|  |  |
| --- | --- |
| **Conseil 2021Consultation virtuelle des Conseillers, 8-18 juin 2021** |  |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.4** | **Document C21/36-F** |
| **22 avril 2021** |
| **Original: anglais** |
| Rapport du Secrétaire général |
| rapport DÉCRIVANT la façon dont le cadre offert par le Programme mondial cybersÉcuritÉ (GCA) est actuellement utilisÉ par l'UIT |

|  |
| --- |
| RésuméÀ sa session de 2019, le Conseil a chargé le Secrétaire général, en parallèle, de lui présenter à sa prochaine session 1) un rapport décrivant la façon dont le cadre offert par le [Programme mondial cybersécurité](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (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 (Documents [C19/117](https://www.itu.int/md/S19-CL-C-0117/en) et [C19/58](https://www.itu.int/md/S19-CL-C-0058/en)).Conformément à ces instructions, un projet de lignes directrices relatives à l'utilisation du Programme GCA par l'UIT a été élaboré avec l'appui de M. Stein Schjolberg, premier juge (retraité et ancien président du Groupe HLEG), et avec la participation des États Membres et d'autres parties prenantes, pour examen par le Conseil (voir le Document C21/71).En parallèle, le présent rapport, qui décrit comment l'UIT utilise actuellement le Programme GCA, est soumis au Conseil pour examen. Une version précédente du présent rapport a initialement été élaborée sous la cote [C20/36](https://www.itu.int/md/S20-CL-C-0036/en) en vue de sa soumission à la session de 2020 du Conseil, mais n'a pas été examinée.Suite à donnerLe Conseil est invité à **prendre note** du présent rapport.\_\_\_\_\_\_\_\_\_\_\_\_Références[*Programme mondial cybersécurité (GCA)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*;* [*Document C21/71*](https://www.itu.int/md/S21-CL-C-0071/en) *du Conseil* |

# 1 Introduction

**1.1** La Conférence de plénipotentiaires de l'UIT tenue à Dubaï en 2018 a adopté la Résolution 130 intitulée *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*, par laquelle il est décidé, entre autres choses, d'utiliser le cadre qu'offre le [*Programme mondial cybersécurité (GCA)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) de l'UIT pour mieux orienter les travaux de l'Union sur les efforts visant à instaurer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC).

**1.2** Lors des discussions qui ont eu lieu en plénière juste avant l'adoption de la Résolution 130 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires, le Secrétaire général de l'UIT a noté avec satisfaction que lors des débats sur le projet de Résolution, l'importance du Programme GCA avait été largement reconnue. Il a invité la plénière à accepter de conserver le point 12.1 du décide, qui permettrait à l'UIT d'utiliser le Programme GCA pour guider ses travaux sur la confiance et la sécurité dans les TIC. Il demanderait l'avis du Conseil et de l'ancien président du Groupe d'experts de haut niveau sur le Programme GCA, M. Stein Schjolberg, juge, à ce sujet[[1]](#footnote-1).

**1.3** Un rapport de l'ancien président du Groupe d'experts de haut niveau sur le Programme GCA (HLEG) a été présenté à la session de 2019 du Conseil de l'UIT, indiquant que des lignes directrices appropriées pourraient être élaborées pour une meilleure utilisation du Programme GCA[[2]](#footnote-2). Le Conseil a chargé le Secrétaire général, en parallèle, de lui présenter à sa prochaine session 1) un rapport décrivant la façon dont le cadre offert par le Programme 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[[3]](#footnote-3).

**1.4** Conformément à ces instructions, un projet de lignes directrices relatives à l'utilisation du Programme GCA par l'UIT a été élaboré avec l'appui de M. Stein Schjolberg, premier juge (retraité et ancien président du Groupe HLEG) et avec la participation des États Membres, pour examen et approbation par le Conseil[[4]](#footnote-4). En parallèle, le Secrétaire général a élaboré le présent rapport qui décrit comment l'UIT utilise actuellement le Programme GCA, pour examen par le Conseil.

# 2 Rappel

**2.1** Une des missions premières de l'Union, qui lui a été confiée dans le cadre du Sommet mondial sur la société de l'information (SMSI) et de la Conférence de plénipotentiaires de l'UIT, est d'instaurer la confiance et la sécurité dans l'utilisation des TIC.

