|  |  |
| --- | --- |
| **Point de l'ordre du jour: PL 2** | **Document C25/18-F** |
| **16 mai 2025** |
| **Original: anglais** |
|  |  |
| Rapport de la Secrétaire générale |
| ACTIVITÉS DE L'UIT RELATIVES AU RENFORCEMENT DU RÔLE DE L'UNION DANS L'INSTAURATION DE LA CONFIANCE ET DE LA SÉCURITÉ DANS L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION |
| **Objet**Le présent rapport rend compte des activités menées par l'UIT en 2024-2025 au titre de la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires, du rôle de l'UIT en tant que coordonnateur unique pour la grande orientation C5 du SMSI et des autres décisions prises par les membres concernant le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC).**Suite à donner par le Conseil**Le Conseil est invité à **prendre note** du présent rapport.**Lien(s) pertinent(s) avec le plan stratégique**Promouvoir la connectivité universelle; transformation numérique durable; infrastructures et services de télécommunication/TIC inclusifs et sûrs.**Incidences financières**Les coûts sont couverts par le budget affecté pour 2024-2025.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Références**Résolutions [71](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-071-F.pdf), [130](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-130-F.pdf), [140](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-140-F.pdf), [179 (Rév. Bucarest, 2022)](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-179-F.pdf) de la Conférence de plénipotentiaires; Résolutions [174 (Rév. Busan, 2014)](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-174-F.pdf), [181 (Guadalajara, 2010)](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-181-F.pdf) de la Conférence de plénipotentiaires; [Règlement des télécommunications internationales (Rév. Dubaï, 2012)](http://www.itu.int/pub/S-CONF-WCIT-2012/fr); Résolution [1306](https://www.itu.int/md/S15-CL-C-0109/fr) du Conseil; [Résolutions 45, 2, 67 et 69 (Rév. Kigali, 2022)](https://www.itu.int/dms_pub/itu-d/opb/tdc/D-TDC-WTDC-2022-PDF-F.pdf) de la CMDT; Priorités de l'UIT-D ([Plan d'action de Kigali](https://www.itu.int/md/D14-WTDC17-C-0115/fr)); Résolutions [50 (Rév. Genève, 2022)](https://www.itu.int/pub/T-RES-T.50-2022/fr), [52 (Rév. Hammamet, 2016)](https://www.itu.int/pub/T-RES-T.52-2022/fr), [75 (Rév. Genève, 2022)](https://www.itu.int/pub/T-RES-T.75-2022/fr), [58 (Rév. Genève, 2022)](https://www.itu.int/pub/T-RES-T.58-2022/fr) de l'Assemblée mondiale de normalisation des télécommunications; Documents [C15/18](http://www.itu.int/md/S15-CL-C-0018/fr), [C16/18](https://www.itu.int/md/S16-CL-C-0018/fr), [C17/18](https://www.itu.int/md/S17-CL-C-0018/fr), [C18/18](https://www.itu.int/md/S18-CL-C-0018/fr), [C19/18](https://www.itu.int/md/S19-CL-C-0018/fr), [C20/18](https://www.itu.int/md/S20-CL-C-0018/fr), [C21/18](https://www.itu.int/md/S21-CL-C-0018/fr), [C22/18](https://www.itu.int/md/S22-CL-C-0018/fr), [C23/38](https://www.itu.int/md/S23-CL-C-0038/fr) et [C24/18](https://www.itu.int/md/S24-CL-C-0018/en) du Conseil. |

Le présent rapport rend compte des activités menées par l'UIT au titre de la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires (PP), du rôle de l'UIT en tant que coordonnateur principal pour la grande orientation C5 du SMSI et des autres décisions prises par les membres concernant le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des TIC.

Le présent rapport, structuré d'après les cinq piliers du Programme mondial cybersécurité (GCA), fait apparaître la complémentarité des programmes de travail existants de l'UIT, y compris des activités menées par le BDT, le TSB et le BR dans ce domaine.

# 1 Mesures juridiques

Dans le cadre de la Priorité 5 du Secteur du développement des télécommunications de l'UIT (UIT-D) définie dans le Plan d'action de Kigali, et compte tenu de la Question 3/2 confiée à la Commission d'études 2 de l'UIT-D, l'UIT aide les États Membres à comprendre les aspects juridiques de la cybersécurité, en mettant à leur disposition ses [ressources sur la législation relative à la cybercriminalité](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx). L'UIT collabore étroitement avec des partenaires tels que l'Office des Nations Unies contre la drogue et le crime (ONUDC).

