|  |  |
| --- | --- |
| **Conseil 2019Genève, 10-20 juin 2019** | **logo_F_** |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.5** | **Document C19/18-F** |
| **1er avril 2019** |
| **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 depuis la session de 2018 du Conseil 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/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 CMDT, 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'AMNT, Documents*[*C05/32*](http://www.itu.int/md/S05-CL-C-0032/en)*,* [*C05/INF/10*](https://www.itu.int/md/S05-CL-INF-0010/en)*,* [*C06/4*](http://www.itu.int/md/S06-CL-C-0004/en)*,* [*C07/21*](http://www.itu.int/md/S07-CL-C-0021/en)*,* [*C08/33*](http://www.itu.int/md/S08-CL-C-0033/en)*,* [*C09/50*](http://www.itu.int/md/S09-CL-C-0050/en)*,* [*C10/12*](http://www.itu.int/md/S10-CL-C-0012/en)*,* [*C11/54*](http://www.itu.int/md/S11-CL-C-0054/en)*,* [*C12/29*](http://www.itu.int/md/S12-CL-C-0029/en)*,* [*C13/23*](http://www.itu.int/md/S13-CL-C-0023/en)*,* [*C14/23*](http://www.itu.int/md/S14-CL-C-0023/en)*,* [*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) *et* [*C18/18*](https://www.itu.int/md/S18-CL-C-0018/en) *du Conseil* |

# 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 oeuvre des activités menées par le BDT, le TSB et le BR dans ce domaine.

1.2 La Conférence de plénipotentiaires de l'UIT, tenue du 29 octobre au 16 novembre 2018 à Dubaï (UAE), a modifié ses Résolutions 130 et 179.

# 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) de l'UIT-D, l'UIT aide les Etats 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 experts.

# 3 Mesures techniques et procédures

3.1 La [Commission d'études 17 (CE 17)](http://www.itu.int/ITU-T/studygroups/com17/) 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 s'est réunie à trois reprises en mars 2018, en août-septembre 2018 et en janvier 2019. La CE 17 a défini [55 nouveaux sujets d'étude en matière de normalisation](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). Elle a approuvé 17 Recommandations UIT-T, nouvelles ou révisées, sur la sécurité des TIC, intitulées: [Applications génériques de l'ASN.1 – Syntaxe de message cryptographique](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12848&lang=fr), [Cadre de sécurité pour l'exploitation des réseaux vocaux VoLTE](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13603&lang=fr)), [Services de sécurité utilisant les réseaux pilotés par logiciel](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13803&lang=fr), [Cadre et exigences de sécurité pour le chaînage de fonctions de service fondé sur les réseaux pilotés par logiciel](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13872&lang=fr), [Contrôle d'accès télébiométrique au moyen de cartes d'identification intelligentes](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13725), [Authentification télébiométrique utilisant des biosignaux](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13873&lang=fr), [Exigences de sécurité et cadre pour l'analyse des mégadonnées dans les services Internet sur mobile](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13726&lang=fr), [Techniques d'évaluation de la sécurité dans les réseaux de télécommunication/TIC](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13404&lang=fr), [Cas d'utilisation pour l'expression structurée d'informations sur les menaces (STIX)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13849&lang=fr), [Cadre technique de lutte contre le spam publicitaire sur les applications mobiles](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13605&lang=fr), [Protocole d'amélioration de l'authentification et métadonnées – Version 1.0](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13606&lang=fr),

[Cadre d'authentification universelle (UAF)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13727&lang=fr), [Protocole client-authentificateur/Cadre applicable au double facteur universel](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13728&lang=fr), [Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13405&lang=fr), [Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13607&lang=fr), [Lignes directrices sur les mécanismes d'authenfication hybride et de gestion de clés dans le modèle client-serveur](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13729&lang=fr) et [Exigences de sécurité des données approuvées pour le service de surveillance de l'informatique en nuage](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13406&lang=fr).

3.3 La CE 17 a approuvé la version révisée du [Supplément à la Recommandation UIT-T X.1051, intitulé "Manuel d'utilisation pour les contrôles de sécurité de l'information au sein des organisations de télécommunication"](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13730&lang=fr) ainsi que cinq nouveaux Suppléments aux Recommandations UIT-T de la série X, à savoir: [Supplément à la Recommandation UIT-T X.805: Lignes directrices sur la sécurité pour les opérateurs de réseaux virtuels mobiles (MVNO)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13410&lang=fr), [Supplément à la Recommandation UIT-T X.660 – Lignes directrices relatives à l'utilisation des identificateurs d'objet pour l'Internet des objets](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13411&lang=fr), [Supplément à la Recommandation UIT-T X.1058: Code de bonne pratique pour la protection des informations d'identification personnelle sur la base de la Recommandation UIT-T X.1058 pour les organisations de télécommunication](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13593&lang=fr), [Supplément à la Recommandation UIT-T X.1231: Cadre technique de lutte contre les escroqueries par service téléphonique](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13731&lang=fr) et [Supplément à la Recommandation UIT-T X.1051 | Norme ISO/CEI 27011 (2016): Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information sur la base de la Norme ISO/CEI 27002 pour les organisations de télécommunication](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13869&lang=fr).

