|  |  |
| --- | --- |
| **Conseil 2022Genève, 21-31 mars 2022** |  |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.4** | **Révision 2 duDocument C22/32-F** |
| **25 mars 2022** |
| **Original: anglais** |
| Rapport du Secrétaire général |
| PROJET de lignes directrices relatives à l'utilisation, par l'UIT,du Programme mondial cybersÉCURITÉ |

|  |
| --- |
| 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 (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 et C19/58).Conformément à ces instructions, un projet de lignes directrices, élaboré avec l'appui de M. Stein Schjolberg, premier juge (retraité et ancien Président du Groupe HLEG), de Mme Solange Ghernaouti et de M. Noboru Nakatani, et avec la participation des États Membres et d'autres parties prenantes, ainsi que le rapport du secrétariat (Document C21/36), ont été soumis à la consultation virtuelle des Conseillers de 2021 (C21/VCC-1) pour examen et approbation (Document C21/71).Suite à la C21/VCC-1, les États Membres du Conseil ont pris note du rapport du secrétariat et, s'agissant du projet de lignes directrices, ont décidé de charger le secrétariat de mener de nouvelles consultations avec les États Membres du Conseil, compte tenu des contributions reçues et des commentaires formulés à cette séance. Le secrétariat devra présenter un document révisé pour examen et approbation à la prochaine session du Conseil.En conséquence, de nouvelles consultations ont été menées avec les États Membres du Conseil et, compte tenu des contributions reçues, le projet de lignes directrices révisées ci-après a été élaboré, assorti d'un document d'information complémentaire (Document [C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/en)). Il importe de noter que cette initiative n'a pas vocation à traiter les questions liées à la révision du Programme GCA.Suite à donnerLe présent document est soumis au Conseil pour **examen** et **approbation**, selon qu'il conviendra.\_\_\_\_\_\_\_\_\_\_\_\_Références[*Résolution 130 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-F.pdf)*,* [*Programme mondial cybersécurité (GCA)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*, Documents*[*C21/36*](https://www.itu.int/md/S21-CL-C-0036/en)*,* [*C21/71*](https://www.itu.int/md/S21-CL-C-0071/en)*,* [*C19/117*](https://www.itu.int/md/S19-CL-C-0117/en)*,* [*C19/58*](https://www.itu.int/md/S19-CL-C-0058/en) *et* [*C22/INF/8*](https://www.itu.int/md/S22-CL-INF-0008/en) *du Conseil* |

# Section 1 Introduction

**1.1** La Conférence de plénipotentiaires de l'UIT tenue à Dubaï en 2018 a adopté la [Résolution 130](https://www.itu.int/en/action/cybersecurity/PublishingImages/Lists/resolutions/AllItems/Res%20130.pdf) (Rév. Dubaï, 2018) 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) 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 cette Résolution, le Secrétaire général de l'UIT *a noté avec satisfaction que lors des discussions 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, 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](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (HLEG) a été présenté à la session de 2019 du Conseil de l'UIT. Ce rapport préconise l'élaboration de lignes directrices appropriées pour une meilleure utilisation du Programme mondial cybersécurité[[2]](#footnote-2). Lors de cette session, 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 (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, le processus d'élaboration du projet de lignes directrices a été défini dans une Lettre circulaire [(CL-20/55)](https://www.itu.int/md/S20-SG-CIR-0055/en) et deux consultations ouvertes ont été menées à l'intention de toutes les parties prenantes du SMSI le 23 avril 2020 et le 1er mars 2021, pour leur permettre de formuler des observations sur le projet de lignes directrices (consultation ouverte). Plus de 160 participants ont assisté aux réunions et présenté des observations sur chaque section du projet de lignes directrices. Tous les commentaires reçus des participants par écrit avant ou après les consultations ouvertes ont également été publiés sur le [site web](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) du Programme GCA.

**1.5** Compte tenu des contributions reçues, le secrétariat a élaboré un rapport décrivant la façon dont l'UIT utilise actuellement le cadre offert par le Programme GCA ([rapport du secrétariat](https://www.itu.int/md/S21-CL-C-0036/en)) et le projet de lignes directrices relatives à l'utilisation du Programme GCA ([projet de lignes directrices](https://www.itu.int/md/S21-CL-C-0071/en)) 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, est soumis pour examen et approbation par le Conseil. Le Secrétaire général remercie aussi Mme Solange Ghernaouti (Swiss Cybersecurity Advisory & Research Group, Université de Lausanne) de ses suggestions et contributions sur les sections relatives aux Piliers 2 et 4 du Programme GCA et M. Noboru Nakatani (ancien Directeur exécutif du Complexe mondial INTERPOL pour l'innovation) sur la section relative au Pilier 3 du Programme GCA. Il importe de noter que cette initiative n'a pas vocation à traiter les questions liées à la révision du Programme GCA.

