|  |  |
| --- | --- |
| **Conseil 2021Consultation virtuelle des conseillers, 8-18 juin 2021** |  |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.4** | **Document C21/18-F** |
| **22 février 2021** |
| **Original: anglais** |
| Rapport du Secrétaire général |
| 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 |

|  |
| --- |
| RésuméLe présent rapport résume les activités menées par l'UIT en 2020 au titre de la Résolution 130 (Rév. Dubaï, 2018) 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).La version de 2020 du présent rapport (Document C20/18) a été établie en vue de sa soumission au Conseil à sa session de 2020, mais n'a pas été examinée.Suite à donnerLe Conseil est invité à **prendre note** du présent rapport et du Document C20/18.\_\_\_\_\_\_\_\_\_\_\_\_Références*Résolutions* [*71*](https://www.itu.int/en/council/2019/Documents/basic-texts/RES-071-F.pdf)*,* [*130*](https://www.itu.int/en/council/2019/Documents/basic-texts/RES-130-F.pdf)*,* [*140*](https://www.itu.int/en/council/2019/Documents/basic-texts/RES-140-F.pdf)*,* [*174*](https://www.itu.int/en/council/2019/Documents/basic-texts/RES-174-F.pdf)*,* [*179*](https://www.itu.int/en/council/2019/Documents/basic-texts/RES-179-F.pdf) *(Rév. Dubaï, 2018) et* [*181*](https://www.itu.int/en/council/2019/Documents/basic-texts/RES-181-F.pdf) *(Guadalajara, 2010) de la Conférence de plénipotentiaires,* [*Règlement des télécommunications internationales*](https://www.itu.int/pub/S-CONF-WCIT-2012/fr) *(Rév.Dubaï, 2012),* [*Résolution 1306*](https://www.itu.int/md/S15-CL-C-0109/en) *du Conseil, Résolutions*[*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf) *(Rév.Dubaï, 2014) et* [*2, 67 et 69 (Rév.Buenos Aires, 2017)*](https://www.itu.int/md/D14-WTDC17-C-0115/en) *de la Conférence mondiale de développement des télécommunications, Objectif 2/Produit 2.2 de l'UIT-D (*[*Plan d'action de Buenos Aires*](https://www.itu.int/md/D14-WTDC17-C-0115/en)*), Résolutions* [*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) *(Rév.Hammamet, 2016) et* [*58*](https://www.itu.int/pub/T-RES-T.58-2016) *(Rév.Dubaï, 2012) de l'Assemblée mondiale de normalisation des télécommunications, Documents récents du Conseil –* [*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) *et* [*C20/18*](https://www.itu.int/md/S20-CL-C-0018/en) |

# 1 Activités relatives à la cybersécurité et à la lutte contre le spam

1.1 Le développement des TIC, étayé par la sécurité et la confiance, est reconnu comme un facteur essentiel du développement durable. Le présent rapport, qui s'articule autour des cinq piliers du [Programme mondial cybersécurité (GCA)](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx), fait apparaître la complémentarité des programmes de travail existants de l'UIT et vise à faciliter la mise en œuvre des activités menées par le BDT, le TSB et le BR dans ce domaine.

# 2 Cadre législatif

2.1 Dans le cadre de l'Objectif 2.2 du Plan d'action de Buenos Aires, et compte tenu de la Question 3/2 (ancienne Question 22/1) confiée à la Commission d'études (CE) 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), afin de contribuer à l'harmonisation de leurs cadres juridiques. En ce qui concerne le cadre législatif, l'UIT collabore étroitement avec des partenaires tels que l'Office des Nations Unies contre la drogue et le crime (ONUDC) et d'autres organisations compétentes qui fournissent une assistance aux États Membres.

# 3 Mesures techniques et procédures

3.1 La [Commission d'études 17](http://www.itu.int/ITU-T/studygroups/com17/) (CE 17) de l'UIT-T, en sa qualité de commission d'études directrice chargée de la sécurité et de la gestion d'identité (IdM), continue de contribuer aux études et à la normalisation concernant la cybersécurité, la lutte contre le spam, la gestion d'identité, les certificats UIT-T X.509, la gestion de la sécurité de l'information, les réseaux de capteurs ubiquitaires, la télébiométrie, la sécurité mobile, la sécurité de la virtualisation dans l'optique de la sécurité de l'informatique en nuage, la protection des informations d'identification personnelle ainsi que l'architecture de la sécurité et de la sécurité des applications, conjointement avec des organisations de normalisation extérieure.

