|  |  |
| --- | --- |
| **Conseil 2021 Consultation virtuelle des Conseillers, 8-18 juin 2021** |  |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.4** | **Document C21/71-F** |
| **22 avril 2021** |
| **Original: anglais** |
| Rapport du Secrétaire général | |
| lignes directrices relatives à l'utilisation  du Programme mondial cybersécurité | |

|  |
| --- |
| Résumé  À 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/fr) et [C19/58](https://www.itu.int/md/S19-CL-C-0058/fr)).  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, est soumis pour examen et approbation par le Conseil. Il importe de noter que cette initiative n'a pas vocation à traiter les questions liées à la révision du Programme GCA.  Conformément au processus d'élaboration du projet de lignes directrices énoncé dans la Lettre circulaire ([CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/en)), deux consultations ouvertes ont eu lieu 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. Une version précédente de ce document avait été élaborée initialement sous la cote C20/65, en vue d'être soumise à la session de 2020 du Conseil, mais n'a pas été examinée.  Suite à donner  Le 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)*,* [*Document C21/36*](https://www.itu.int/md/S21-CL-C-0036/en) |

Table des matières

Page

[**Section 1 Introduction 3**](#_Toc41368783)

[Rappel 4](#_Toc41368784)

[Contexte 5](#_Toc41368785)

[Le Programme GCA: un cadre d'action mondial qui reste pertinent et applicable 8](#_Toc41368786)

[**Section 2 Pilier 1: Mesures juridiques 9**](#_Toc41368787)

[Introduction 9](#_Toc41368788)

[Évolution du contexte juridique depuis 2008 9](#_Toc41368789)

[Lignes directrices pour l'utilisation du Pilier 1 – Mesures juridiques 13](#_Toc41368797)

[**Section 3 Pilier 2: Mesures techniques et de procédure 14**](#_Toc41368798)

[Introduction 14](#_Toc41368799)

[Évolution de l'environnement des mesures techniques et de procédure depuis 2008 14](#_Toc41368800)

[Lignes directrices pour l'utilisation du Pilier 2 – Mesures techniques et de procédure 16](#_Toc41368802)

[**Section 4 Pilier 3: Structures administratives 17**](#_Toc41368803)

[Introduction 17](#_Toc41368804)

[Évolution de l'environnement des structures administratives depuis 2008 17](#_Toc41368805)

[Lignes directrices pour l'utilisation du Pilier 3 – Structures administratives 19](#_Toc41368806)

[**Section 5 Pilier 4: Renforcement des capacités 20**](#_Toc41368807)

[Introduction 20](#_Toc41368808)

[Évolution de l'environnement du renforcement des capacités depuis 2008 20](#_Toc41368809)

[Lignes directrices pour l'utilisation du Pilier 4 – Renforcement des capacités 21](#_Toc41368810)

[**Section 6 Pilier 5: Coopération internationale 23**](#_Toc41368811)

[Introduction 23](#_Toc41368812)

[Évolution de l'environnement de la coopération internationale 2008 23](#_Toc41368813)

[Lignes directrices pour l'utilisation du Pilier 5 – Coopération internationale 26](#_Toc41368815)

[**Section 7 Lignes directrices générales pour le cadre du Programme GCA 27**](#_Toc41368816)

# 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). 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, un projet de lignes directrices relatives à l'utilisation du Programme GCA par l'UIT, 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[[4]](#footnote-4). 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.

**1.5** Conformément au processus d'élaboration du projet de lignes directrices énoncé dans la Lettre circulaire [(CL-20/55)](https://www.itu.int/md/S20-SG-CIR-0055/en), deux consultations ouvertes ont eu lieu 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. 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.

Rappel

**1.6** Une mission fondamentale de l'UIT, fondée sur les orientations du Sommet mondial sur la société de l'information (SMSI) et de la Conférence de plénipotentiaires de l'UIT, consiste à renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC).

**1.7** Lors du SMSI en 2005, 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"[[5]](#footnote-5). Pour s'acquitter de cette mission, l'UIT a lancé le GCA en 2007, cadre de coopération internationale dans ce domaine.

**1.8** Le GCA est composé de cinq Piliers ou domaines d'activité: mesures juridiques, mesures techniques et de procédure, structures organisationnelles, renforcement des capacités et coopération internationale. Il est conçu pour favoriser la coopération multi-parties prenantes et l'efficacité, en encourageant la collaboration avec et entre toutes les parties prenantes concernées et en tirant parti des initiatives existantes pour éviter tout chevauchement d'activité.