**1.6** En raison de la pandémie de COVID-19, la présentation de ces documents a été repoussée à la VCC 2021, qui s'est tenue du 8 au 18 juin 2021. Suite à la VCC 2021, les États Membres du Conseil ont pris note du rapport du secrétariat et, s'agissant du projet de lignes directrices, ont décidé par correspondance de "*charger le secrétariat de mener de nouvelles consultations avec les États Membres du Conseil, compte tenu des contributions reçues et des commentaires formulés à cette séance. Le secrétariat devra présenter le* [*Document 71*](https://www.itu.int/md/S21-CL-C-0071/en) *révisé pour examen et approbation à la prochaine session du Conseil*".

**1.7** En conséquence, de nouvelles consultations ont été menées avec les États Membres du Conseil et, compte tenu des contributions reçues, deux documents ont été élaborés:

a) un document d'information (Document [C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/en)) décrivant le cadre général, l'évolution de l'environnement et le contexte de l'élaboration du présent projet de lignes directrices; et

b) le présent projet de lignes directrices, présenté ci-dessous, qui a été élaboré en vue d'être soumis à la session de 2022 du Conseil pour examen et approbation.

Pour élaborer ces documents, il a été tenu compte des recommandations du Rapport du groupe HLEG de 2008, des activités de l'UIT depuis lors, des évolutions sur le terrain depuis 2008 et des [contributions soumises par les États Membres](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) et d'autres parties prenantes (conformément aux Lettres circulaires [CL-20/18](https://www.itu.int/md/S20-SG-CIR-0018/en) et [CL‑20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)).

**1.8** Tout en reconnaissant l'interdépendance mutuelle des cinq Piliers, chaque section traite d'un pilier spécifique du Programme GCA et propose des lignes directrices spécifiques pour son utilisation. La Section 2 porte sur les mesures juridiques. La Section 3 porte sur les mesures techniques et de procédure. La Section 4 porte sur le renforcement des capacités. La Section 5 porte sur les structures administratives et la Section 6 sur la coopération internationale. La Section 7 contient quelques lignes directrices générales et transversales pour l'utilisation du cadre du Programme GCA.

# Section 2 Pilier 1 – Mesures juridiques

**2** Compte tenu des progrès rapides de la technologie, les mesures prises par les organisations et les pays doivent évoluer pour suivre le rythme du changement. Cela rend le défi de la cybersécurité encore plus complexe et exige un examen approfondi sous différents angles. Dans ce contexte, les lignes directrices proposées pour l'utilisation du Pilier 1 par l'UIT dans le cadre de son mandat sont présentées ci‑dessous:

**a)** L'UIT devrait poursuivre ses efforts pour faciliter les discussions et la collaboration multipartites en vue de surmonter les difficultés liées à la cybersécurité et, en particulier, renforcer ses relations avec toutes les parties prenantes pour fournir une assistance aux États Membres à cet égard.

**b)** L'UIT devrait continuer de collaborer avec les partenaires concernés pour favoriser le développement et la tenue à jour des ressources sur la cybersécurité et les législations relatives à la cybercriminalité, pour aider les États Membres à mieux cerner les aspects juridiques de la cybersécurité, y compris les cadres et les bonnes pratiques régionaux et internationaux pertinents existants, tout en favorisant l'échange de données d'expériences et de connaissances entre les États Membres pour les aider à élaborer des cadres dans ce domaine.

**c)** L'UIT, en collaboration avec toutes les parties prenantes concernées, devrait favoriser une meilleure compréhension des difficultés et des risques juridiques liés à la cybersécurité que présentent les technologies émergentes et faciliter l'échange d'études de cas et de bonnes pratiques aux niveaux national, régional et international.

**d)** L'UIT devrait continuer à renforcer le programme Protection en ligne des enfants en tant que plate-forme de travail avec des partenaires et des parties prenantes pour favoriser l'échange de connaissances, d'informations et d'activités (y compris celles qui concernent les mesures juridiques) pouvant faciliter et soutenir l'action des pays sur cette question essentielle.