**2.2** Lors du SMSI, des chefs d'État et des dirigeants mondiaux ont désigné l'UIT comme coordonnateur de la grande orientation C5, intitulée "*Établir la confiance et la sécurité dans l'utilisation des TIC*". Pour s'acquitter de ce mandat, l'UIT a lancé le Programme GCA en 2007, cadre de coopération internationale dans ce domaine.

**2.3** Le GCA a été lancé en 2007. Il est conçu pour favoriser la coopération et l'efficacité, en encourageant la collaboration avec et entre toutes les parties prenantes.Le GCA est composé de cinq Piliers ou domaines d'activité: mesures juridiques, mesures techniques et de procédure, structures administratives, renforcement des capacités et coopération internationale.

**2.4** Par la suite, le Groupe d'experts de haut niveau sur le Programme GCA a été créé en octobre 2007, avec pour mission d'aider le Secrétaire général de l'UIT à formuler à l'intention des États Membres des propositions stratégiques sur la promotion de la cybersécurité. Il était présidé par M. Stein Schjolberg, premier juge (retraité).

**2.5** Le Groupe d'experts de haut niveau était composé de près de cent experts internationaux indépendants représentant de multiples parties prenantes du monde entier. Il a regroupé les avis à l'intention du Secrétaire général de l'UIT concernant les cinq Piliers dans un Rapport du Président établi en août 2008 (Rapport du HLEG de 2008)[[5]](#footnote-5).

**2.6** En 2008, les travaux sur les Piliers du GCA ont constitué une innovation majeure dans l'approche mondiale des questions de cybersécurité. Plus d'une décennie s'est écoulée depuis la présentation du Rapport du HLEG de 2008. Globalement, il est reconnu sur le plan international que les TIC sont un outil indispensable pour atteindre les Objectifs de développement durable (ODD) définis par les Nations Unies, et que pour atteindre ces Objectifs, il est important que tout un chacun, partout dans le monde ait confiance dans l'utilisation des TIC. L'objectif de "*renforcer la confiance et la sécurité dans l'utilisation des TIC*" est donc plus que jamais un but essentiel à la réalisation des ODD.

**2.7** Largement salué par les membres de l'UIT, le cadre qu'offrent les cinq Piliers du Programme GCA a, d'une manière générale, résisté à l'épreuve du temps et constitue toujours un large cadre de coopération internationale sur la cybersécurité, délimité par les documents adoptés par le SMSI, en particulier les principes énoncés dans la grande orientation C5. Toutes les activités de l'UIT dans ce domaine restent structurées autour des cinq Piliers du Programme GCA.

**2.8** Depuis le lancement du Programme GCA, l'UIT a toujours rendu compte au Conseil de ses activités visant à renforcer la confiance et la sécurité dans l'utilisation des TIC par le biais d'un rapport annuel organisé autour des cinq Piliers, qui montre la nature complémentaire des programmes de travail existants de l'UIT et facilite la mise en œuvre des activités du BDT, du TSB et du BR dans ce domaine.

**2.9** Des informations détaillées sur ces activités sont disponibles dans les Documents [C08/33](https://www.itu.int/md/S08-CL-C-0033/en), [C09/50](https://www.itu.int/md/S09-CL-C-0050/en), [C10/12](https://www.itu.int/md/S10-CL-C-0012/en), [C11/54](https://www.itu.int/md/S11-CL-C-0054/en), [C12/29](https://www.itu.int/md/S12-CL-C-0029/en), [C13/23](https://www.itu.int/md/S13-CL-C-0023/en), [C14/23](https://www.itu.int/md/S14-CL-C-0023/en), [C15/18](https://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), [C20/18](https://www.itu.int/md/S20-CL-C-0018/en) et [C21/18](https://www.itu.int/md/S21-CL-C-0018/en). Les sections suivantes contiennent quelques exemples d'activités menées par l'UIT dans le cadre du Programme GCA.

# 3 Quelques exemples des activités de l'UIT

**3.1** En tant que coordonnateur de la grande orientation C5, l'UIT s'appuie sur le cadre du Programme GCA pour réunir les différentes parties prenantes afin d'aider les pays à faire face aux risques associés aux TIC et travaille en étroite collaboration avec d'autres organisations, dans tous ses Secteurs et activités, pour instaurer la confiance dans l'utilisation des TIC.

**3.2** Tout en reconnaissant l'interdépendance mutuelle des cinq Piliers, des exemples des activités de l'UIT sur chacun des Piliers sont mis en évidence dans les sections ci-dessous. Celles-ci visent à donner un aperçu de certaines des activités, de plus amples détails étant disponibles dans les rapports annuels individuels soumis au Conseil depuis 2008 (voir le paragraphe 2.9 ci-dessus).