**1.9** 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).

**1.10** 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[[6]](#footnote-6) (Rapport HLEG 2008). Dans le Rapport, le Président du groupe HLEG a souligné ce qui suit:

*Les coûts associés aux cyberattaques sont considérables – en termes de manque à gagner, de pertes de données sensibles, de dégâts causés aux équipements, d'attaques par déni de service et d'interruptions de réseau. Le développement futur et les possibilités associées à la société de l'information en ligne sont remis en cause par la multiplication des cybermenaces. De plus, le cyberespace ne connaît pas de frontières: en quelques minutes seulement, les cyberattaques peuvent causer des dégâts inimaginables dans plusieurs pays. Les cybermenaces sont un problème mondial et nécessitent une réponse mondiale faisant intervenir toutes les parties prenantes.*

**1.11** En 2008, les travaux sur les cinq 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 groupe 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.

Contexte

**1.12** 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. Il 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. Les recommandations associées figurant dans le Rapport du groupe HLEG de 2008 restent d'actualité aujourd'hui[[7]](#footnote-7), sauf pour quelques éléments particuliers qui sont obsolètes ou ont été remplacés à l'occasion d'autres manifestations.

**1.13** Bien sûr, le paysage des TIC a subi de profonds changements depuis 2008, les TIC étant aujourd'hui la base de chaque secteur de la société et de la plus grande partie des infrastructures essentielles[[8]](#footnote-8). Le monde assiste à l'émergence et à l'adoption de nouvelles technologies à un rythme soutenu, avec par exemple:

• la généralisation de l'adoption de l'Internet des objets qui rassemble des dizaines, si ce n'est des centaines, de milliards de nouveaux dispositifs interconnectés, ce qui est aussi à l'origine d'un nombre considérable de nouvelles vulnérabilités potentielles;

• l'essor de l'intelligence artificielle en tant qu'outil pour exploiter les données, en particulier les mégadonnées, qui permet à l'homme de prendre des décisions plus éclairées et permet aux machines de prendre de manière autonome et sans intervention humaine des décisions dites intelligentes, tout en allant de pair avec des défis concernant la confiance et la sécurité ainsi que la sauvegarde des droits de l'homme;

• les nouvelles technologies et normes de communication, comme la 5G, qui permettent d'accroître de manière exponentielle le débit des communications par rapport à celui que nous connaissons aujourd'hui;

• l'informatique quantique qui offre des vitesses de calcul bien supérieures aux capacités actuelles, ouvrant de nouveaux horizons incroyables mais rendant par ailleurs vulnérables, entre autres, les algorithmes cryptographiques actuels; et

• les nouvelles technologies de sécurité, comme les technologies de registres distribués (dont la "blockchain" est l'une des mises en œuvre les plus utilisées), qui offrent des solutions bien plus efficaces pour préserver les systèmes et les données associées. Un nombre croissant de pays partout dans le monde s'orientent aussi de plus en plus vers l'adoption de systèmes d'identités numériques.

**1.14** En outre, l'adoption à grande échelle, partout dans le monde, des réseaux sociaux, a largement contribué à façonner l'écosystème mondial des TIC depuis 2008. Les utilisateurs que rassemblent certains réseaux sociaux sont parfois plus nombreux que les habitants de plusieurs pays réunis – c'est par exemple le cas avec Facebook, qui comptait en 2020 près de 2,8 milliards d'utilisateurs actifs par mois[[9]](#footnote-9). Les réseaux sociaux jouent un rôle essentiel pour connecter les personnes partout dans le monde, gommant les frontières géographiques et permettant d'accéder facilement, à une vitesse et à des échelles sans précédent, à l'information et aux possibilités offertes. Ils sont également à l'origine de graves préoccupations en matière de confiance – concernant la vie privée et la sécurité des utilisateurs et des données qu'ils génèrent, l'authenticité et la fiabilité des informations disponibles sur les réseaux sociaux, la diffusion de contenus haineux, etc.[[10]](#footnote-10)

**1.15** De plus, d'autres facteurs, comme l'apparition du "dark web", continuent de susciter des préoccupations croissantes dans le monde entier concernant les activités criminelles dans le cyberespace, notamment sur des aspects comme l'accès à des outils, services et contenus malveillants.

