) with the Strategic Plan**Advancing universal connectivity; sustainable digital transformation; inclusive and secure telecommunication/ICT infrastructure and services.**Financial implications**Within the allocated budget 2024-2025.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**References***Resolutions* [*71*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-071-E.pdf)*,* [*130*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-130-E.pdf)*,* [*140*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-140-E.pdf)*,* [*179*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-179-E.pdf) *(Rev. Bucharest, 2022) of the Plenipotentiary Conference; Resolution* [*174*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-174-E.pdf) *(Rev. Dubai, 2018),* [*181*](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-181-E.pdf) *(Guadalajara, 2010) of the Plenipotentiary Conference;* [*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, 2, 67, 69 (Rev. Kigali, 2022)*](https://www.itu.int/dms_pub/itu-d/opb/tdc/D-TDC-WTDC-2022-PDF-E.pdf)*; ITU-D priorities (*[*Kigali Action Plan*](https://www.itu.int/md/D14-WTDC17-C-0115/en)*); Resolutions* [*50 (Rev. Geneva, 2022)*](https://www.itu.int/pub/T-RES-T.50-2022)*,* [*52*](https://www.itu.int/pub/T-RES-T.52-2022) *(Rev. Hammamet, 2016),* [*75 (Rev. Geneva, 2022)*](https://www.itu.int/pub/T-RES-T.75-2022)*,* [*58 (Rev. Geneva, 2022)*](https://www.itu.int/pub/T-RES-T.58-2022) *of World Telecommunication Standardization Assembly, 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)*,* [*C22/18*](https://www.itu.int/md/S22-CL-C-0018/en)*,* [*C23/38*](https://www.itu.int/md/S23-CL-C-0038/en) |

This document reports on ITU’s activities in relation to Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference (PP), 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 ICTs.

Organized around the five pillars of the Global Cybersecurity Agenda (GCA), this report shows the complementary nature of existing ITU work programmes, including BDT, TSB, and BR activities in this domain.

**1. Legal measures**

As part of ITU-D Priority 5 of the Kigali Action Plan, and taking into account ITU-D Q 3/2, 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). ITU collaborates closely with partners such as the United Nations Office on Drugs and Crime (UNODC).

**2.** **Technical and procedural measures**

2.1 [ITU-T Study Group 17 (SG-17)](http://www.itu.int/ITU-T/studygroups/com17/) held two meetings in August/September 2023 and February/March 2024, established 82 [new standardization work items, and approved 25 new or revised Recommendations on security of 5G, cloud, IoT, ITS, digital twin network, quantum key distribution, authentication, digital financial services and other smart services](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). ITU-T SGs 5, 11, 13, 16 and 20 also approved recommendations on ICT security (see [catalogue of ITU-T Recommendations](https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx)) across a wide range of issues from circular economy, electromagnetic security, signalling procedures and protocols, cloud computing, quantum key distribution networks, trust in ICT, JPEG 2000 and oneM2M Security Solutions.

2.2 Several ITU-T focus groups, referenced on [this page](https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx), are also exploring the trust aspect of various emerging technologies as part of their work. For example, the Focus Group on metaverse (FG-MV) has approved 4 Technical Reports on issues such as Cyber risks, threats, and harms in the metaverse, and Embedding safety standards and user control of Personally Identifiable Information (PII) in the development of the metaverse.

2.3 ITU-T SG13 approved new Recommendations ITU-T Y.3060 "Autonomous Networks – overview of trust" and Y.TiAN-eval "Trustworthiness Evaluation for IMT-2020 and Beyond with Autonomous Network Functions" based on the ITU-T FG-AN deliverables.

2.4 SG11 continues its activities on [signalling security](https://itu.int/go/SIG-SECURITY) to combat attacks on telephone networks (e.g. telephone spam, robocalls, spoofing numbers, etc). After ITU-T Q.3057 (2020), which describes the use of digital signature (digital certificates) in the signalling exchange, Q.3062 (2022) “Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks” and Q.3063 (2022) “Signalling procedures of calling line identification authentication”, SG11 approved in 2023 amendments to SS7 and BICC related standards to support calling line identification authentication.

2.5 ITU-R has established clear security principles for International Mobile Telecommunication (IMT) (3G, 4G and 5G) networks. It has also issued Recommendations on security issues in network management architecture for digital satellite systems and performance enhancements of transmission control protocol over satellite networks (see [here](https://www.itu.int/pub/R-REC)). Information on Futuristic mobile technologies – “IMT for 2020 and beyond” can be found [here](https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx).

**3.** **Organizational structures**

3.1 Since 2012, ITU has been collaborating with Member States, partners, and global organizations to strengthen cybersecurity by creating national and regional Computer Incident Response Teams (CIRTs). Additionally, ITU conducts CIRT Maturity Assessments to further enhance CIRT capabilities. So far, ITU has assisted 84 countries by evaluating their cybersecurity readiness, leading to the establishment or improvement of National CIRTs. ITU is currently working on implementing CIRTs in three countries.

ITU continues to actively collaborates with the FIRST community to enhance the Computer Security Incident Response Team (CSIRT) Service Framework and revise training materials for capacity-building in managing national CIRT operations.

