|  |  |
| --- | --- |
| **Conseil 2020 Genève, 9-19 juin 2020** |  |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.4** | **Document C20/18-F** |
| **30 mars 2020** |
| **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 | |

|  |
| --- |
| Résumé  Le présent rapport résume les activités menées par l'UIT depuis la session de 2019 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 donner  Le 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 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) *et* [*C19/18*](https://www.itu.int/md/S19-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 oeuvre 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/Produit 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 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 [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 a tenu une réunion en septembre 2019, à laquelle elle a défini [25 nouveaux sujets d'étude en matière de normalisation](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). La CE 17 a approuvé plus de 30 Recommandations UIT-T nouvelles ou révisées sur la sécurité des TIC, notamment: 9ème édition des normes essentielles en matière de cybersécurité pour les Recommandations de la série X.500 sur l'infrastructure de clé publique; X.1044 "Exigences de sécurité de la virtualisation de réseau"; X.1045 "Architecture de la chaîne de services de sécurité pour les réseaux et les applications"; X.1059 "Guide de mise en œuvre à l'intention des organisations de télécommunication sur la gestion des risques liés à leurs actifs mondialement accessibles dans les réseaux IP"; X.1702 "Architecture d'un générateur de nombres aléatoires pour le bruit quantique"; X.1232 "Cadre technique de lutte contre le spam publicitaire dans les informations générées par les utilisateurs"; X.677 "Mécanisme d'identification pour les aéronefs sans pilote utilisant des identificateurs d'objet"; X.1402 "Menaces de sécurité pour la technologie des registres distribués"; Amendement 1 à la Recommandation UIT-T X.1197 "Lignes directrices révisées relatives aux critères de sélection d'algorithmes cryptographiques pour la protection de service et de contenu de TVIP"; Corrigendum 1 à la Recommandation UIT-T X.694 et Corrigendum 1 à la Recommandation UIT-T X.893 – Notation de syntaxe abstraite numéro un (ASN.1); version révisée de la série Z.100 – Langage SDL et version révisée de la série Z.160 – Notation de texte et de commande de test version 3 (TTCN-3). La CE 17 a aussi approuvé un nouveau Supplément sur les cas d'utilisation du cadre de garantie d'authentification des entités (EAA) et a révisé le guide de mise en œuvre des Recommandations UIT-T de la série Z.

3.3 La CE 17 a organisé un [Atelier de l'UIT d'une journée sur la sécurité des technologies financières](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx), le 26 août 2019, au terme duquel des propositions ont été formulées concernant les activités de suivi que la CE 17 pourrait mener en collaboration avec d'autres organismes reconnus de normalisation s'occupant de la sécurité des technologies financières, à l'instar du Groupe spécialisé de l'UIT-T sur l'application de la technologie des registres distribués (FG-DLT), du Groupe spécialisé de l'UIT-T sur la monnaie numérique, y compris la monnaie fiduciaire numérique (FG-DFC), du Comité technique (TC) 307 de l'ISO et du World Wide Web Consortium (W3C) sur les technologies DLT. La CE 17 a aussi organisé un [mini-atelier sur les problèmes de cybersécurité que pose la conduite automatisée](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx), le 26 août 2019, en coopération avec la Collaboration de l'UIT sur les normes de communication pour les systèmes de transport intelligents (CITS) et le Groupe de travail 29 (WP29) de la Commission économique des Nations Unies pour l'Europe (CEE).

3.4 En raison de l'épidémie de maladie à coronavirus dans le monde, la réunion de la CE 17 qui s'est déroulée du 17 au 26 mars 2020 a été la première réunion d'une Commission d'études de l'UIT-T à se tenir de manière entièrement virtuelle. En outre, la CE 17 a dû reporter son atelier [organisé conjointement avec le TC 307 de l'ISO sur le thème "Sécurité des technologies de registres distribués (DLT), gestion des identités et vie privée"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200316/Pages/default.aspx), prévu initialement le 16 mars 2020.

3.5 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)".

3.6 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.

3.7 La CE 13 de l'UIT-T a approuvé l'Amendement 1 à la Recommandation UIT-T Y.3053 (2018) "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", le Corrigendum 1 à la Recommandation UIT-T Y.3514 "Informatique en nuage – Cadre et exigences concernant la confiance pour les échanges inter-nuages" et la Recommandation UIT-T Y.3517 "Informatique en nuage – Aperçu de la gestion de la confiance inter-nuages".

3.8 La CE 15 de l'UIT-T élabore actuellement le Supplément (G.Sup.otnsec) qui contient une description du langage et d'une infrastructure de données commune dans les couches de protocole existantes du réseau de transport optique (OTN), qui sont nécessaires pour utiliser de manière indépendante les protocoles cryptographiques proposés en vue d'élaborer des solutions de transport sécurisées sur certaines couches OTN.