3.4 Le [Groupe régional de la CE 17 pour la région des Etats arabes](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/sg17rgarb/Pages/default.aspx) a tenu sa deuxième réunion au Koweït (octobre 2018). Le Groupe régional pour l'Afrique et le Groupe régional pour la région des Etats arabes de la CE 17 se réuniront à Tunis (Tunisie) en avril 2019.

3.5 La CE 17 a organisé un [atelier de l'UIT sur la sécurité de la 5G (mars 2018)](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx), un [atelier de l'UIT sur les attaques de cybersécurité avancées et les rançongiciels (août 2018)](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx), un [atelier de l'UIT sur l'intelligence artificielle/l'apprentissage automatique et la sécurité (janvier 2019)](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190121/Pages/committee.aspx) et un [atelier sur les communications quantiques sécurisés (janvier 2019)](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Secure%20quantum%20communication.aspx), en vue de déterminer les moyens permettant à la CE 17 d'entreprendre l'étude, à terme, des questions de normalisation se rapportant à ces thèmes, notamment en définissant de nouveaux sujets d'étude possibles.

3.6 La CE 17 a poursuivi ses travaux sur la sécurité de l'IoT et a continué d'assurer une coordination avec la CE 20 de l'UIT-T, chargée de l'étude de: "L'Internet des objets et ses applications, y compris les villes et les communautés intelligentes (SC&C)".

3.7 La CE 9 de l'UIT-T a déterminé cinq projets de Recommandation (UIT-T J.1012 J.1013, J.1014, J.1015 et J.1015.1) sur l'interface commune intégrée pour les solutions CA/DRM interchangeables.

3.8 La CE 13 de l'UIT-T a approuvé la Recommandation UIT-T Y.3053 (2018) Amd.1 "Cadre applicable aux réseaux de confiance ayant des domaines de réseau centrés sur la confiance: Amendement 1 – Architecture et procédures de déploiement des réseaux de confiance".

3.9 La CE 15 de l'UIT-T a approuvé la Recommandation révisée UIT-T G.9978 "Admission sécurisée dans un réseau G.hn".

3.10 La CE 20 de l'UIT-T a approuvé la Recommandation UIT-T Y.4205 "Exigences et modèle de référence des systèmes externalisés liés à l'Internet des objets".

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).

# 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)](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx) dans 75 pays, et prend actuellement les mesures de suivi nécessaires. La participation directe à 14 de ces activités a pris fin et d'autres activités sont en cours ou en projet pour 2019.

4.2 L'UIT a travaillé en partenariat avec le Centre mondial des capacités de cybersécurité (Oxford Martin School), afin de mener à bien des évaluations communes des capacités de cybersécurité en Thaïlande, en Sierra Leone et à Madagascar. Grâce au financement apporté par le Gouvernement australien (DOCA), l'UIT procédera à des évaluations CIRT aux Samoa, au Tonga, à Vanuatu, et en Papouasie-Nouvelle-Guinée, après quoi elle mènera une évaluation des capacités de cybersécurité. En outre, l'UIT a procédé à des évaluations CIRT pour l'Albanie, la Bosnie‑Herzégovine, le Malawi, la Mauritanie et la République démocratique du Congo.

4.3 L'UIT a organisé 24 [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), auxquels plus de 100 pays ont participé. Ces cyberexercices ont eu lieu à [Grand Bassam, Côte d'Ivoire](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/IvoryCoastcyberdrill2018.aspx) (région Afrique, octobre 2018); à [La Plata City, Argentine](https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2018/20577.aspx) (région Amériques, juin 2018); à [Koweït City (Koweït)](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx) (région des États arabes, octobre 2018); à [Limassol, Chypre](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBDRILL/ITU-ALERT-Cyber-drill.aspx) (région Europe, novembre 2018) et à [Bakou (Azerbaïdjan)](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/EVENTS/2018/09_Baku/09_Baku.aspx) (région de la CEI, septembre 2018). Un cyberexercice pour l'Europe est en cours d'organisation en [Roumanie (mai 2019)](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberDrill/ITU-Cyber-Drill-for-Europe-Region-.aspx).