3.2 As of May 2024, ITU has organized over 42 international, regional, or national [CyberDrills](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) (including 3 Global CyberDrills), involving more than 140 countries and 2,500 professionals across all six ITU regions. The first-ever in-person global CyberDrill is planned in April 2024, hosted by the Cybersecurity Council of the United Arab Emirates.

**4. Capacity building**

4.1 BDT organized regional cybersecurity forums for all ITU regions to build capacity.

Following WTDC 2022, work on Question 3/2 continues ([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)).

4.2 ITU has built on the [Second edition of The Guide to Developing a National Cybersecurity Strategy](https://ncsguide.org/) (NCS), published in 2021 in collaboration with over 20 international partners, and is working with several countries and territories to advance their cybersecurity strategies through in-person table top exercises and Action Plan assessments in collaboration with the United Kingdom. ITU, in conjunction with stakeholders, plans to begin the process of updating The Guide to Developing a National Cybersecurity Strategy in 2025.

4.3 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), and the ITU Centres of Excellence and Academy Training Centres, ITU continues to deliver training activities and workshops in various areas of the cybersecurity domain. An [online self-paced training based](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx) on the NCS of the Guide was launched in 2021 and in 2023 reached over 730 participants from 131 countries through ITU Academy.

4.4 The fifth edition of the [ITU Global Cybersecurity Index](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) Questionnaire has worked with 172 countries to gather data. The GCI Expert Group recommended weightages and how to move to a tier-based reporting model, as requested in PP Resolution 130 (Rev. Bucharest, 2022), and WTDC Resolution 46 (Rev. Kigali, 2022).

4.5 In its efforts for cyber skills development, ITU has successfully completed three editions of the [Women in Cyber Mentorship Programme](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme.aspx). The third cohort has been launched in April 2023, with target groups in the Africa, Arab and Asia-Pacific regions. “[Her CyberTracks](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx)”, supported by GIZ and Microsoft, successfully targeted at women policy-makers and diplomats in 2023, and is expanding to tackle specific needs in incident response and cybercrime (in cooperation with UNODC).

4.6 ITU is working with 23 countries through [Cyber for Good](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyber4Good/Cyber4Good.aspx), supported by the Republic of Korea, providing free access to tools, trainings, and services through 5 ITU-D Sector Members, including NCS assessments, cyber vulnerability monitoring tools, and cyber skills trainings.

4.7 ITU worked with Organization of American States to develop a systems approach to cybersecurity education, and is working to develop in-country workshops and help countries take next steps using the framework.

4.8 ITU collaborated with the Kingdom of Sweden, Microsoft, and Global Forum for Cybersecurity Expertise (GFCE) on developing a Compendium on Mainstreaming Cybersecurity in Development.

**5. International cooperation**

5.1 ITU is enhancing relationships and [partnerships](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) with various regional/international organizations and initiatives, including OAS, ENISA, INTERPOL, ECOWAS, the World Bank, FIRST, the GFCE, and regional CSIRT/CERT associations, such as AP CERT, AFRICA CERT, and OIC CERT, with an aim to avoid unnecessary duplication and identify areas for collaboration.

5.2 Pursuant to [Decision 630](https://www.itu.int/md/S23-CL-C-0124/en) (Council 2023), ITU is developing an [informational resource](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Council/CD630/Global-Cybersecurity-Knowledgebase.aspx) to help Member States build their cybersecurity and cyber resilience capacity, and has invited Member States and other stakeholders to contribute best practices, resources and related information for this purpose.

5.3 As the lead facilitator for WSIS Action Line C5, ITU organized an Action Line C5 facilitator session on “Digital Resilience: The Next Frontier – Cyber and Space” at the [WSIS Forum 2023](https://www.itu.int/net4/wsis/forum/2023/en), which also had several sessions addressing trust and confidence in areas related to new and emerging technologies such as AI, Quantum and others as well as protection of women and children online, among others.

5.4 ITU has continued to engage with stakeholders in Open-ended Working Group on security of and in the use of ICTs (OEWG), providing inputs into its capacity development mapping exercise, understanding current cybersecurity needs based on the Global Cybersecurity Index, and showcasing the impact of the HerCyberTracks initiative.

5.5 ITU continues to participate as an observer in the work of the [Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes](https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home). UNODC serves as Secretariat for the Ad Hoc Committee.

5.6 ITU is collaborating with Member States to deliver its work, notably the Czech Republic, Germany, the Kingdom of Saudi Arabia, and the United Kingdom.

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

6.1 Pursuant to ITU’s collaboration agreement with the SCORT Foundation, ITU co-organized an event at WSIS Forum 2023 on “[Safe Play in the Digital Age: Child Online Safety and Sports](https://www.itu.int/net4/wsis/forum/2023/en/Agenda/Session/463)”, leveraging the power of sports to increase child online safety awareness.

6.2 ITU has been implementing the project “Creating a safe and empowering cyber environment for children”, pursuant to the agreement signed with the Kingdom of Saudi Arabia. This has involved the launch and implementation of a number of online self-paced trainings for all relevant stakeholders on ITU Academy. In mid-2023 ITU is set to launch two interactive solutions designed to help equip children and young people to become responsible digital citizens – a webapp and an online game.

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