# 2 Mesures techniques et de procédure

2.1 La [Commission d'études 17 de l'UIT-T (CE 17)](https://www.itu.int/fr/ITU-T/studygroups/2022-2024/17/Pages/default.aspx) a tenu deux réunions en septembre 2024 et en avril 2025, lors desquelles elle a établi 50 nouveaux sujets d'étude en matière de normalisation et approuvé 36 Recommandations nouvelles ou révisées sur la sécurité de l'intelligence artificielle, les systèmes de télécommunications mobiles internationales, l'informatique en nuage, l'Internet des objets (IoT), les systèmes de transport intelligents (ITS), les systèmes de jumeaux numériques, la distribution de clés quantiques, le contrôle des accès, les services financiers numériques, la protection de la vie privée et d'autres services intelligents. Les CE 5, 11, 13, 15, 20 et 21 de l'UIT-T ont également approuvé des Recommandations relatives à la sécurité des TIC (voir le [catalogue des Recommandations UIT-T](https://www.itu.int/fr/ITU-T/publications/Pages/recs.aspx)) dans plusieurs domaines dont la lutte contre la contrefaçon et le vol de dispositifs mobiles TIC, la fiabilité des IMT-2020 et des systèmes ultérieurs, les infrastructures (par exemple le réseau électrique ou le réseau optique passif), la convergence fixe, mobile et satellite, la sécurité de l'IoT, le métavers et les villes intelligentes, la gestion des droits numériques pour la diffusion de contenus vidéo et audio et l'authenticité des contenus multimédias.

2.2 La CE 11 poursuit ses activités en matière de [sécurité de la signalisation](https://itu.int/go/SIG-SECURITY), afin de lutter contre la contrefaçon et le vol de dispositifs mobiles TIC et contre les attaques visant les réseaux téléphoniques (par ex. le spam téléphonique, les appels robotisés, l'usurpation des numéros, etc.). Par suite de l'adoption de la Recommandation UIT-T Q.3057 (2020), qui décrit l'utilisation de la signature numérique (certificats numériques) dans les échanges de signalisation, ainsi que des Recommandations UIT-T Q.3062 (2022) "Procédures et protocoles de signalisation visant à permettre l'interconnexion entre entités de réseau de confiance à l'appui des réseaux existants ou nouveaux" et Q.3063 (2022) "Procédures de signalisation pour l'authentification de l'identification de la ligne appelante", la CE 11 a approuvé en 2023 des amendements aux normes relatives au système de signalisation N° 7 (SS7) et à la commande BICC, afin de prendre en charge l'authentification de l'identification de la ligne appelante, ainsi que la Recommandation Q.5054 "Cadre axé sur le consommateur pour la lutte contre la contrefaçon et le vol de dispositifs mobiles TIC" en 2025.

2.3 L'UIT-R a défini des principes de sécurité précis concernant les réseaux des Télécommunications mobiles internationales (IMT) (3G, 4G et 5G). Il a également publié des Recommandations sur les questions de sécurité relatives à l'architecture de gestion des réseaux pour les systèmes numériques à satellites et sur l'amélioration de la qualité de fonctionnement du protocole de commande de transmission sur les réseaux à satellite (voir [ici](https://www.itu.int/pub/R-REC/fr)). Des informations relatives aux technologies mobiles futuristes prévues pour les "IMT à l'horizon 2020 et au-delà" sont disponibles [ici](https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx).

# 3 Structures institutionnelles

3.1 Depuis 2012, l'UIT collabore avec des États Membres, des partenaires et des organisations mondiales en vue de renforcer la cybersécurité, moyennant la création d'[équipes d'intervention en cas d'incident informatique (CIRT)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx) aux niveaux national et régional. De plus, l'UIT mène des évaluations du niveau de maturité des équipes CIRT afin d'améliorer encore les capacités de ces équipes. Jusqu'à présent, l'UIT a fourni une assistance à 85 pays, dans le cadre de l'évaluation de leur état de préparation en matière de cybersécurité, en vue de créer des équipes nationales CIRT ou d'améliorer les équipes existantes. L'UIT travaille actuellement à la mise en place d'équipes CIRT dans quatre pays.