3.9 La CE 20 de l'UIT-T a approuvé la Recommandation UIT-T Y.4807 "Intégration du principe d'agilité dès la conception pour la sécurité des systèmes de télécommunication/TIC utilisés dans l'Internet des objets".

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'apprentissage machine pour les réseaux futurs, y compris la 5G (FG-ML5G*](https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx#/fr)*)*; 2) [*Groupe spécialisé de l'UIT-T sur les technologies pour le réseau 2030 (FG NET-2030)*](https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx#/fr); 3) [*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); 4) [*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);

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#/fr); et 6) [*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).

3.11 L'UIT, en collaboration avec la Fondation Bill & Melinda Gates, le Groupe de la Banque mondiale et la Banque des règlements internationaux, a organisé un [atelier sur la sécurité, l'infrastructure et la confiance dans les services financiers numériques](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Pages/default.aspx), les 4 et 5 décembre 2019 au siège de l'UIT, à Genève (Suisse).

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).

# 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 76 pays, et prend actuellement les mesures de suivi nécessaires. La participation directe à 14 de ces activités a pris fin. Dans le cadre du projet "*Mise en œuvre de services CIRT et des capacités connexes*", l'État de Palestine a bénéficié d'une assistance dans la mise en place et le déploiement des capacités techniques et des formations associées concernant les activités d'une équipe CIRT. Les Kiribati et les îles Salomon ont bénéficié d'une assistance afin d'élaborer leur stratégie nationale en matière de cybersécurité. En Papouasie-Nouvelle-Guinée et à Vanuatu, les capacités des équipes CIRT ont été renforcées dans le cadre du [projet de l'UIT en coopération avec le Département des communications et des arts de l'Australie (UIT-DoCA](https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9RAS18061)). Des ateliers visant à évaluer l'état de préparation en vue de la création d'une équipe CIRT ont été organisés au Libéria et au Tchad. En Gambie, les parties prenantes nationales de l'équipe CIRT ont bénéficié d'une formation concernant les activités de cette équipe. Quatre projets visant à créer des équipes CIRT ont débuté au Botswana, au Burundi, en Gambie et au Malawi, et sont encore en cours de mise en œuvre. Au Kenya, l'équipe CIRT existante est en cours de consolidation (achèvement prévu en 2020).

4.2 L'UIT a réalisé 28 [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), auxquels plus de 100 pays ont participé. Des cyberexercices ont été organisés en [Ouganda](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Africa-Cyberdrill-2019.aspx) (pour la région Afrique, en novembre 2019), à [Oman](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx) (pour la région des États arabes, en octobre 2019), en [Malaisie](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/ASP-CIS-Cyberdrill-2019.aspx) (pour la région Asie-Pacifique, en septembre 2019) et en Roumanie (pour la région Europe et la Communauté des États indépendants, en mai 2019). Il est prévu d'organiser cinq cyberexercices en 2020.

# 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.

5.2 À la suite de la CMDT-17, la CE 2 de l'UIT-D poursuit ses travaux sur 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)) pendant la période d'études 2018-2021.

5.3 Le Guide UIT sur l'élaboration d'une stratégie nationale en matière de cybersécurité de l'UIT est un guide rassemblant des bonnes pratiques qui est utilisé par des pays de toutes les régions. Les ateliers suivants ont été organisés en 2019: a) un atelier régional, organisé par le Ministère de l'informatique et l'agence de la cybersécurité de l'Indonésie à Jakarta, sur les stratégies en matière de cybersécurité (les débats ont porté notamment sur le règlement général sur la protection des données); b) un atelier régional, organisé par la Macédoine du Nord sur l'amélioration des stratégies nationales de cinq États de la région des Balkans; c) un atelier régional, organisé en Tunisie sur l'amélioration des stratégies nationales des pays des régions Afrique et des États arabes. Vingt pays ont participé de manière active. Trois pays ont bénéficié d'une assistance directe afin d'élaborer et de réviser des stratégies nationales en matière de cybersécurité, en s'inspirant du guide.

5.4 Le Soudan a bénéficié d'une assistance technique et du renforcement de ses capacités, en vue d'améliorer sa stratégie en matière de protection de l'infrastructure informatique essentielle.

5.5 Lors de la semaine régionale sur la cybersécurité organisée pour la région des États arabes, le Centre régional de cybersécurité de l'UIT pour la région des États arabes (UIT ARCC) a encouragé l'échange d'informations et le renforcement des capacités dans le domaine de la cybersécurité. Cette manifestation a offert un cadre à des hauts responsables dans le domaine des TIC et de la cybersécurité issus de la région pour rencontrer les principales parties prenantes et débattre des menaces, des progrès accomplis, des perspectives et des défis que pose la cybersécurité.