**1.16** Compte tenu de cette évolution, toutes les parties prenantes, y compris les pouvoirs publics, reconnaissent de plus en plus la diversité des mesures urgentes à prendre pour faire progresser la cybersécurité, qui vont de la protection des infrastructures critiques à la sauvegarde de la vie privée des utilisateurs. La cybersécurité, qui pourrait constituer une menace pour la sécurité nationale de tous les pays, est une priorité au plus haut niveau politique des gouvernements, qui investissent toujours plus dans des mesures de gouvernance et d'administration pour susciter une réponse faisant intervenir toutes les entités publiques dans le but de renforcer leur cyberrésilience nationale.

**1.17** La pandémie de COVID-19 n'a fait que souligner encore le caractère essentiel des TIC pour la santé et la sécurité et pour que notre économie et notre société continuent d'aller de l'avant. Du télétravail et du commerce électronique à la télémédecine et à l'apprentissage à distance, les services et les infrastructures des TIC permettent de répondre en permanence à des besoins

essentiels. La crise liée au COVID-19 a également accentué la nécessité de traiter les problèmes critiques et en évolution rapide de la cybersécurité que pose le degré élevé de dépendance de la société à l'égard des TIC.

**1.18** Dans le cadre du GCA, chacun des cinq Piliers a évolué de façon autonome depuis une dizaine d'années.

**1.19** En 2020, plus de 125 pays ont signé et/ou ratifié des conventions, déclarations, lignes directrices ou accords divers sur la cybersécurité et la cybercriminalité comme la [Convention du Conseil de l'Europe sur la cybercriminalité de 2001](https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185) (Convention de Budapest), l'[Accord entre les gouvernements des États membres de l'Organisation de Shanghai pour la coopération, qui porte sur la coopération destinée à garantir la sécurité de l'information au niveau international](http://eng.sectsco.org/documents/) (2009) et la [Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles](https://au.int/fr/node/29560) (2014).

**1.20** Conformément aux Résolutions de l'Assemblée générale des Nations Unies, un Groupe d'experts gouvernementaux (GGE)[[11]](#footnote-11) et un Groupe de travail à composition non limitée (OEWG)[[12]](#footnote-12) ont étudié plusieurs questions liées à l'utilisation des TIC dans le contexte de la sécurité internationale, notamment les mesures propres à promouvoir la conduite responsable des États dans le cyberespace, l'applicabilité du droit international au cyberespace, le renforcement des capacités et la nécessité de mettre en œuvre et d'intensifier les mesures visant à instaurer la confiance dans le cyberespace.

**1.21** Les technologies TIC innovantes, comme l'informatique en nuage, les réseaux pilotés par logiciel (SDN), la virtualisation des fonctions de réseau (NFV), la 5G, les mégadonnées, l'IA, etc., effacent les frontières du marché et les frontières géographiques, rendant l'écosystème de la cybersécurité de plus en plus dynamique et complexe. Les nouvelles technologies et les nouveaux acteurs commerciaux peuvent entraîner une exposition à de nouvelles vulnérabilités et menaces, d'autant plus que la priorité donnée par le secteur privé aux performances, aux parts de marché et aux coûts est souvent privilégiée par rapport aux investissements dans la sécurité au stade de la conception. Un certain nombre de questions posent des défis majeurs face à ces technologies, comme trouver un moyen de réduire et de maîtriser le nombre de vulnérabilités en assurant la sécurité dès la conception (car des produits restent encore vulnérables dès leur phase de conception elle-même), renforcer la confiance dans les produits et les services tout au long de leur cycle de vie par des mécanismes, des protocoles et des normes d'accréditation et assurer l'utilisation légitime des données produites par l'utilisateur tout en protégeant la vie privée de ce dernier. La normalisation et des processus de certification/accréditation périodiques pourraient aider à réduire le nombre et les incidences des vulnérabilités en contribuant à créer une culture de la sécurité dès la conception, ce qui permettrait de renforcer la confiance dans ces technologies. Toutefois, la normalisation de la sécurité, c'est-à-dire l'élaboration de mesures techniques et de procédure pour la sécurité, reste une cible mouvante car elle nécessite un secteur d'activité à la pointe de la technologie, des autorités de réglementation spécialistes de la technologie et, le cas échéant, des organismes de contrôle.