3.2 Depuis le dernier rapport à l'intention du Conseil, la CE 17 a tenu une réunion en septembre 2020, à laquelle elle a défini [15 nouveaux sujets d'étude en matière de normalisation](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17), et une séance plénière électronique, le 7 janvier 2021. Elle a approuvé plus de 40 Recommandations nouvelles ou révisées portant sur la sécurité des TIC, à savoir: [X.510 | ISO/CEI 9594-11](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14320); séries [X.680-690](https://www.itu.int/rec/T-REC-x/en); [X.1046](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1046); [X.1052 (révisée)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14044) et [X.1054 (révisée, en cours d'approbation)](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1054); [X.1148](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14249); [X.1149](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14250); [X.1216](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14259), [X.1217](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1217) et [X.1218](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14444); [X.1254 (révisée)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14260), [X.1279](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14261), [D.1140/X.1261](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1261), [X.1451](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14252) et [X.1452](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14451); [X.1363](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14087), [X.1364](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14088), [X.1365](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14089), [X.1366](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14262), [X.1367](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14263) et [X.1368](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1368); [X.1371](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14090), [X.1374](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14446), [X.1375](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14447), [X.1376](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1376), [X.1400](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14449), [X.1401](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14092), [X.1402](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14251), [X.1403](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14264), [X.1404](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14450) et [X.1606](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14265); [X.1710](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14452) et [X.1714](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14453); [X.1750](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14266), [X.1751](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14267) et X.1811 (en cours d'approbation).

3.3 La CE 17 a en outre approuvé les rapports techniques suivants: "Cadre de sécurité pour la distribution de clés quantiques dans les réseaux de télécommunication", "Problèmes, exigences et solutions possibles en matière de résolution des identificateurs d'objet", "Sécurité dans les télécommunications et les technologies de l'information (7ème édition)", "Utilisation efficace des normes de sécurité (2ème édition)", "Description du mécanisme d'incubation et moyens d'amélioration de ce mécanisme", "Approches stratégiques de la transformation des études relatives à la sécurité" et "Modèle de sécurité harmonisé (USM) – approche systémique, neutre et coordonnée de la cybersécurité".

3.4 En vue de l'AMNT-20, la CE 17 a décidé de ramener à 12 le nombre des Questions qui lui ont été confiées, soit jusque-là 14. Compte tenu du report de l'AMNT-20, ce nouvel ensemble de 12 Questions a été approuvé par le Groupe consultatif de la normalisation des télécommunications (GCNT), à sa réunion de janvier 2021, et cette nouvelle structure est entrée en vigueur le 18 janvier 2021 et le restera jusqu'à la fin de la période d'études.

3.5 La CE 3 de l'UIT-T continue d'étudier les aspects économiques et politiques des mégadonnées et des identités numériques en lien avec les services internationaux de télécommunication dans le cadre de sa Question 11/3. Elle a récemment approuvé la [Recommandation UIT-T D.267/X.1261](https://www.itu.int/rec/T-REC-D.1140-202008-I).

3.6 La CE 11 de l'UIT-T continue d'améliorer les protocoles de signalisation afin de les rendre plus sûrs, y compris en définissant des exigences additionnelles concernant les échanges de messages de signalisation et les protocoles particuliers. Elle a approuvé le rapport [technique QSTR-SS7-DFS](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-TUT-PROTO-2019), révisé l'ensemble des protocoles SS7 (Q.731.3-Q.731.6) et approuvé la Recommandation UIT-T [Q.3057](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.3057). De plus, elle continue d'élaborer les normes UIT-T [Q.5050](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5050), [Q.5051](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5051), [Q.5052](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5052) et [Q.5053](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5053) portant sur la lutte contre la contrefaçon et le vol de dispositifs de télécommunication/TIC.

3.7 La CE 9 de l'UIT-T a approuvé les Recommandations relatives à la sécurité suivantes: UIT‑T [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13573), [J.1013](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13574), [J.1014](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13575), [J.1015](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13576) et [J.1015.1](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13837); UIT-T [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357); et UIT-T [J.1031](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14280), [J.1032](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14355) et [J.1033](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14356). Elle a en outre approuvé trois Suppléments à des Recommandations de la série J (UIT‑T J.1012‑J.1015.1), à savoir [J.Sup7](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14286), [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287) et [J.Sup9](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14288).