**3.3** Une section séparée a été incluse sur [l'Initiative sur la protection en ligne des enfants](https://www.itu.int/en/cop/Pages/default.aspx) comme exemple d'initiative transversale qui couvre les cinq Piliers du Programme GCA.

## 3.4 Pilier 1 du Programme GCA: Mesures juridiques

a) L'adoption d'une législation appropriée contre l'utilisation abusive des TIC à des fins criminelles et harmonisée avec les politiques et pratiques régionales et internationales fait partie intégrante de toute stratégie nationale de cybersécurité.

b) En ce qui concerne les mesures juridiques, l'UIT collabore étroitement avec des partenaires comme l'ONUDC et d'autres experts. En coopération avec ses partenaires, l'UIT continue d'aider 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.

## 3.5 Pilier 2 du Programme GCA: Mesures techniques et de procédure

a) Les [Commissions d'études de l'UIT](https://www.itu.int/fr/mediacentre/backgrounders/Pages/itu-study-groups.aspx) constituent une plate-forme neutre et mondiale permettant aux membres de l'UIT de se réunir et de travailler sur la normalisation liée à la sécurité dans divers domaines: les architectures et les cadres de sécurité; la sécurité des applications et des services des technologies actuelles et émergentes telles que les technologies des registres distribués (dont la chaîne de blocs est une mise en œuvre), l'informatique en nuage, les mégadonnées, l'intelligence artificielle et l'apprentissage machine, les réseaux pilotés par logiciel, la 5G, l'Internet des objets, les systèmes de transport intelligent et les réseaux intelligents; les bases de sécurité comme l'infrastructure PKI, la gestion de l'identité et l'authentification; et la cybersécurité (y compris l'échange de renseignements sur les cybermenaces).

b) [La Commission d'études 17 de l'UIT-T](https://www.itu.int/fr/ITU-T/studygroups/2013-2016/17/Pages/default.aspx) est chargée d'instaurer la confiance et la sécurité dans l'utilisation des TIC. Cela comprend l'étude de plusieurs technologies en matière de cybersécurité. En sa qualité de Commission d'études directrice chargée de la sécurité et de la gestion d'identité (IdM), elle continue de contribuer aux études et à la normalisation concernant la cybersécurité, la lutte contre le spam, la gestion d'identité, l'infrastructure de clé publique (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 extérieures. À ce jour la Commission a élaboré plus de 200 normes. Entre autres, elle travaille actuellement sur la sécurité quantique et a élaboré la Recommandation X.1702, qui spécifie l'"Architecture d'un générateur de nombres aléatoires pour le bruit quantique".

c) D'autres commissions d'études, comme la CE 9, la CE 13, la CE 15 et la CE 20 (IoT) travaillent aussi sur des normes dans le domaine de la sécurité.

d) Dans le cadre de leurs travaux, plusieurs [Groupes spécialisés de l'UIT-T](https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx) ont étudié ou étudient actuellement les aspects liés à la confiance et à la sécurité. C'est le cas notamment des groupes suivants: [*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)*;* [*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)*;*[*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)*;* [*Groupe spécialisé de l'UIT-T sur les technologies de l'information quantiques pour les réseaux (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx)*;* [*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)*;* [*Groupe spécialisé de l'UIT-T sur les réseaux autonomes (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx)*.*

e) 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).

## 3.6 Pilier 3 du Programme GCA: Structures administratives

a) Il faut mettre en place des mécanismes et des structures institutionnelles efficaces au niveau national pour lutter en toute fiabilité contre les cybermenaces et les incidents. L'absence de telles institutions et le manque de capacités nationales posent un véritable problème pour répondre de manière adéquate et efficace aux cyberattaques. Les [équipes nationales d'intervention en cas d'incident informatique (CIRT)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx) jouent un rôle essentiel dans la solution.

b) À ce jour, plus de 80 pays ont bénéficié d'une assistance en vue d'évaluer, au niveau national, leur état de préparation en matière de cybersécurité et leurs capacités d'intervention en cas d'incident. L'UIT a mis en œuvre 22 projets liés aux équipes CIRT, parmi lesquels sept sont en cours et quatre sont sur le point d'être achevés.

c) L'UIT organise régulièrement des [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) interrégionaux, régionaux, sous-régionaux et nationaux afin d'améliorer la capacité des pays à répondre aux menaces, renforçant ainsi la coopération nationale et internationale entre les États Membres de l'UIT contre les cybermenaces et les cyberattaques. À ce jour, l'UIT a organisé 31 [cyberexercices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) auxquels ont participé plus de 100 pays.

