|  |  |
| --- | --- |
| **Conseil 2022Genève, 21-31 mars 2022** |  |
|  |  |
|  |  |
|  | **Document C22/18-F** |
| **18 février 2022** |
| **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 2021 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).Suite à donnerLe Conseil est invité à **prendre note** du présent rapport.\_\_\_\_\_\_\_\_\_\_\_\_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/fr) *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/fr) *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*](https://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/en)*,* [*C18/18*](https://www.itu.int/md/S17-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) *et* [*C21/18*](https://www.itu.int/md/S21-CL-C-0018/fr) |

# 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 deux réunions en avril et août/septembre 2021, lors desquelles elle a défini [22 nouveaux sujets d'étude en matière de normalisation](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17), et deux séances plénières électroniques en janvier 2021 et 2022. La CE 17 a approuvé plus de 30 Recommandations nouvelles ou révisées sur la sécurité des TIC, notamment: X.1011, X.1046, X. 1047, X.1054 (révisée), X.1060, X.1061, X.1080.2, X.1217, X.1233, X.1234, X.1235, X.1252, X.1333, X.1369, X.1376, X.1405, X.1406, X.1407, X.1408, X.1453, X.1470, X.1643, X.1712, X.1752, X.1770, X.1811 et Supplément 36 aux Recommandations de la série X.

3.3 En outre, la CE 17 a approuvé le rapport technique "Cadre pour la normalisation de la sécurité des services virtualisés".

3.4 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.1102 sur les [mécanismes de recours et de protection pour les consommateurs OTT](https://www.itu.int/rec/T-REC-D.1102).

3.5 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. La CE 11 de l'UIT-T a approuvé le rapport technique QSTR-USSD "Cryptage des messages USSD nécessitant peu de ressources et résistant aux attaques quantiques à utiliser dans les services financiers" et le Supplément 75 aux Recommandations de la série Q portant sur la lutte contre la contrefaçon et le vol de dispositifs de télécommunication/TIC.

3.6 La CE 9 de l'UIT-T a approuvé les Recommandations UIT-T [J.1026](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14868), [J.1027](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14869), [J.1028](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14870) et [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357) révisées. Elle a également approuvé la Recommandation J.1205 et a poursuivi la mise à jour du Guide de mise en œuvre de la Recommandation UIT-T [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13573&lang=fr) et de deux Suppléments aux Recommandations de la série J (Recommandations UIT-T J.1012 à J.1015.1), à savoir [J.Sup7](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14286) et [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287).

3.7 La CE 13 de l'UIT-T a approuvé les Recommandations suivantes: UIT-T Y.3056 et Y.3057 sur la gestion des données personnelles basée sur la confiance et UIT-T Y.3805 et Y.3806 sur les réseaux de distribution de clés quantiques.

3.8 La CE 15 de l'UIT-T a approuvé le Supplément UIT-T G.Suppl.OTNSec "Sécurité du réseau de transport optique".

3.9 La CE 16 de l'UIT-T a approuvé la Recommandation UIT-T F.747.10 "Exigences des systèmes de registres distribués (DLS) pour les services intégrant un facteur humain sécurisé" (en cours de publication), qui définit les exigences générales et les capacités fonctionnelles des systèmes de registres distribués (DLS) pour les services intégrant un facteur humain sécurisé.

3.10 La CE 20 de l'UIT-T a élaboré les Recommandations relatives à la sécurité suivantes: UIT‑T [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381), Y.4810 et Y.4811.

3.11 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 les fédérations de bancs d'essai pour les IMT‑2020 et les systèmes ultérieurs (FG-TBFxG)*](https://www.itu.int/en/ITU-T/focusgroups/tbfxg/Pages/default.aspx); 2) [*Groupe spécialisé de l'UIT-T sur l'intelligence artificielle (IA) et l'Internet des objets (IoT) au service de l'agriculture numérique (FG-AI4A)*](https://www.itu.int/en/ITU-T/focusgroups/ai4a/Pages/default.aspx); 3) [*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); 4) [*Groupe spécialisé de l'UIT-T sur les réseaux autonomes (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx); 5) [*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); 6) [*Groupe spécialisé de l'UIT-T sur l'efficacité environnementale de l'intelligence artificielle et d'autres technologies émergentes (FG-AI4EE)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ee/Pages/default.aspx); 7) [*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/Pages/default.aspx) et 8) [*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).