3.8 La CE 13 de l'UIT-T a approuvé les Recommandations suivantes: UIT-T [Y.3055](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14393) sur la gestion des données personnelles basée sur la confiance et UIT-T [Y.3801](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14258), [Y.3802](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3802), [Y.3803](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3803) et [Y.3804](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14409) sur les réseaux de distribution de clés quantiques.

3.9 La CE 20 de l'UIT-T a élaboré les Recommandations relatives à la sécurité suivantes: UIT‑T [Y.4560](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14379), [Y.4561](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14380), [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381) et [Y.4907](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14382).

3.10 Dans le cadre de leurs travaux, plusieurs groupes spécialisés de l'UIT-T étudient actuellement les aspects liés à la confiance pour diverses technologies émergentes. C'est le cas notamment des groupes suivants: 1) [*Groupe spécialisé de l'UIT-T sur l'intelligence artificielle au service de la santé (FG-AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h); 2) [*Groupe spécialisé de l'UIT-T sur le multimédia dans les véhicules (FG-VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx#/fr);3) [*Groupe spécialisé de l'UIT-T sur l'intelligence artificielle au service de la conduite autonome et de la conduite assistée (FG-AI4AD)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx#/fr); 4) [*Groupe spécialisé de l'UIT-T sur l'informatique quantique pour les réseaux (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx#/fr); 5) [*Groupe spécialisé de l'UIT-T sur l'intelligence artificielle au service de la gestion des catastrophes naturelles (FG-AI4NDM)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx);et6)[*Groupe spécialisé de l'UIT-T sur les réseaux autonomes (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx).

3.11 L'UIT-R poursuit ses travaux dans le domaine de la normalisation des radiocommunications, de façon à répondre à l'évolution constante des réseaux modernes de télécommunication. Ce Secteur a défini des principes de sécurité précis concernant les réseaux IMT (3G, 4G et 5G) (Recommandations UIT-R M.1078, M.1223, M.1457, M.1645, M.2012 et M.2083). 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 (Recommandation UIT-R S.1250) et sur l'amélioration de la qualité de fonctionnement du protocole de commande de transmission sur les réseaux à satellite (Recommandation UIT-R S.1711). On trouvera sur le [site web des informations relatives aux technologies mobiles futuristes prévues pour les IMT à l'horizon 2020 et au-delà](https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx).

# 4 Structures organisationnelles

4.1 L'UIT a procédé à des évaluations techniques pour faire le point sur l'état de préparation à la création d'équipes d'intervention en cas d'incident informatique (CIRT) dans plus de 80 pays, et prend actuellement les mesures de suivi nécessaires pour aider les États Membres à mettre sur pied ces équipes. En 2020, elle a mené des évaluations en vue de la mise en place d'équipes CIRT au Guyana et dans les Bermudes, et a achevé le rapport d'évaluation pour le Libéria. Elle a directement participé à la création et/ou au renforcement des capacités de 14 équipes CIRT de pays, et sur les 7 projets actuellement en cours, 3 devraient arriver à terme dans le courant du premier trimestre de 2021. L'UIT et le Gouvernement des Bahamas ont en outre signé un accord de coopération prévoyant notamment la mise en place d'une équipe CIRT nationale.

4.2 À ce jour, l'UIT a organisé 29 [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), auxquels plus de 100 pays ont participé. De septembre à décembre 2020, elle a organisé et exécuté son [cyberexercice mondial](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx) de 2020 sous la forme de manifestations en ligne (dialogues régionaux, webinaires techniques et de politique générale et séances de formation à des outils et de perfectionnement) ainsi qu'un [cyberexercice régional à l'intention des îles du Pacifique](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2020/Pacific%20Cyberdrill/Pacific-Cyberdrill21.aspx).

# 5 Renforcement des capacités

5.1 Au cours du cyberexercice mondial de l'UIT, le BDT a organisé des [forums régionaux sur la cybersécurité](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) à l'intention de toutes les régions de l'Union, afin d'en renforcer les capacités humaines et organisationnelles.