L'UIT continue de collaborer activement avec le Forum pour les équipes d'intervention en cas d'incident (FIRST), en vue de renforcer le cadre de services des équipes de réponse aux incidents de sécurité informatique (CSIRT) et de réviser des supports de formation pour le renforcement des capacités dans la gestion des interventions des équipes CIRT nationales.

3.2 Au mois de mai 2025, l'UIT avait organisé 55 [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) internationaux, régionaux ou nationaux (y compris trois cyberexercices mondiaux), auxquels plus de 160 pays des six régions de l'UIT ont pris part. Le deuxième cyberexercice mondial en présentiel s'est tenu en mai 2025, à l'aimable invitation du Conseil de la cybersécurité des Émirats arabes unis.

# 4 Renforcement des capacités

4.1 Le BDT a organisé des forums régionaux sur la cybersécurité à l'intention de toutes les régions de l'Union, afin de renforcer leurs capacités dans ce domaine.

Après la CMDT-22, les travaux relatifs à la Question 3/2 ([Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité](https://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=2&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2)) se poursuivent.

4.2 L'UIT met actuellement à jour le Guide sur l'élaboration d'une stratégie nationale en matière de cybersécurité, en collaboration avec 20 partenaires internationaux. Le Guide sera actualisé sur la base de la [deuxième édition](https://ncsguide.org/) publiée en 2021 et devrait être diffusé au cours du quatrième trimestre de l'année 2025. L'UIT s'appuie sur ce Guide dans le cadre des travaux qu'elle mène avec plusieurs pays et territoires pour faire progresser les stratégies de ces derniers dans le domaine de la cybersécurité, moyennant des exercices de simulation en présentiel et l'évaluation des plans d'action, notamment en collaboration avec le Royaume‑Uni et le Japon.

4.3 Par l'intermédiaire de [l'Académie de l'UIT](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), des Centres d'excellence de l'UIT et des Centres de formation de l'Académie de l'UIT, l'Union continue de proposer des activités de formation et des ateliers dans divers domaines liés à la cybersécurité. Par exemple, un [cours de formation en ligne adapté au rythme de chacun](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx) sur les stratégies nationales en matière de cybersécurité a été lancé en 2021 et suivi en 2023 par plus de 730 participants issus de 131 pays via l'Académie de l'UIT.

4.4 La cinquième édition du questionnaire sur l'[Indice mondial de cybersécurité (GCI) de l'UIT](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) a été diffusée en septembre 2024 auprès de 172 pays afin de recueillir des données. Le prochain questionnaire sur l'Indice GCI devrait permettre de commencer la collecte de données au début de l'année 2026.

4.5 Dans le cadre des efforts qu'elle déploie pour renforcer les compétences en matière de cybersécurité, l'Initiative "[Her CyberTracks](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx)", soutenue par l'Agence allemande pour la coopération internationale (GIZ) et Microsoft, s'est adressée avec succès aux décideuses et aux femmes diplomates, et a permis de répondre aux besoins particuliers en matière d'intervention en cas d'incident et de cybercriminalité (en coopération avec l'ONUDC) en 2024. En 2025, la portée géographique de cette initiative a été élargie pour inclure tous les membres de l'Union africaine, ainsi que cinq pays de la région Amériques (en coopération avec l'OEA) et des pays d'Europe précédemment ciblés.

4.6 L'UIT coopère actuellement avec 30 pays dans le cadre du projet "[La cybersécurité au service du bien social](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyber4Good/Cyber4Good.aspx)", soutenu par la République de Corée, en vue d'assurer un accès gratuit à des outils, des formations et des services par l'intermédiaire de huit Membres du Secteur de l'UIT-D, comprenant des évaluations sur les stratégies nationales de cybersécurité, des outils de suivi de la vulnérabilité dans le cyberespace et des formations aux compétences en matière de cybersécurité.

4.7 L'UIT a coopéré avec l'Organisation des États américains pour définir une [approche systémique concernant l'éducation à la cybersécurité](https://www.itu.int/hub/publication/d-phcb-cyb_educ-2024/#/fr), et s'efforce actuellement d'élaborer un guide de mise en œuvre destiné aux pays concernés.