3.12 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 En 2021, 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. Elle a directement participé à la création et/ou au renforcement des capacités de 17 équipes CIRT de pays avant 2021, trois (3) projets sont arrivés à terme en 2021, des évaluations ont été menées en vue de la mise en place d'une équipe CIRT en Guinée-Bissau, aux Bahamas, en Mongolie et en Guyane, les modalités de conception de l'équipe CIRT de l'Eswatini ont été examinées et quatre projets relatifs à la mise en œuvre d'équipes CIRT sont en cours. En outre, l'UIT a aidé le Mali et le Malawi à concevoir un cadre relatif à l'infrastructure de clé publique (PKI) dans chacun de ces pays.

4.2 À ce jour, l'UIT a organisé 34 [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), auxquels plus de 120 pays ont participé. Entre septembre et décembre 2021, elle a organisé et exécuté son [cyberexercice mondial](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberdrills-2021.aspx) de 2021 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 que deux cyberexercices sous-régionaux à l'intention des pays de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) et de la Communauté de développement de l'Afrique australe (SADC) ainsi qu'un cyberexercice national à l'intention de l'Inde. En outre, deux publications ont été élaborées en 2021, à savoir: "Cadre et lignes directrices opérationnels pour la planification et l'exécution des cyberexercices régionaux de l'UIT" et "Programme de travail de l'UIT sur la cybersécurité: cadre relatif aux équipes CIRT".

# 5 Renforcement des capacités

5.1 Au cours du [cyberexercice mondial de l'UIT](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), le BDT a organisé des forums régionaux sur la cybersécurité 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 L'UIT a facilité 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). Plus de [20 organisations](https://ncsguide.org/partners/) ont contribué à l'élaboration de la deuxième [édition du guide](https://ncsguide.org/the-guide/), qui a été lancée en novembre 2021 dans le cadre d'un webinaire mondial, où les participants ont débattu du cycle d'élaboration et de mise en œuvre d'une stratégie nationale en matière de cybersécurité, souligné les enjeux et les perspectives, et invité à davantage de coopération. Des activités consistant à fournir une assistance technique sur ces stratégies ont été lancées aux Bahamas, au Rwanda, au Maroc et dans les pays de la Communauté des États de l'Afrique australe (SADEC), et des discussions sont en cours avec d'autres États Membres qui ont besoin d'une assistance. En outre, l'UIT a achevé et mis à disposition la formation en ligne "[Cycle de vie, principes et bonnes pratiques pour l'élaboration et la mise en œuvre d'une stratégie nationale de cybersécurité](https://academy.itu.int/training-courses/full-catalogue/lifecycle-principles-and-good-practices-national-cybersecurity-strategy-development-and)" en trois langues (anglais, français et espagnol) sur la plate-forme de l'Académie de l'UIT. La formation sera disponible en russe en mars 2021. L'UIT travaille en partenariat avec le Groupe de la Banque mondiale pour organiser des webinaires régionaux visant à fournir des renseignements opérationnels sur les modalités d'élaboration d'un plan d'action relatif à une stratégie nationale de cybersécurité. L'UIT élabore actuellement un outil de référence sur les stratégies nationales de cybersécurité pour appuyer les efforts que les États Membres et les spécialistes de la cybersécurité déploient dans le cadre des stratégies nationales de cybersécurité. La version pilote de l'outil a été achevée en janvier et les travaux de mise au point se poursuivront en 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 La quatrième édition du rapport 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 [publiée le 29 juin 2021](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI/GCIv4-Report-Launch.aspx). Cette édition de l'indice couvre 193 États Membres ainsi que l'État de Palestine et 169 pays ont contribué à la collecte de données. Les travaux relatifs à un questionnaire actualisé pour l'Indice GCI ont déjà commencé. La nouvelle série de documents a été présentée virtuellement au Groupe du Rapporteur pour la Question 3 de la Commission d'études 2 de l'UIT-T en octobre 2021, et la commission d'études a établi un groupe de travail virtuel par correspondance pour contribuer à la révision du questionnaire. Une nouvelle édition du questionnaire sur l'Indice GCI devrait être publiée au début de 2022.

5.6 Afin d'encourager les jeunes à prendre part aux activités sur la cybersécurité et de sensibiliser l'opinion à la pénurie de main-d'œuvre dans ce domaine à l'échelle mondiale, l'UIT planifie des activités et des efforts de collaboration pour les jeunes et par les jeunes, dans le cadre de l'Initiative Generation Connect.