5.2 À la suite de la CMDT-17, les responsables de 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)) ont poursuivi leurs travaux pendant la période d'études 2018-2021.

5.3 Le processus de mise à jour du [Guide d'élaboration d'une stratégie nationale en matière de cybersécurité](https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018/fr) est en cours et devrait s'achever en octobre 2021. Plus de 20 organisations contribuent actuellement à cette mise à jour. L'UIT a en outre organisé un webinaire intitulé "[Stratégies nationales de cybersécurité – mise en œuvre et suivi](https://www.itu.int/fr/ITU-D/Cybersecurity/Pages/2020-NCS-IM-webinar.aspx)", le 19 octobre 2020, afin d'examiner le cycle d'élaboration et de mise en œuvre de telles stratégies. Des activités consistant à fournir une assistance technique sur ces stratégies ont été lancées aux Fiji, au Libéria et au Tchad, et des discussions sont en cours avec d'autres États Membres qui ont besoin d'une assistance en la matière. Un atelier régional intitulé "[Cycle et élaboration des stratégies nationales de cybersécurité](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/ITU-regional-workshop-national-cybersecurity-strategies.aspx)" a été organisé à Melbourne, en Australie, le 20 février 2020, à l'intention de la région Asie-Pacifique. L'UIT s'emploie en outre à terminer de mettre au point les supports de formation en ligne sur l'élaboration de telles stratégies, qui seront utilisés dans le cadre d'un cours de l'Académie de l'UIT au deuxième trimestre de 2021.

5.4 Grâce à 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), l'Union et les centres d'excellence continuent de proposer des activités de formation et des ateliers dans divers domaines liés à la cybersécurité.

5.5 Pour faire face aux problèmes de cybersécurité pendant la pandémie de COVID-19 et [renforcer l'infrastructure de santé des États Membres grâce à des informations actualisées sur les cybermenaces](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Covid-19-CNI-Solution.aspx), le Membre de Secteur de l'UIT BitSight a permis aux États Membres de l'UIT d'accéder à sa plate-forme d'évaluation de la cybersécurité.

5.6 La quatrième version de l'enquête sur l'[Indice mondial de cybersécurité](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) de l'UIT, dont le questionnaire et la méthodologie ont été perfectionnés, a été présentée et déployée. L'enquête a pris fin le 30 septembre 2020. Tous les États Membres ont été invités à nommer des experts chargés de participer et de contribuer à la réunion du [Groupe d'experts sur la pondération de l'Indice GCI](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (composé en outre d'experts issus des milieux universitaires et du secteur privé), qui s'est tenue le 15 octobre 2020.

5.7 Afin d'encourager les jeunes à prendre part aux activités sur la cybersécurité et de remédier à la pénurie de main d'œuvre dans ce domaine à l'échelle mondiale, l'UIT va lancer l'initiative Youth4Cyber.

5.8 L'UIT tâche en outre de mettre la dernière main au plan de lancement du programme de mentorat intitulé "Les femmes dans le secteur de la cybersécurité", qui vise à renforcer les capacités des jeunes professionnelles désireuses d'obtenir un poste ou de poursuivre leur carrière dans le secteur de la cybersécurité.

# 6 Coopération internationale

6.1 L'UIT noue des relations et des [partenariats](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) avec diverses organisations et initiatives régionales ou internationales, notamment la Commonwealth Cybercrime Initiative, 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 et les associations régionales d'équipes CSIRT/CERT, comme AP CERT, AFRICA CERT et OIC CERT.

6.2 Conformément aux instructions données par le Conseil à sa session de 2019, le Secrétaire général soumettra à la prochaine session du Conseil (1) un rapport décrivant la façon dont le cadre offert par le Programme mondial cybersécurité (GCA) est actuellement utilisé par l'UIT et (2) des lignes directrices appropriées relatives à l'utilisation du Programme GCA par l'UIT, élaborées avec la participation des États Membres, pour examen et approbation par le Conseil. Conformément au processus d'élaboration du projet de lignes directrices défini par le Conseil à sa session de 2019, et comme suite à la première consultation ouverte en ligne de toutes les parties prenantes du SMSI organisée le 23 avril 2020 afin de recueillir des observations sur le projet de lignes directrices, une seconde consultation ouverte en ligne de toutes les parties prenantes du SMSI aura lieu le 1er mars 2021.