4.4 Un [Guide d'élaboration d'une stratégie nationale en matière de cybersécurité (NCS)](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf), élaboré avec le concours de l'UIT dans le cadre d'un processus de collaboration multi-parties prenantes, et réunissant 15 organisations intergouvernementales et représentants du secteur privé, d'établissements universitaires et de la société civile, a été publié en septembre 2018. L'initiative NCS est un outil fonctionnel destiné à aider les gouvernements à concevoir et améliorer leurs stratégies en matière de cybersécurité. L'UIT organise des ateliers régionaux et nationaux sur la stratégie relative à la cybersécurité pour aider les États Membres à concevoir leur stratégie nationale en matière de cybersécurité. Un atelier national a eu lieu en Pologne en 2018 et un atelier régional pour la région Europe sera organisé en juin 2019. Des discussions sont également en cours afin d'organiser des ateliers analogues pour les pays membres de la SADC, Malte, le Bénin et la Guinée. L'UIT a apporté une assistance à la Mauritanie pour l'élaboration de sa stratégie en matière de cybersécurité et a organisé un atelier de validation (Nouakchott –décembre 2018), en vue de présenter le rapport intérimaire sur la stratégie en matière de cybersécurité pour la période 2019-2022 en Mauritanie. L'UIT a également aidé Kiribati et le Bhoutan à concevoir leur stratégie en matière de cybersécurité (novembre 2018).

# 5 Renforcement des capacités

5.1 L'UIT a organisé des [forums régionaux sur la cybersécurité](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) à l'intention de toutes ses régions, afin de renforcer les capacités pour différents programmes/ diverses activités du BDT et de fournir un cadre opérationnel pour la coopération régionale et internationale.

5.2Suite à la CMDT-17, les travaux au titre 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)) se poursuivront pendant la période d'études 2018-2021.

5.3 L'UIT, l'ICANN et l'ARTAO ont organisé un atelier de renforcement des capacités sur le thème "Cybersécurité, équipes CIRT et écosystème de l'ICANN" (Ouagadougou, Burkina Faso – octobre 2018), à l'invitation de Autorité de régulation des communications électroniques et des postes (ARCEP).

5.4 L'UIT et le Centre régional de cybersécurité pour la région des Etats arabes ont organisé la [Semaine régionale de la cybersécurité](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx) (Koweït, octobre 2018), qui a servi de cadre pour améliorer la coopération et la communication entre les équipes CIRT des États arabes.

5.5 L'UIT, le Centre supérieur de formation aux télécommunications et la Faculté des sciences appliquées des postes et télécommunications (Faculté des TIC, République islamique d'Iran) ont organisé [une formation sur la cybersécurité dispensée par le Centre d'excellence de l'UIT pour la région Asie-Pacifique (Téhéran, Iran – décembre 2018)](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2018/CybersecurityASPCOE/cybersecurity.aspx).

5.6 La troisième version de l'[Indice mondial de cybersécurité](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCIv3), à laquelle ont participé 155 Etats Membres, a été lancée en mars 2019, à l'occasion des réunions des Commissions d'études de l'UIT-D. Cette version fournit davantage de renseignements sur la cybersécurité, tout en élargissant les partenariats pour qu'ils servent de cadre de collaboration multi-parties prenantes. L'UIT a lancé la phase de préparation du processus GCIv4, qui débutera en avril 2019.

5.7 L'UIT a organisé l'[Atelier régional pour l'Europe et la CEI sur la cybersécurité et la protection en ligne des enfants](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/EVENTS/2018/04_Odessa/04_Odessa.aspx) (Odessa, Ukraine, avril 2018).

# 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'ENISA, INTERPOL, la CEDEAO, la Banque mondiale le Forum FIRST et les associations régionales d'équipes CSIRT/CERT, comme AP CERT, AFRICA CERT et OIC CERT.

Toutes les activités menées dans le cadre du partenariat entre l'UIT et IMPACT ont pris fin en 2016, une fois mis en oeuvre les projets qui demeuraient en suspens. IMPACT a annoncé la dissolution officielle de ce Partenariat au début de 2018. Cette dissolution signifie que le mémorandum d'accord et l'accord de coopération signés entre l'UIT et IMPACT ont été résiliés avec effet immédiat.