5.6 La semaine de la cybersécurité organisée en Moldavie s'est tenue à Chisinau avec l'appui de l'UIT. Cette manifestation a offert des possibilités de nouer des contacts ainsi qu'une plate-forme où échanger des idées, débattre et collaborer en vue de promouvoir, grâce à l'innovation, des stratégies et des solutions en matière de cybersécurité à l'échelle mondiale.

5.7 La manifestation "Cyber Shield" de 2019 s'est tenue à Ankara (Turquie) avec l'appui de l'UIT. Les principaux objectifs étaient d'augmenter les capacités d'intervention et les niveaux de préparation en cas d'incident, d'approfondir la compréhension mutuelle des cyberrisques et de leurs effets, et de garantir une collaboration constante entre les acteurs de la cybersécurité dans le monde, en particulier les équipes CIRT des pays, afin de limiter les cybermenaces. L'UIT a aussi organisé une formation à l'intention du Kirghizistan sur la manière de créer un centre d'activités liées à la cybersécurité.

5.8 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)

5.9 Le troisième [Indice mondial de cybersécurité](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) de l'UIT montre un renforcement considérable de l'importance accordée à la cybersécurité partout dans le monde. La quatrième version de l'enquête sur l'Indice mondial de cybersécurité, dont le questionnaire et la méthodologie ont été perfectionnés, a été présentée. En partenariat avec le cabinet Deloitte, un examen de l'environnement de la cybersécurité a été réalisé pour la Côte d'Ivoire, portant également sur les résultats concernant l'Indice GCI du pays. Grâce à cet examen, le pays a pu recenser les initiatives relatives à la cybersécurité qu'il devra déployer en priorité pour améliorer sa stratégie en la matière.

# 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 L'UIT fournit actuellement un appui à la Présidence du G20 en 2020 (Arabie saoudite), à sa demande, en tant que partenaire pour le partage des connaissances dans divers volets, notamment le volet prioritaire sur la sécurité dans l'économie numérique, dans le cadre de l'action multi-parties prenantes menée par le secrétariat du G20 pour solliciter la participation des organisations internationales compétentes.

6.3 En tant que coordonnateur principal pour la grande orientation C5 du SMSI, l'UIT a organisé plusieurs sessions au [Forum 2019 du SMSI](https://www.itu.int/net4/wsis/forum/2019/), en particulier une session de haut niveau sur l'intelligence artificielle et la confiance, ainsi qu'une session sur l'importance des mesures dans le domaine de la cybersécurité.

6.4 Conformément aux instructions données par le Conseil à sa session de 2019, le Secrétaire général soumet à la session de 2020 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.

# 7 Protection en ligne des enfants (COP)

7.1 Un groupe de travail multi-parties prenantes composé de plus de 50 organisations et experts a entamé l'examen des [Lignes directrices sur la protection en ligne des enfants](https://www.itu.int/en/cop/Pages/guidelines.aspx), qui ont été publiées pour la première fois en 2009.

7.2 En Afrique, des discussions ont commencé avec le Kenya, le Malawi, le Rwanda et le Tchad concernant la mise en œuvre de cadres stratégiques au niveau national. En particulier, le Forum régional sur la protection en ligne des enfants, organisé au Ghana, a rassemblé un large éventail d'experts en vue d'examiner des solutions et les mesures qui pourraient être prises. Dans la région Asie-Pacifique, une assistance a été fournie pour l'élaboration du cadre régional ASEAN sur la protection en ligne des enfants, conformément aux Lignes directrices sur la protection en ligne des enfants et en coordination avec d'autres partenaires, tels que TELSOM/TELMIN. D'autres activités ont été organisées en Europe, dans le cadre de l'initiative régionale visant à renforcer la confiance dans l'utilisation des TIC.

7.3 L'UIT assure le secrétariat de la Commission "Le large bande au service du développement durable". Le Groupe de travail sur la sécurité en ligne des enfants, dirigé par la Fondation World Childhood et par Zain, a publié son [rapport](https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf) exhaustif en octobre 2019 à New York. Les lignes directrices sur la protection en ligne des enfants ont été incluses en tant que référence et ont servi de base à la mise en œuvre des recommandations figurant dans le rapport.

7.4 Une étude régionale sur les stratégies nationales en vue d'assurer la sécurité en ligne des adolescents et des enfants a été rédigée pour examen et soumise à la consultation des pays. En outre, une assistance a été fournie à la Géorgie et à l'Ukraine concernant l'élaboration d'une stratégie nationale sur la protection en ligne des enfants.

7.5 L'UIT a organisé diverses activités pour célébrer la Journée 2020 pour un Internet plus sûr, notamment avec la promotion de la protection en ligne des enfants. La nouvelle mascotte de la protection en ligne des enfants a été présentée à cette occasion. [Le personnage et son histoire](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) ont été imaginés et créés par des enfants début janvier 2020.

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