**1.22** Un certain nombre d'organisations nationales, régionales et internationales ont été mises en place pour s'attaquer au problème de la cybersécurité. Parmi les exemples d'initiatives nationales et régionales, citons AFRIPOL, AMERIPOL, GCCPOL, le Centre océanien de cybersécurité (OCSC), le Centre australien de cybersécurité (ACSC), le Centre européen de lutte contre la cybercriminalité (EC3), le Centre de coordination national russe sur les incidents informatiques et le Centre de coordination indien sur la cybercriminalité (I4C). En ce qui concerne les entités internationales, les efforts récents comprennent le Centre mondial de capacité en matière de cybersécurité (GCSCC), le Forum mondial sur la cyberexpertise (GFCE), le Complexe mondial INTERPOL pour l'innovation (IGCI), le Centre mondial pour la cybersécurité du WEF, le Programme cybersécurité du Comité interaméricain contre le terrorisme (CICTE) de l'Organisation des États américains (OEA), la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), la Communauté de développement de l'Afrique australe (SADC), pour ne citer que ces initiatives.

**1.23** En outre, le manque de compétences et de connaissances pour ce qui est des aspects techniques, juridiques, administratifs et humains de la cybersécurité peut également nuire aux infrastructures nationales vitales. Il est probable qu'actuellement, de nombreux utilisateurs finals des TIC ne comprennent pas pleinement les questions de cybersécurité ou ne disposent pas des compétences ou des outils nécessaires pour protéger au mieux leurs données, leur vie privée et leurs biens, les utilisateurs les plus vulnérables, notamment les femmes et les enfants, étant particulièrement exposés. Le renforcement des aptitudes, des compétences et des mesures qui contribueront à l'instauration d'une culture de la cybersécurité efficace reste un enjeu fondamental.

Le Programme GCA: un cadre d'action mondial qui reste pertinent et applicable

**1.24** Les activités mises en œuvre dans le cadre du Programme GCA, y compris celles menées par l'UIT au titre de sa mission et de son rôle en tant que coordonnateur pour la grande orientation C5 du SMSI, évoluent, tout comme l'environnement des TIC.

**1.25** Le Programme GCA est très utile pour l'action menée par l'UIT en vue d'instaurer la confiance et la sécurité dans l'utilisation des TIC. En tant que cadre, il s'applique aux niveaux mondial, régional et national et devrait continuer d'être mis en œuvre de cette façon. Au titre de son mandat, s'appuyant sur le cadre du Programme GCA, l'UIT travaille afin d'amener des parties prenantes différentes à collaborer sur un certain nombre d'initiatives, y compris pour aider les États Membres à définir leur stratégie nationale en matière de cybersécurité, à renforcer leur infrastructure en élaborant et en appliquant des normes internationales de sécurité, à créer des équipes d'intervention en cas d'incident informatique, à mettre en place des initiatives visant à protéger les enfants en ligne et à renforcer les capacités humaines et les compétences nécessaires. Différentes initiatives multi-parties prenantes comme celle pour la protection en ligne des enfants ont été lancées dans le cadre du Programme GCA[[13]](#footnote-13).

**1.26** Afin de renforcer les efforts en vue de l'utilisation du Programme GCA, des orientations supplémentaires sont proposées dans les sections suivantes. Pour élaborer ces orientations, 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/md/S20-GCA-C/en) 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)).

**1.27** 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

Introduction

**2.1** La dimension juridique de la cybersécurité est l'un des principaux facteurs propres à favoriser la confiance dans l'utilisation des TIC.

**2.2** Le Rapport du groupe HLEG de 2008 indiquait que le premier Pilier du Programme GCA visait à promouvoir la coopération et à fournir des conseils stratégiques au Secrétaire général de l'UIT sur les réponses législatives à apporter aux questions juridiques en constante évolution dans le domaine de la cybersécurité, notamment sur la manière dont les activités criminelles commises au moyen des TIC pouvaient être traitées par la législation d'une manière compatible au niveau international. Les discussions ont permis de constater que l'UIT pourrait concevoir des stratégies pour l'élaboration d'une législation modèle en matière de cybercriminalité sous forme de lignes directrices. Dans son Rapport, le Groupe HLEG a également recommandé des initiatives régionales pertinentes à titre de référence.

Évolution du contexte juridique depuis 2008

**2.3** Des organisations régionales ont élaboré nombre de conventions, de déclarations, d'accords et de lignes directrices sur la cybersécurité après 2008. Comme indiqué ci-dessus, de nombreux pays ont signé et/ou ratifié diverses conventions, déclarations et lignes directrices ou divers accords sur la cybersécurité et la cybercriminalité, ce qui a, dans une certaine mesure, entraîné une fragmentation et une diversité au niveau international.