# Section 3 Pilier 2 – Mesures techniques et de procédure

**3** Toutes les recommandations relatives au Pilier 2 figurant dans le Rapport du groupe HLEG de 2008 restent valables. Compte tenu de cela, les lignes directrices suivantes sont proposées pour le Pilier 2:

**a)** Les commissions d'études de l'UIT devraient se concentrer sur les technologies émergentes associées aux télécommunications/TIC, afin d'étudier et de proposer des lignes directrices en matière de cybersécurité et des recommandations visant à instaurer la confiance et la sécurité dans l'utilisation de ces technologies, et recommander aux États Membres d'adopter ces lignes directrices à titre volontaire et en temps utile.

**b)** Un mécanisme de coopération étroite devrait être établi entre les différentes commissions d'études de l'UIT-T concernant l'étude des questions liées à la cybersécurité, la CE 17 jouant un rôle de coordination ou de direction, de façon que le plus haut degré possible de sécurité de bout en bout soit maintenu tout au long du processus de normalisation de tous les composants et toutes les interfaces des produits TIC.

**c)** Une coordination et une collaboration étroites, sur la base de la réciprocité, entre l'UIT et d'autres organisations de normalisation, devraient être encouragées pour garantir que la sécurité de bout en bout des diverses applications et des divers services soit maintenue tout au long du cycle de vie du produit.

**d)** L'UIT devrait continuer de diffuser les normes de sécurité des TIC au niveau mondial et travailler avec d'autres organisations de normalisation et les groupes du secteur privé pour les encourager à soumettre leurs normes sur les mesures techniques et de procédure à l'UIT‑T et à l'UIT-R pour approbation en tant que Recommandations UIT-T et UIT-R.

**e)** L'UIT devrait poursuivre ses efforts en vue d'élaborer des Recommandations sur les mesures techniques et de procédure en matière de cybersécurité dans les domaines relevant de son mandat, en incitant ses membres à renforcer leur participation aux activités de normalisation connexes de l'UIT, en établissant des partenariats stratégiques et en menant des consultations avec les établissements universitaires et les organisations de normalisation.

**f)** L'UIT devrait continuer d'encourager ses membres à prendre l'initiative d'accords de certification mutuelle, ou à participer à de tels accords, en vue de mettre en place des normes harmonisées en matière de cybersécurité.

# Section 4 Lignes directrices pour l'utilisation du Pilier 3 – Structures administratives

**4** Tout en reconnaissant que les recommandations du Rapport du groupe HLEG de 2008 ont contribué à orienter les efforts de l'UIT dans le cadre du Pilier 3 et restent pertinentes, les lignes directrices proposées ci-après, qui concernent en particulier les travaux du Bureau de développement de l'UIT (BDT), pourraient permettre d'intensifier les efforts à cet égard:

**a)** L'UIT devrait continuer à aider les pays en développement, les pays les moins avancés et les petits États insulaires en développement (PEID) à concevoir et à mettre en place des équipes CIRT nationales et d'autres unités/organisations techniques connexes.

**b)** Pour éviter tout chevauchement d'activité, l'UIT devrait continuer d'encourager une collaboration ouverte et inclusive ainsi que, dans le cadre de son mandat, la coordination entre les diverses organisations nationales, régionales ou internationales participant à la mise en place de structures administratives nationales.

**c)** L'UIT devrait intensifier ses efforts pour mesurer les engagements institutionnels des États Membres, en s'appuyant sur des outils comme l'Indice mondial de cybersécurité (GCI), pour promouvoir la cybersécurité en tant que catalyseur intersectoriel des efforts qu'ils déploient en faveur de la transformation numérique.

**d)** Pour les structures nationales en particulier, et à la demande des États Membres, l'UIT devrait aider ces derniers à concevoir des stratégies relatives à un cadre de coordination faisant intervenir toutes les entités publiques, afin d'améliorer la mise en œuvre cohérente et transversale des efforts nationaux en matière de cybersécurité.

**e)** L'UIT devrait continuer d'encourager une plus grande collaboration entre les structures administratives de cybersécurité aux niveaux régional et mondial en menant des activités comme les cyberexercices, entre autres.