5.7 L'UIT a mené à bien la première édition 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. Une nouvelle cohorte destinée à certains groupes cibles des régions Afrique, États arabes et Asie‑Pacifique devrait être lancée en avril 2022.

# 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 À sa session de 2019, le Conseil a chargé le Secrétaire général de lui soumettre des lignes directrices appropriées relatives à l'utilisation du Programme mondial cybersécurité (GCA), pour examen et approbation. Le [Document C21/71](https://www.itu.int/md/S21-CL-C-0071/en) a été élaboré en conséquence et soumis par le Secrétaire général à la consultation virtuelle des Conseillers de 2021 (C21/VCC1). à la suite des débats de la C21/VCC1, les États Membres du Conseil ont chargé le secrétariat "*de mener de nouvelles consultations avec les États Membres du Conseil, compte tenu des contributions reçues et des commentaires formulés à la séance. Le secrétariat devra présenter une version révisée du Document 71 pour examen et approbation à la prochaine session du Conseil*". Des consultations sont menées actuellement avec les États Membres du Conseil et un document révisé sera soumis à la session de 2022 du Conseil pour examen et approbation.

6.3 En tant que coordonnateur principal pour la grande orientation C5 du SMSI, l'UIT a organisé un volet consacré à la cybersécurité comprenant plusieurs séances au cours de l'[édition de 2021 du Forum du SMSI](https://www.itu.int/net4/wsis/forum/2021/fr)[,](https://www.itu.int/net4/wsis/forum/2020/en) notamment une séance de coordination pour cette grande orientation sur le thème "Cybersécurité: Mesures de cybersécurité multidimensionnelles – perspectives et enjeux actuels de l'utilisation des indices pour comprendre la cybersécurité" ainsi qu'une deuxième consultation ouverte sur le projet de lignes directrices relatives à l'utilisation du Programme GCA et un dialogue de haut niveau sur le thème "Évaluation de la préparation à l'intelligence artificielle: conséquences pour les politiques, perspectives et enjeux".

# 7 Protection en ligne des enfants (COP)

7.1 La protection en ligne des enfants a été intégrée parmi les principaux éléments du quatrième pilier du projet Giga, lancé conjointement par l'UIT et l'UNICEF.

7.2 En outre, l'UIT a signé un accord de collaboration avec la Fondation SCORT dans le domaine de la protection en ligne des enfants. L'UIT a contribué à de nombreuses discussions, notamment dans le cadre de l'édition de 2021 de la journée pour un Internet plus sûr, de la quinzième Conférence européenne du football au service du développement et d'une table ronde avec les clubs de football européens.

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 a été lancée en 2021 par la signature d'un document de projet interne de l'UIT. Dans le cadre du projet, l'UIT a d'abord mis l'accent sur le renforcement des capacités, en concevant des formations à son propre rythme pour tous les publics et d'autres solutions interactives visant à permettre aux enfants et aux jeunes de devenir des citoyens numériques responsables.

7.4 Toutes les régions de l'UIT ont commencé à mener des activités relevant du projet mondial visant à créer un cyberenvironnement sûr et de nature à autonomiser les enfants. L'exécution du projet a débuté par l'Albanie, suivie du Malawi et du Maroc.

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. En outre, la mascotte de la protection en ligne des enfants a animé plusieurs manifestations virtuelles, notamment le volet sur la sécurité en ligne organisé dans le cadre des [célébrations de la Journée internationale des jeunes filles dans le secteur des TIC](https://www.itu.int/women-and-girls/girls-in-ict/girlsinict-online-safety-moment/) et la session 4 du Colloque mondial des régulateurs (GSR-21) de 2021 sur le thème "[Inclusion numérique sûre: protection en ligne des enfants](https://www.itu.int/fr/ITU-D/Conferences/GSR/2021/Pages/global.aspx)".

7.6 En outre, la mascotte de la protection en ligne des enfants a [annoncé le lancement d'un projet de 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. Le cours "[En ligne en sécurité avec Sango](https://www.itu-cop-guidelines.com/children)", divisé en cinq épisodes, offre des conseils pratiques aux enfants jusqu'à neuf ans pour les sensibiliser aux risques auxquels ils peuvent être exposés en ligne.

7.7 Dans le cadre de l'Académie de l'UIT, l'Union a assuré une séance de formation sur la protection en ligne des enfants à l'intention des régulateurs de la région des États arabes.

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