6.2 En tant que coordonnateur principal de la grande orientation C5 du SMSI, l'UIT a organisé plusieurs sessions à l'occasion du [Forum 2018 du SMSI](https://www.itu.int/net4/wsis/forum/2018/), en accordant une attention toute particulière au 10ème anniversaire du lancement du Programme mondial cybersécurité (GCA) et de l'initiative pour la protection en ligne des enfants. Des sessions de haut niveau, portant notamment sur l'intelligence artificielle et la sécurité, ont également été organisées à l'occasion du [Forum 2019 du SMSI](https://www.itu.int/net4/wsis/forum/2019/).

6.3 En juillet 2018, un "[Dialogue mondial sur l'intelligence artificielle, l'Internet des objets et la politique en matière de cybersécurité – Problèmes et perspectives sur le plan politique et réglementaire](https://www.itu.int/net4/ITU-D/CDS/GSR/2018/default.asp)", réunissant des régulateurs de différents États Membres et de différentes organisations, a été organisée à l'UIT.

6.4 L'UIT a conclu des partenariats avec des établissements universitaires de la région des États arabes (Réseau de recherche et d'enseignement des Etats arabes et Naïf Arab University for Security Sciences), afin de renforcer leur rôle dans la promotion d'une culture de la cybersécurité et d'encourager leur participation active aux travaux de l'UIT. Dans le cadre de ces partenariats, des activités ont été organisées dans la région des États arabes.

6.5 Dans le cadre de l'Initiative régionale de l'UIT pour l'Europe, l'UIT a coorganisé une série de réunions sur la cybersécurité, notamment la [6ème édition de la Plate-forme de dialogue entre secteur public et secteur privé sur la cybersécurité en Europe centrale](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBR/Cyber-Security-in-Romania.aspx) (Sibiu, Roumanie – septembre 2018), le Forum international sur "[Les nouveaux enjeux mondiaux de la cybersécurité](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CERT-ROForum/default.aspx)" (Bucarest, Roumanie – octobre 2018), la [Plate-forme de dialogue entre secteur public et secteur privé sur la cybersécurité en Europe occidentale](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBCONGR/Second-Western-European-Cybersecurity-Public-Private-Dialogue-Platform.aspx) (Porrentruy, Suisse – novembre 2010) et la [Semaine de la cybersécurité organisée à Vienne – Protection des infrastructures essentielles](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/cybervienna.aspx) (Vienne, Autriche (coorganisée par la CEI, avec le concours de l'OSCE) – mars 2019).

# 7 Protection en ligne des enfants (COP)

7.1 L'UIT a aidé le Soudan à élaborer sa stratégie nationale en matière de protection en ligne des enfants. En outre, des activités de sensibilisation et des concours ont été organisés dans plusieurs Etats arabes pour faire prendre davantage conscience les enfants, les éducateurs et les parents de la sécurité de l'Internet, en collaboration avec les parties prenantes concernées.

7.2 Dans le cadre de l'Initiative régionale de l'UIT pour l'Europe, l'UIT a aidé la Géorgie à élaborer sa stratégie nationale en matière de protection en ligne des enfants. Il est prévu d'organiser des activités analogues dans d'autres pays au cours de la période à venir. En outre, l'UIT a coorganisé une série de réunions destinées à renforcer les capacités humaines, notamment la [Manifestation nationale sur la protection en ligne des enfants, la Journée de sensibilisation à l'intention des enfants et des adolescents](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/NECOP/default.aspxhttps%3A/www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/NECOP/default.aspx) (Noto, Italie – mai 2019), le [Forum sur les jeunes et le numérique](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/DYF/default.aspx) (Varsovie, Pologne – mai 2018) , la Conférence internationale sur le thème "[Assurer la sécurité des enfants et des adolescents en ligne](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/COP/default.aspx) " (Varsovie, Pologne – septembre 2018) et la [Journée 2019 pour un Internet plus sûr](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/SID/Safer-Internet-Day-2019.aspx) (Tirana, Albanie – février 2019).

7.3 En novembre 2018, l'UIT a aidé Kiribati et le Bhoutan à procéder à des évaluations de la protection en ligne des enfants. L'UIT a également élaboré un document intitulé "Améliorer les mesures de protection en ligne des enfants dans les pays membres de l'ASEAN: Partenariats avec le secteur privé" et conçu [un environnement d'apprentissage virtuel 3D multi-utilisateurs](https://www.youtube.com/watch?v=SymYlZq5v1k&feature=youtu.be) pour sensibiliser davantage l'opinion aux risques auxquels les enfants sont exposés sur l'Internet.

7.4 L'UIT a organisé diverses activités dans le cadre de la Journée 2019 pour un Internet plus sûr et s'est notamment employée à promouvoir la protection en ligne des enfants.

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