# Section 5 Lignes directrices pour l'utilisation du Pilier 4 – Renforcement des capacités

**5** À la lumière de ce qui précède, le Programme GCA et les recommandations contenues dans ce Pilier du Rapport du groupe HLEG de 2008 continuent de fournir un cadre solide qui améliore et favorise une approche interdisciplinaire du renforcement des capacités. Au regard de cette considération, il est proposé que l'UIT, par l'intermédiaire de son Bureau de développement des télécommunications (BDT):

**a)** Continue de favoriser une collaboration plus ouverte et plus inclusive, ainsi que la coordination, entre les diverses organisations nationales, régionales ou internationales participant au renforcement des capacités en matière de cybersécurité, afin de garantir l'efficacité et d'éviter tout chevauchement d'activité.

**b)** Continue d'apporter une assistance aux pays en développement, aux pays les moins avancés et aux PEID dans le cadre de leurs activités de renforcement des capacités en matière de cybersécurité, avec l'appui des communautés nationales et internationales de renforcement des capacités en matière de cybersécurité.

**c)** Continue d'aider les pays en développement, les pays les moins avancés et les PEID, en collaboration avec les partenaires intéressés et les communautés de développement des capacités, à élaborer des stratégies, des plans, des politiques et des capacités d'intervention en cas d'incident en matière de cybersécurité au niveau national.

Poursuive les activités de renforcement des capacités pour réduire l'écart en matière de normalisation, notamment en fournissant une assistance technique aux pays qui en font la demande.

**d)** Renforce et facilite l'échange de bonnes pratiques des États Membres, afin d'aider les pays en retard dans le domaine de la cybersécurité à améliorer leur situation en matière de cybersécurité et à réduire l'écart en matière de capacités.

**e)** Continue de faire évoluer ses activités de renforcement des capacités, en tenant compte de la nécessité d'acquérir de nouvelles compétences pour s'adapter aux possibilités offertes et aux difficultés posées par les technologies émergentes dans le domaine de la cybersécurité. À cet égard, il convient de favoriser une plus grande collaboration avec les établissements universitaires, le secteur privé et les États Membres.

**f)** Continue d'accorder une attention particulière aux besoins des groupes les plus vulnérables – comme les femmes, les enfants, les personnes handicapées et les personnes ayant des besoins particuliers ainsi que les personnes présentant un handicap lié à l'âge – dans les efforts de renforcement des capacités.

**g)** Continue de développer et de renforcer l'Indice GCI en tant qu'outil de renforcement des capacités et de sensibilisation.

**h)** Continue de soutenir les États Membres par le biais de programmes de renforcement des capacités pour les jeunes dans les systèmes d'éducation primaire, secondaire, universitaire et professionnelle des adultes afin de contribuer à la formation d'un plus grand nombre de professionnels de la cybersécurité dans le monde et de sensibiliser à la cybersécurité.

**i)** Continue de faciliter le recensement des activités de recherche liées à la cybersécurité entre les parties prenantes, en particulier dans les domaines des technologies émergentes, en tirant parti de la participation des membres de l'UIT issus du secteur privé et des milieux universitaires.

**j)** Diffuse des outils, des ressources et des bonnes pratiques aux États Membres, au secteur privé et aux autres parties prenantes, en vue d'appuyer leurs efforts pour renforcer la capacité des MPME à instaurer la confiance dans l'utilisation des TIC, et continue de promouvoir une culture de la cybersécurité.

# Section 6 Lignes directrices pour l'utilisation du Pilier 5 – Coopération internationale

**6** Les Nations unies ont un rôle unique à jouer pour favoriser la coopération, le dialogue et la coordination entre tous les pays, ainsi qu'avec le secteur privé et les autres parties prenantes, sur les questions de cybersécurité mondiale. Étant donné la nature transversale de ce Pilier et compte tenu de la diversité des collaborations et des partenariats dans les différents Secteurs de l'UIT, il est essentiel que tous les Secteurs de l'UIT travaillent en étroite collaboration et coordonnent leurs efforts, tant au niveau interne qu'externe, en utilisant des mécanismes de coordination intersectorielle efficaces et des coordonnateurs désignés. Les Recommandations du Rapport du groupe HLEG de 2008 à cet égard restent pertinentes et, sur la base des informations fournies dans la section ci-dessus, les lignes directrices suivantes sont proposées pour l'utilisation du Pilier 5 par l'UIT dans les domaines relevant de son mandat:

**a)** Compte tenu de sa position au sein du système des Nations Unies en tant qu'institution spécialisée dans le domaine des TIC et coordonnateur unique de la grande orientation C5 (Instaurer la confiance et la sécurité dans l'utilisation des TIC), l'UIT devrait continuer à jouer un rôle de premier plan en la matière.