# 5 Coopération internationale

5.1 L'UIT renforce ses relations et ses [partenariats](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) avec diverses organisations et initiatives régionales ou internationales, notamment l'OEA, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), INTERPOL, la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), la Banque mondiale, le Forum FIRST, le Forum GFCE et les associations régionales d'équipes CSIRT/CERT, comme AP CERT, AFRICA CERT et OIC CERT, en vue d'éviter le chevauchement inutile d'activités et d'identifier les domaines dans lesquels une collaboration peut être instaurée.

5.2 Conformément à la [Décision 630 (Conseil 2023)](https://www.itu.int/md/S23-CL-C-0124/fr), l'UIT a mis en place des [sources d'information](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Council/CD630/Global-Cybersecurity-Knowledgebase.aspx) basées sur les réponses fournies par les États Membres afin de les aider à renforcer leurs capacités en matière de cybersécurité et de cyberrésilience. Neuf (9) États Membres ont contribué à l'élaboration de ces sources d'information.

5.3 En tant que coordonnateur principal pour la grande orientation C5 du SMSI, l'UIT a organisé une séance de coordination pour cette grande orientation, sur le thème "[Sous les vagues: préserver la connectivité mondiale grâce à des réseaux sous-marins sécurisés](https://www.itu.int/net4/wsis/forum/2024/fr/Agenda/Session/170)", lors du [Forum de 2024 du SMSI](https://www.itu.int/net4/wsis/forum/2024/fr). Dans le cadre du Forum, plusieurs séances ont été organisées sur la confiance dans les domaines liés aux technologies nouvelles et émergentes, comme l'intelligence artificielle (IA) et les technologies quantiques, ainsi que sur la protection en ligne des femmes et des enfants. L'UIT prévoit d'organiser une session sur la grande orientation C5 lors du [Forum de 2025 du SMSI](https://www.itu.int/net4/wsis/forum/2025/fr).

5.4 L'UIT a continué de travailler avec les parties prenantes dans le cadre du [Groupe de travail à composition non limitée sur la sécurité des TIC et de leur utilisation (OEWG)](https://meetings.unoda.org/meeting/57871), en contribuant à l'exercice de mise en correspondance des activités de renforcement des capacités du Groupe, en acquérant une meilleure compréhension des besoins actuels en matière de cybersécurité à l'aide de l'Indice mondial de cybersécurité et en présentant les retombées de l'Initiative "HerCyberTracks".

5.5 En novembre 2024, l'UIT a également mis en place [l'Organe consultatif international sur la résilience des câbles sous-marins](https://www.itu.int/digital-resilience/submarine-cables/advisory-body/#/fr), en partenariat avec le Comité international de protection des câbles (CIPC), composé de 40 dirigeants et experts des secteurs public et privé, dans le but de promouvoir le dialogue et la collaboration sur les moyens pouvant être mis en œuvre pour améliorer la résilience de cette infrastructure essentielle aux communications mondiales et à l'économie numérique. La première réunion en présentiel de cet Organe a eu lieu à l'occasion du [Sommet international sur la résilience des câbles sous-marins de 2025 à Abuja (Nigéria), les 26 et 27 février 2025](https://www.itu.int/digital-resilience/submarine-cables/events/about-nigeria-summit/#/fr), et a réuni des gouvernements, des dirigeants du secteur et des organisations internationales en vue de surmonter les défis de taille qui se posent pour les câbles sous-marins.

# 6 Protection en ligne des enfants (COP)

6.1 En avril 2025, l'UIT a soutenu l'élaboration de cadres nationaux relatifs à la protection en ligne des enfants ou d'évaluations en la matière dans les 13 pays suivants: Albanie, Arménie, Bahamas, Bhoutan, Bolivie, Équateur, Kazakhstan, Malawi, Mongolie, Pakistan, Pérou, Suriname et Thaïlande. D'autres mesures d'aide en matière de politiques sont mises en œuvre en Andorre, en Eswatini et au Liban. Ces cadres intègrent des mesures juridiques et réglementaires qui s'alignent sur les normes internationales et les priorités nationales en matière de protection de l'enfance.

6.2 Les outils pratiques et les ressources d'apprentissage numériques sont au cœur des travaux de l'UIT en matière de protection en ligne des enfants. Pour favoriser l'intégration des principes relatifs à la protection de l'enfance à l'échelle nationale, vingt-six pays ont récemment traduit les Lignes directrices de l'UIT sur la protection en ligne des enfants dans leurs langues locales, y compris en quechua (Équateur), en aymara (Bolivie), en néerlandais (Suriname) et en maltais au cours de la période 2024-2025.