6.3 En tant que coordonnateur principal pour la grande orientation C5 du SMSI, l'UIT a organisé plusieurs séances au cours de l'[édition de 2020 du Forum du SMSI](https://www.itu.int/net4/wsis/forum/2020/fr)[,](https://www.itu.int/net4/wsis/forum/2020/en) notamment une séance de coordination pour cette grande orientation sur le thème "La cybersécurité à l'ère de l'informatique quantique: enjeux et considérations pour les réseaux TIC" ainsi qu'un dialogue de haut niveau sur les mesures propres à garantir des soins de santé fiables à l'ère de l'intelligence artificielle.

# 7 Protection en ligne des enfants (COP)

7.1 Un groupe de travail multi-parties prenantes composé de plus de 50 organisations et experts issus de différents secteurs a révisé les quatre volumes de [Lignes directrices sur la protection en ligne des enfants](https://www.itu.int/en/cop/Pages/guidelines.aspx) destinées aux décideurs, au secteur privé, aux parents et aux éducateurs ainsi qu'aux enfants. La manifestation d'envergure mondiale organisée à l'occasion de la [publication des nouvelles Lignes directrices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-COP-Guidelines-launch-webinar.aspx) a été suivie de [manifestations régionales](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/2020/Regional-Launches-COP-2020-Guidelines.aspx), qui ont permis de discuter de leur mise en application aux niveaux régional et national.

7.2 En Afrique, la première formation à la protection en ligne des enfants destinée aux décideurs a eu lieu en anglais et en français en amont de la manifestation organisée dans la région pour la publication des Lignes directrices. Dans la région de la CEI, le Bureau régional de l'UIT pour la CEI et l'Académie nationale des télécommunications A.S. Popov Odessa ont conjointement élaboré un [cours sur la sécurité en ligne](https://onlinesafety.info/#/home). Dans la région Asie-Pacifique, six petits États insulaires et pays en développement ont reçu une assistance pour l'élaboration de stratégies nationales de protection en ligne des enfants et de cadres connexes, conformément aux Lignes directrices sur la protection en ligne des enfants et en coordination avec d'autres partenaires. Ces services d'appui ont été fournis dans le cadre d'un projet mené conjointement avec le Département des communications et des arts de l'Australie. Dans la région Amériques, des discussions sur l'élaboration et la mise en œuvre de cadre stratégiques nationaux ont été entamées avec la Colombie, le Costa Rica, le Brésil et le Paraguay. En Europe, l'application des Lignes directrices sur la protection en ligne des enfants a beaucoup avancé, et de nombreuses activités ont été organisées dans le cadre de l'initiative régionale visant à renforcer la confiance dans l'utilisation des TIC.

7.3 Le Royaume d'Arabie saoudite et l'UIT ont signé un accord de mise en œuvre d'un programme triennal mondial visant à créer un cyberenvironnement sûr et de nature à autonomiser les enfants. Ce programme consiste à fournir une assistance aux pouvoirs publics en matière de politiques générales et à renforcer les compétences numériques et la maîtrise des outils numériques des utilisateurs finals. Sa mise en œuvre débutera au premier trimestre 2021.

7.4 Un rapport d'étape sur [les écosystèmes nationaux de protection en ligne des enfants en Europe du Sud-Est](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/FINAL%20REPORT.pdf) a été publié, à la suite de quoi de nombreux forums et manifestations sur la protection en ligne des enfants ont été coorganisés en Europe.

7.5 L'UIT a célébré l'édition de 2021 de la Journée pour un Internet plus sûr en publiant diverses communications, notamment un article de [blog](https://www.itu.int/en/myitu/News/2021/02/08/18/38/Sango-Internet-safety-drawing-child-online-protection-COP) sur le concours national de dessin organisé en Hongrie, qui mettait en scène la mascotte de l'Union pour la protection en ligne des enfants. Cette occasion a en outre permis d'annoncer le lancement d'une [collaboration avec Eni et Deloitte Italia](https://www.bing.com/videos/search?q=sango+announcing+eni+youtube&docid=13903411089711&mid=271E2ABE304F85C97D50271E2ABE304F85C97D50&view=detail&FORM=VIRE), afin de sensibiliser les enfants et les éducateurs à la sécurité en ligne et de renforcer leurs capacités en la matière.

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