**b)** Sur la base du processus du SMSI, notamment les processus liés à la grande orientation C5, et compte tenu des efforts du Groupe de haut niveau du Secrétaire général des Nations Unies sur la coopération numérique, l'UIT devrait contribuer à soutenir les efforts de facilitation en réunissant les différents acteurs, y compris dans le cadre du Forum du SMSI et de l'IGF, entre autres.

**c)** Étant donné la nature mondiale des inquiétudes en matière de cybersécurité, il convient de continuer à encourager et à faciliter des échanges plus larges entre les principaux acteurs dans le cadre de groupes plus nombreux, comprenant le secteur privé, les organisations du système des Nations Unies, les milieux universitaires, la société civile et d'autres parties prenantes, en vue d'atténuer les problèmes qui y sont associés. L'UIT devrait jouer un rôle important dans ces échanges plus larges, selon qu'il convient.

**d)** L'UIT devrait continuer à étudier des mécanismes novateurs et souples pour établir des partenariats, en tenant compte de l'évolution rapide du secteur technologique et de l'éventail des nouvelles entités qui apparaissent – en particulier les start-up et les MPME.

**e)** L'UIT devrait continuer de collaborer avec d'autres institutions clés du système des Nations Unies afin d'appuyer les initiatives internes prises par le secrétariat des Nations Unies pour harmoniser et rationaliser ses programmes et activités en matière de cybersécurité, de façon à être plus efficace au service de la communauté internationale.

# Section 7 Lignes directrices générales pour le cadre du Programme GCA

**7** Le processus d'élaboration de lignes directrices pour l'utilisation du Programme GCA a permis de dégager quelques grandes lignes directrices transversales qui sont applicables et pertinentes dans le cadre des travaux de l'UIT et des cinq Piliers du Programme GCA. Reconnaissant les liens étroits entre les Piliers et la nécessité pour l'UIT et ses membres d'œuvrer à une vision globale et complète de l'action en matière de cybersécurité, ces lignes directrices générales sont proposées ci-dessous:

**a)** Compte tenu de la multiplication de parties prenantes, d'organisations, de partenariats et de tribunes qui travaillent sur la cybersécurité et sont à l'origine de différents aspects des progrès accomplis, l'UIT devrait continuer de renforcer et d'étendre sa collaboration et son action au profit de toutes ces parties prenantes, pour améliorer le partage des connaissances et l'échange de renseignements et de compétences tout en évitant tout chevauchement des activités.

**b)** L'UIT devrait regrouper les informations pour les diverses activités, initiatives et projets mondiaux qui sont menés sur différents aspects de la cybersécurité par d'autres parties prenantes et organisations actives dans ce domaine qui pourront être investies du mandat, du rôle et/ou des responsabilités principaux pour ces aspects spécifiques, de façon à permettre à la communauté internationale d'avoir un point d'accès facile à toutes ces ressources.

**c)** Tous les travaux menés par l'UIT dans le cadre du Programme GCA devraient être guidés par une évaluation claire des besoins et des objectifs de ses membres, au moyen d'outils tels que le GCI, des résultats requis pour y répondre et conformément à des mesures et des paramètres appropriés conçus spécialement à cette fin.

**d)** L'UIT devrait continuer de suivre l'évolution et l'utilisation des TIC nouvelles et émergentes pour guider les États Membres et les parties prenantes sur les aspects de sécurité de ces technologies, dans les domaines relevant de son mandat, et, le cas échéant, sur leur application potentielle pour contrer les cybermenaces.

**e)** Étant donné les incidences intrinsèquement transnationales et intersectorielles de la cybersécurité, l'UIT devrait promouvoir des activités, des initiatives et des projets qui peuvent aider les États Membres à favoriser une approche faisant intervenir toutes les entités publiques pour s'attaquer à ce problème.

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

1. Procès-verbal de la dix-septième séance plénière de la Conférence de plénipotentiaires, Dubaï, jeudi 15 novembre 2018, disponible à l'adresse <https://www.itu.int/md/S18-PP-C-0174/en>. [↑](#footnote-ref-1)
2. Soumission du rapport de l'ancien Président du groupe d'experts de haut niveau sur le Programme GCA (C19/58), UIT, 8 mai 2019, disponible à l'adresse <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, disponible à l'adresse <https://www.itu.int/md/S19-CL-C-0117/en>. [↑](#footnote-ref-3)