|  |  |
| --- | --- |
| **Point de l'ordre du jour: PL 2** | **Document C24/18-F** |
| **18 avril 2024** |
| **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 2023-2024 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. Dubaï, 2018)*](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/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) *et* [*C23/38*](https://www.itu.int/md/S23-CL-C-0038/fr) *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 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 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 août/septembre 2023 et en février/mars 2024, lors desquelles elle a établi 82 [nouveaux sujets d'étude en matière de normalisation et approuvé 25 Recommandations nouvelles ou révisées sur la sécurité de la 5G, l'informatique en nuage, l'Internet des objets, les systèmes de transport intelligents (ITS), les réseaux de jumeaux numériques, la distribution de clés quantiques, l'authentification, les services financiers numériques et d'autres services intelligents](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). Les CE 5, 11, 13, 16 et 20 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 l'économie circulaire, la sécurité électromagnétique, les procédures et protocoles de signalisation, l'informatique en nuage, les réseaux de distribution de clés quantiques, la confiance dans les TIC, le système JPEG 2000 et les solutions de sécurité oneM2M.

2.2 Dans le cadre de leurs travaux, plusieurs groupes spécialisés de l'UIT-T (dont la liste est disponible sur [cette page](https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx)) étudient actuellement les aspects liés à la confiance pour diverses technologies émergentes. Par exemple, le Groupe spécialisé sur le métavers (FG-MV) a approuvé quatre rapports techniques sur des questions telles que les cyberrisques, les menaces et les dangers dans le métavers et l'intégration des normes de sécurité et du contrôle par les utilisateurs des informations d'identification personnelle (PII) dans le développement du métavers.

2.3 La CE 13 de l'UIT-T a approuvé les nouvelles Recommandations UIT-T Y.3060 "Réseaux autonomes – aperçu de la confiance" et Y.TiAN-eval "Évaluation de la fiabilité des systèmes IMT-2020 et au-delà dotés de fonctions de réseau autonomes", sur la base des produits du Groupe spécialisé de l'UIT-T sur les réseaux autonomes (FG-AN).

2.4 La CE 11 poursuit ses activités en matière de [sécurité de la signalisation](https://itu.int/go/SIG-SECURITY), afin de lutter 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.

2.5 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) 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 84 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 trois 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 2024, l'UIT avait organisé 42 [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) internationaux, régionaux ou nationaux (y compris trois cyberexercices mondiaux), auxquels plus de 140 pays et 2 500 professionnels des six régions de l'UIT ont pris part. Le tout premier cyberexercice mondial en présentiel aura lieu en avril 2024, 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 s'est appuyée sur la [deuxième édition du Guide sur l'élaboration d'une stratégie nationale en matière de cybersécurité](https://ncsguide.org/), publiée en 2021 en collaboration avec 20 partenaires internationaux, et travaille actuellement 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 en collaboration avec le Royaume-Uni. L'UIT, en concertation avec les parties prenantes, prévoit de lancer le processus de mise à jour de ce Guide en 2025.

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. 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 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 auprès de 172 pays afin de recueillir des données. Le Groupe d'experts sur l'Indice GCI a fait des recommandations en matière de pondération et sur la manière de passer à un modèle de présentation de l'information fondé sur des niveaux, conformément à la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires et à la Résolution 46 (Rév. Kigali, 2022) de la CMDT.

4.5 Dans le cadre des efforts qu'elle déploie pour renforcer les compétences en matière de cybersécurité, l'UIT a mené à bien avec succès trois éditions du [Programme de mentorat intitulé "Les femmes dans le secteur de la cybersécurité"](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme.aspx). La troisième édition a été lancée en avril 2023, avec des groupes cibles en Afrique, en Asie-Pacifique et dans la région des États arabes. L'Initiative "[Her CyberTracks](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx)", soutenue par GIZ et Microsoft, s'est adressée avec succès aux décideuses et aux femmes diplomates en 2023, et est en passe d'être élargie pour répondre aux besoins particuliers en matière d'intervention en cas d'incident et de cybercriminalité (en coopération avec l'ONUDC).

4.6 L'UIT coopère actuellement avec 23 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 cinq 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, et s'efforce actuellement d'organiser des ateliers au niveau national et d'aider les pays à franchir de nouvelles étapes en utilisant le cadre.

4.8 L'UIT a collaboré avec le Royaume de Suède, Microsoft et le Forum mondial sur la cyberexpertise (GFCE) concernant la création d'un recueil consacré à l'intégration de la cybersécurité dans le développement.

# 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 met actuellement en place des [sources d'information](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Council/CD630/Global-Cybersecurity-Knowledgebase.aspx) visant à aider les États Membres à renforcer leurs capacités en matière de cybersécurité et de cyberrésilience, et a invité les États Membres ainsi que d'autres parties prenantes à contribuer à ces efforts en fournissant des bonnes pratiques, des ressources et des informations dans ce domaine.

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 "Résilience numérique: la nouvelle frontière – le monde numérique et l'espace", lors du [Forum de 2023 du SMSI](https://www.itu.int/net4/wsis/forum/2023/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, pour ne citer que ces exemples.

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), 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 L'UIT continue de participer en tant qu'observateur aux travaux du [Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des TIC à des fins criminelles](https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home). Le secrétariat du Comité spécial est assuré par l'ONUDC.

5.6 L'UIT collabore avec des États Membres pour s'acquitter de sa mission, notamment avec la République tchèque, l'Allemagne, le Royaume d'Arabie saoudite et le Royaume-Uni.

# 6 Protection en ligne des enfants (COP)

6.1 Dans le cadre de leur accord de collaboration, l'UIT et la Fondation SCORT ont organisé conjointement une manifestation lors du Forum de 2023 du SMSI, sur le thème "[Jouer en toute sécurité à l'ère du numérique: le sport au service de la sécurité en ligne des enfants](https://www.itu.int/net4/wsis/forum/2023/fr/Agenda/Session/463)", afin de tirer parti du potentiel de ce secteur pour sensibiliser davantage à la sécurité en ligne des enfants.

6.2 Conformément à l'accord signé avec le Royaume d'Arabie saoudite, l'UIT met en œuvre le projet "Créer un cyberenvironnement sûr et de nature à autonomiser les enfants", dans le cadre duquel un certain nombre de cours de formation en ligne adaptés au rythme de chacun sont dispensés à toutes les parties prenantes concernées, par l'intermédiaire de l'Académie de l'UIT. Il était prévu que l'UIT présente, à la mi-2023, deux solutions interactives – une application web et un jeu en ligne – destinées à donner les moyens aux enfants et aux jeunes de devenir des citoyens responsables de la société du numérique.

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