## 3.7 Pilier 4 du Programme GCA: Renforcement des capacités

a) 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.

b) L'UIT aide les États Membres à élaborer et à améliorer des stratégies nationales efficaces en matière de cybersécurité. [Le Guide UIT sur l'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-F.pdf), élaboré dans le cadre d'un processus de collaboration entre de multiples parties prenantes, constitue un manuel de bonnes pratiques et un kit pratique qui a été utilisé par les pays de toutes les régions pour élaborer et améliorer leurs stratégies de cybersécurité. Depuis son lancement en septembre 2018, des ateliers nationaux et régionaux ont été organisés dans plus de vingt pays, dont trois ont reçu une assistance directe pour élaborer et réviser leurs stratégies nationales de cybersécurité à l'aide du Guide. Le processus de mise à jour du Guide NCS est en cours et devrait se conclure en octobre 2021.

c) En 2015, l'UIT a lancé [l'Indice mondial de cybersécurité](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI), qui est devenu une référence fiable mesurant l'engagement des pays en faveur de la cybersécurité au niveau mondial – pour sensibiliser à l'importance et aux différentes dimensions de la question. Le niveau de développement ou de mobilisation de chaque pays est évalué en fonction des cinq Piliers du Programme GCA, qui constituent la base et le cadre général de l'initiative. Fondé sur une approche et une initiative multi-parties prenantes, l'indice GCI tire parti des compétences et des capacités de différentes organisations, dans l'objectif d'améliorer la qualité de l'enquête, d'instituer une coopération au niveau international et d'encourager l'échange de connaissances à ce sujet. Le rapport sur la quatrième version de l'indice GCI sera publié en 2021. Les travaux concernant la cinquième version de l'indice devraient débuter au troisième trimestre de 2021.

d) 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 ses partenaires continuent de proposer des activités de formation et des ateliers dans divers domaines liés à la cybersécurité.

e) En collaboration avec ses partenaires, l'UIT participe en outre à un certain nombre d'activités en matière de cybersécurité centrées sur l'égalité hommes-femmes et sur les jeunes, telles que l'initiative [Youth4Cyber](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Youth-for-Cyber/Youth4Cyber.aspx) et le [Programme de mentorat "Les femmes dans le secteur de la cybersécurité"](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme.aspx).

## 3.8 Pilier 5 du Programme GCA: Coopération internationale

a) Le GCA repose sur la coopération internationale et vise à faire en sorte que toutes les parties prenantes concernées unissent leurs efforts pour instaurer la confiance et la sécurité dans l'utilisation des TIC.

b) L'UIT continue de nouer et d'entretenir des relations et des partenariats avec diverses organisations et initiatives régionales ou internationales, notamment le Forum économique mondial, la Commonwealth Cybercrime Initiative, l'ENISA, INTERPOL, la CEDEAO, la Banque mondiale, l'ONUDC, FIRST et des associations régionales d'équipes CSIRT/CERT, comme AP CERT, AFRICA CERT et OIC CERT. Ces partenariats facilitent la collaboration entre de multiples parties prenantes sur des activités qui recoupent tous les Piliers du Programme GCA.

c) En tant que coordonnateur de la grande orientation C5 du SMSI, l'UIT s'appuie sur le processus du SMSI, y compris le Forum annuel du SMSI, pour faciliter le dialogue multi-parties prenantes. L'UIT organise chaque année des dialogues de haut niveau, des réunions de coordonnateurs de la grande orientation C5 et des ateliers ciblés sur le thème de la cybersécurité lors du [Forum du SMSI](https://www.itu.int/net4/wsis/forum/2019/fr).

d) Reconnaissant l'importance d'œuvrer à l'établissement d'une communauté de vues au sein des Nations Unies sur les besoins et les exigences à remplir pour établir correctement des programmes et des initiatives qui appuieraient efficacement les efforts entrepris par toutes les parties prenantes, une première étape importante a été franchie en 2010 en vue de renforcer la coordination interne entre les institutions spécialisées des Nations Unies dans leur assistance aux États Membres en matière de cybersécurité. Sur demande du Conseil des Chefs de secrétariat des organismes des Nations Unies pour la coordination (CCS), l'UIT et l'ONUDC, en collaboration avec 33 autres institutions des Nations Unies, ont mené pendant deux ans un effort pour mettre au point un cadre à l'échelle du système des Nations Unies sur la cybersécurité et la cybercriminalité, qui a été approuvé par le CCS en novembre 2013. Depuis lors, l'UIT a continué à contribuer à diverses initiatives connexes qui visent à améliorer la coordination et la coopération internes au sein du système des Nations Unies.