6.3 Dix formations en ligne à suivre à son propre rythme ont été mises au point et mises à disposition par l'intermédiaire de l'Académie de l'UIT, dont une formation destinée au secteur des TIC lancé en 2024 en partenariat avec l'UNICEF. En parallèle, des formations en ligne, adaptées à trois groupes d'âge différents, destinées aux enfants et élaborées grâce à leur collaboration, ont été diffusées lors de l'édition de 2025 de la Journée pour un Internet plus sûr dans les six langues officielles de l'ONU.

6.4 Des supports de sensibilisation supplémentaires, notamment des brochures et des vidéos pédagogiques, ont été élaborés et diffusés dans certains pays, comme au Maroc en 2025, pour soutenir les campagnes nationales de sensibilisation. L'UIT a également soutenu la mise en œuvre des Lignes directrices sur la protection en ligne des enfants en Serbie en février 2024. Il était notamment question d'une campagne de diffusion et de présentation des documents nouvellement traduits dans la langue nationale. La campagne a permis de sensibiliser 957 enfants, ainsi que 60 enseignants, pédagogues et psychologues.

6.5 Au total, environ 170 000 enfants ont participé à des activités d'éducation et d'autonomisation axées sur la sécurité en ligne, tandis que 2 500 parents et éducateurs ainsi que 1 000 parties prenantes gouvernementales ont reçu une formation par le biais d'ateliers, de sessions de formation à l'intention des formateurs et de programmes d'apprentissage en ligne. Ces activités de renforcement des capacités ont été mises en œuvre dans toutes les régions de l'UIT, des programmes de formation à l'intention des formateurs ayant été menés dans des pays tels que les Bahamas, le Costa Rica, l'Équateur, le Kirghizistan, les Maldives, le Malawi, Malte, la Micronésie, le Maroc et le Suriname. D'autres initiatives menées à l'échelle nationale ont permis d'élargir la portée des activités de renforcement des capacités en matière de protection en ligne des enfants. En Équateur, un webinaire de formation destiné aux jeunes entraîneurs sportifs a été organisé, en collaboration avec la Fondation Scort, afin de les sensibiliser à la protection en ligne des enfants dans des contextes sportifs. En outre, des sessions de formation ont été organisées à l'intention des décideurs, des représentants du secteur des TIC et des acteurs de la société civile en Équateur.

6.6 L'initiative sur la protection par la participation en ligne (PoP), codirigée par l'UIT et la Représentante spéciale du Secrétaire général de l'ONU chargée de la question de la violence à l'encontre des enfants, rassemble plus de 30 partenaires issus du système des Nations Unies et représentants de plates-formes technologiques, d'organisations de la société civile et d'universités. Les membres de cette initiative élaborent des principes directeurs à l'intention des décideurs, des lignes d'appel d'urgence pour les enfants et des plates-formes technologiques, dont la publication est prévue en 2025. Parallèlement, l'UIT collabore avec le Comité des droits de l'enfant, l'UNICEF et plus de dix institutions cosignataires dans le but de rédiger une Déclaration commune interinstitutions sur l'intelligence artificielle et la protection en ligne des enfants, qui devrait être adoptée par le Comité en 2025.

6.7 Dans le domaine de la recherche et de l'innovation, les conclusions formulées par les membres de l'initiative PoP, grâce à la collaboration de lignes d'appel d'urgence pour les enfants, de plates-formes numériques, de fournisseurs de services, d'enfants et de jeunes, mettent en évidence la double nature des environnements numériques, qui constituent à la fois des espaces potentiellement dangereux et des canaux essentiels pour accéder aux services d'aide. Ces résultats ouvrent la voie à une méthode davantage axée sur l'autonomisation et la prévention en ce qui concerne la protection en ligne des enfants.

En outre, fin 2024, l'UIT a lancé un programme de collaboration mondiale en matière de recherche avec l'Organisation mondiale de la Santé (OMS) afin de mettre en place un réseau mondial d'éducation, de partage de ressources et de prévention dans le domaine de la sécurité en ligne. Reconnaissant l'importance de la participation des enfants, l'UIT a permis en 2024 et 2025 la création de groupes d'action composés d'enfants en Indonésie, au Malawi et au Liban, afin de leur permettre de contribuer directement à l'élaboration de stratégies nationales relatives à la protection en ligne des enfants.

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