|  |  |
| --- | --- |
| **Agenda item: PL.2** | **Document C25/18-E** |
| **16 May 2025** |
| **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 2024-2025 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. Busan, 2014),* [*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), [*C24/18*](https://www.itu.int/md/S24-CL-C-0018/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 lead 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 (SG17)](http://www.itu.int/ITU-T/studygroups/com17/) held two meetings in September 2024 and April 2025, established 50 [new standardization work items, and approved 36 new or revised Recommendations on security of Artificial Intelligence, International Mobile Telecommunication systems, cloud, Internet of Things, Intelligent Transport Systems, digital twin systems, quantum key distribution, access control, digital financial, privacy preserving and other smart services](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). ITU-T SGs 5, 11, 13, 15, 20 and 21 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 combating counterfeit and stolen ICT mobile devices, trustworthiness of IMT-2020 and beyond, infrastructure (e.g. power grid, passive optical network), fixed, mobile and satellite convergence, security of IoT, metaverse and smart cities, digital rights management for video/audio content distribution, and multimedia authenticity.

2.2 SG11 continues its activities on [signalling security](https://itu.int/go/SIG-SECURITY) to combat counterfeit and stolen ICT mobile devices and 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, and Q.5054 “Consumer centric framework for combating counterfeit and stolen ICT mobile devices” in 2025.

2.3 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)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx). Additionally, ITU conducts CIRT Maturity Assessments to further enhance CIRT capabilities. So far, ITU has assisted 85 countries by evaluating their cybersecurity readiness, leading to the establishment or improvement of National CIRTs. ITU is currently working on implementing CIRTs in four countries.

ITU continues to actively collaborate 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 2025, ITU has organized over 55 international, regional, or national [CyberDrills](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) (including 3 Global CyberDrills), involving more than 160 countries across all six ITU regions. The second global CyberDrill was held in May 2025, 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 is in the process of updating the Guide to Developing a National Cybersecurity Strategy (NCS) with 20 international partners. The updated guide will build on the [Second Edition](https://ncsguide.org/) published in 2021, and is expected to launch in Q4, 2025. ITU leverages the Guide when working with several countries and territories to advance their cybersecurity strategies through in-person tabletop exercises and Action Plan assessments, such as in collaboration with the United Kingdom and Japan.

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. For example, 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 launched in September 2024, working with 172 countries to gather data. The next edition of the GCI is expected to start data collection in early 2026.

4.5 In its efforts for cyber skills development, “[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 in policy-making and diplomacy, has addressed needs in incident response and cybercrime (in cooperation with UNODC) in 2024. Geographic reach for 2025 has expanded to include all African Union members, in addition to 5 countries from the Americas (in cooperation with OAS) and previously targeted countries in Europe.

4.6 ITU is working with 30 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 8 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](https://www.itu.int/hub/publication/d-phcb-cyb_educ-2024/), and is working to develop a guide for implementation for countries.

# 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 developed an [informational resource](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Council/CD630/Global-Cybersecurity-Knowledgebase.aspx) based on Member State responses, to help Member States build their cybersecurity and cyber resilience capacity. Nine (9) Member States have contributed to this resource.

5.3 As the lead facilitator for WSIS Action Line C5, ITU organized an Action Line C5 facilitator session on “[Beneath the Waves: Safeguarding Global Connectivity through Secure Submarine Networks](https://www.itu.int/net4/wsis/forum/2024/Agenda/Session/170)” at the [WSIS Forum 2024,](https://www.itu.int/net4/wsis/forum/2024/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. ITU plans to have a session related to Action Line C5 at the [WSIS Forum 2025](https://www.itu.int/net4/wsis/forum/2025/).