## 3.9 L'Initiative de protection en ligne des enfants

a) L'UIT a lancé [l'Initiative de protection en ligne des enfants (COP)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) en novembre 2008. Celle-ci est un effort de multiples parties prenantes dans le cadre du Programme GCA. Elle réunit des partenaires issus de tous les secteurs de la communauté internationale pour élaborer des stratégies de cybersécurité et favoriser des environnements en ligne sûrs pour les enfants du monde entier.

b) Les principaux objectifs de l'Initiative sont a) d'identifier les risques et les vulnérabilités auxquels les enfants sont confrontés dans le cyberespace, b) de les y sensibiliser, c) d'élaborer des outils pratiques pour contribuer à minimiser les risques et d) de partager des connaissances et des données d'expérience.

c) L'Initiative adopte une méthode globale de promotion de la sécurité en ligne des enfants et élabore des stratégies qui couvrent les cinq Piliers du Programme GCA:

**• mesures juridiques**: en vue de promouvoir un environnement en ligne propice et plus sûr pour les enfants et les jeunes, il est essentiel de pouvoir s'appuyer sur un cadre juridique sans faille. L'Initiative COP recense les approches adoptées par divers pays dotés de systèmes juridiques différents, et formule des lignes directrices visant à aider les États Membres à atteindre leurs objectifs;

**• mesures techniques et de procédure**: l'Initiative COP élabore des recommandations et des normes fondamentales en vue de faciliter la protection en ligne des enfants par toutes les parties prenantes essentielles;

**• structures administratives**: l'Initiative COP promeut l'application d'un cadre national type afin de favoriser la mise en place d'un environnement en ligne positif pour les enfants et les jeunes. Elle encourage la création d'équipes de protection en ligne des enfants au niveau national et élabore actuellement une série d'indicateurs destinés à faciliter la mesure des progrès accomplis dans la mise en œuvre des initiatives de protection en ligne des enfants aux niveaux national, régional et mondial;

**• renforcement des capacités**: l'Initiative COP aide les pays à mettre en œuvre des cadres nationaux de protection en ligne des enfants et organise des manifestations stratégiques aux niveaux régional et mondial afin d'appuyer ces processus;

**• coopération internationale**: l'Initiative COP promeut une culture de citoyenneté numérique mondiale et encourage la création d'accords de coopération portant sur le partage d'informations, afin d'éliminer ou d'atténuer les risques auxquels sont exposés les enfants et les jeunes en ligne.

d) Diverses activités ont été entreprises au titre des différents Piliers du Programme GCA, dont les détails sont disponibles sur le [site web de l'Initiative COP](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) ainsi que dans les rapports annuels présentés au Conseil depuis le lancement de l'Initiative. Ces activités comprennent l'élaboration d'outils et de ressources comme des lignes directrices pour les enfants, les parents et les éducateurs, le secteur privé et les décideurs. Un groupe de travail multi-parties prenantes composé de plus de 50 organisations et experts individuels ont examiné les quatre volumes des [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, et ont publié un ensemble révisé de Lignes directrices en 2020.

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

1. Procès-verbal de la dix-septième séance plénière de la Conférence de plénipotentiaires, Dubaï, jeudi 15 novembre 2018. [↑](#footnote-ref-1)
2. Transmission du Rapport de l’ancien président du Groupe d’experts de haut niveau sur le Programme GCA (C19/58), UIT, 8 mai 2019, <https://www.itu.int/md/S19-CL-C-0058/en>. [↑](#footnote-ref-2)
3. Compte rendu de la sixième séance plénière (C19/117), UIT, 20 juin 2019, <https://www.itu.int/md/S19-CL-C-0117/en>. [↑](#footnote-ref-3)
4. Pour obtenir de plus amples informations, veuillez consulter la page <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. Voir juge Stein Schjolberg: Rapport du président du HLEG:
<https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-5)