5.4 ITU has continued to engage with stakeholders in the [Open-ended Working Group on security of and in the use of ICTs (OEWG)](https://meetings.unoda.org/meeting/57871), 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 In November 2024, ITU also launched the [International Advisory Body on Submarine Cable Resilience](https://www.itu.int/digital-resilience/submarine-cables/advisory-body/) in partnership with the International Cable Protection Committee (ICPC), comprising 40 leaders and experts from the public and private sectors, with the aim of promoting dialogue and collaboration on potential ways and means to improve the resilience of this vital infrastructure that powers global communications and the digital economy. The first in-person meeting of the Body took place at the [International Submarine Cable Resilience Summit 2025 (Abuja, Nigeria, 26-27 February 2025)](https://www.itu.int/digital-resilience/submarine-cables/events/about-nigeria-summit/) that brough together governments, industry leaders, and international organizations to address critical challenges facing submarine cables.

# 6 Child Online Protection (COP)

6.1 As of April 2025, ITU has supported the development of national COP frameworks or related assessments in 13 countries: Albania, Armenia, Bahamas, Bhutan, Bolivia, Ecuador, Kazakhstan, Malawi, Mongolia, Pakistan, Peru, Suriname, and Thailand. Further policy assistance is being undertaken in Andorra, Eswatini, and Lebanon. These frameworks embed legal and regulatory measures that align with international standards and national child protection priorities.

6.2 Practical tools and digital learning resources have been central to ITU’s work on COP. To support national integration of child protection principles, 26 countries have translated the ITU COP Guidelines into local languages, including recent localisations into Quechua (Ecuador), Aymara (Bolivia), Dutch (Suriname), and Maltese during 2024-2025.

6.3 Ten online self-paced training courses were developed and made available through the ITU Academy, including a sector-specific course for the ICT industry launched in 2024 in partnership with UNICEF. In parallel, online trainings for children—tailored to three different age groups and co-developed with children—were released on Safer Internet Day 2025 in all six official UN languages.

6.4 Additional awareness-raising materials, including brochures and educational videos, were developed and deployed in countries such as in 2025 in Morocco to support national awareness raising campaigns. ITU further supported the roll-out of the COP Guidelines in Serbia in February 2024. Activities included a dissemination campaign and the presentation of newly translated materials in the national language. The campaign successfully reached 957 children, along with 60 teachers, pedagogues, and psychologists.

6.5 A total of around 170 000 children have participated in educational and empowerment activities focused on online safety, while 2 500 parents and educators and 1 000 government stakeholders have received training through workshops, Training of Trainers (ToT) sessions, and e-learning programmes. These capacity-building efforts have been implemented across all ITU regions, with ToT programmes conducted in countries such as the Bahamas, Costa Rica, Ecuador, Kyrgyzstan, Maldives, Malawi, Malta, Micronesia, Morocco, and Suriname. Additional country-level efforts have further expanded the reach of COP capacity-building. In Ecuador, in collaboration with the Scort Foundation, a training webinar was held for young sports coaches to raise awareness on COP in sports contexts. Furthermore, training sessions were conducted for policymakers, the ICT industry, and civil society actors in Ecuador.

6.6 The Protection through Online Participation (PoP) initiative, co-led by ITU and the UN Special Representative of the Secretary-General on Violence Against Children, brings together over 30 partners from across the UN system, technology platforms, civil society organizations, and academia. The initiative is developing guiding principles for policy-makers, child helplines, and technology platforms, which are scheduled for release in 2025. In parallel, ITU is collaborating with the Committee on the Rights of the Child, UNICEF, and more than ten co-signatory agencies to finalize an interagency Joint Statement on Artificial Intelligence and child online protection, expected to be adopted by the Committee in 2025.

6.7 In terms of Research and Innovation, findings emerging from the PoP initiative—including engagement with child helplines, digital platforms and service providers, and children and young people—has highlighted the dual nature of digital environments as spaces of potential harm and critical channels for accessing support services. These insights are shaping a shift toward a more empowering and preventive approach to online child protection. In addition, ITU has launched a global research collaboration with the World Health Organization (WHO) in late 2024 to establish a Global Online Safety Prevention Education and Resource Network. Recognizing the importance of child participation, throughout 2024 and 2025, ITU has enabled the creation of child taskforces in Indonesia, Malawi, and Lebanon, enabling children to contribute directly to the development of national COP strategies.

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