**2.4** Dans le cadre du système des Nations Unies, comme indiqué précédemment dans la Section 1, l'Assemblée générale des Nations Unies a également mis en place deux processus pour étudier la question de la sécurité dans l'utilisation des TIC, à savoir le Groupe d'experts gouvernementaux (GGE) et le Groupe de travail à composition non limitée (OEWG). Depuis 2004, l'Assemblée générale des Nations Unies a créé six Groupes d'experts gouvernementaux chargés d'étudier les risques que font peser l'utilisation des TIC dans le contexte de la sécurité internationale et la manière d'y faire face, le dernier en date étant le [Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale](https://www.un.org/disarmament/group-of-governmental-experts/) (2019/2021) ([Résolution 73/266](https://dig.watch/instruments/resolution-ares73266-advancing-responsible-state-behaviour-cyberspace-context-international)). Dans ses conclusions, le Groupe d'experts gouvernementaux (2014/2015) est convenu que les obligations existantes en vertu du droit international sont applicables à l'utilisation des TIC par les États et que ceux-ci doivent se conformer aux obligations qui leur incombent en matière de respect et de protection des droits de l'homme et des libertés fondamentales. En 2018, il a été constitué un [Groupe de travail à composition non limitée (OEWG) pour examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale](https://www.un.org/disarmament/open-ended-working-group/) (Résolution 73/27), associant "tous les États intéressés", pour passer en revue les risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et les mesures de coopération qui pourrait être prises pour y parer; pour poursuivre l'élaboration des règles, normes et principes de comportement responsable des États; pour étudier la manière dont le droit international s'applique à l'utilisation des TIC par les États; pour examiner les mesures de confiance et de renforcement des capacités; et pour étudier la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies. Le Groupe de travail à composition non limitée (2019-2021) a adopté par consensus, en mars 2021, son [rapport final de fond](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf), dans lequel il réaffirme que le droit international, et en particulier la Charte des Nations Unies, est applicable dans le cyberespace et recommande en outre aux États de soutenir les mesures de renforcement des capacités dans le domaine du droit international, de la législation nationale et des politiques, en ce sens que cela permettra à tous les États de contribuer à la définition d'interprétations communes concernant l'application du droit international à l'utilisation des TIC par les États. Le Groupe de travail à composition non limitée devrait poursuivre ses travaux, puisque conformément à la Résolution 75/240, il a été créé un Groupe de travail à composition non limitée sur la sécurité des technologies de l'information et des communications et leur utilisation (2021-2025).

**2.5** Plusieurs initiatives et processus ont également été lancés au sein du système des Nations unies pour contribuer à recenser et résoudre les problèmes juridiques que pose la cybersécurité dans le monde. Ainsi, un certain nombre de Résolutions de l'Assemblée générale des Nations Unies ont été adoptées à cet égard, par exemple la [Résolution en date du 27 décembre 2019 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles (Résolution 74/247)](https://undocs.org/pdf?symbol=fr/A/RES/74/247), par laquelle il a été décidé d'établir un Comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions, ayant pour mission d'élaborer une Convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

**2.6** Compte tenu de ce qui précède, les États participant aux travaux de ces diverses instances étudient actuellement la nécessité de poursuivre leur coopération et de collaborer avec d'autres parties prenantes, afin de trouver un terrain d'entente au niveau mondial sur la compréhension, l'interprétation et le respect du droit international dans le contexte du cyberespace, en particulier en facilitant l'échange accru d'informations et de bonnes pratiques.

Mesures juridiques et nouvelles technologies

**2.7** Pour certains experts, il conviendrait que les nouvelles technologies et les comportements dont l'intention est criminelle dans le cyberespace soient couverts par le droit pénal[[14]](#footnote-14). De nombreux pays ont adopté ou se préparent à adopter de nouvelles législations visant certains de

ces comportements. Il est important que les mesures juridiques pertinentes conçues à cet égard soient conformes aux obligations incombant aux pays en matière de droits de l'homme. Quelques exemples de technologies et de tendances récentes qui pourraient avoir un effet sur les mesures juridiques sont présentés ci-dessous.

a) Cyberattaques mondiales

Les cyberattaques mondiales contre des infrastructures de communication et d'information essentielles constituent une menace qui pèse sur la sécurité aux niveaux international et national. Des gouvernements, des organisations internationales et des institutions privées ont tous été la cible de ces cyberattaques mondiales, qui les ont amenés à mettre en place des cadres juridiques nationaux solides pour faire face à ce problème

b) Comportements criminels sur les réseaux sociaux

Des appels sont lancés pour que des mesures soient prises afin de contrer les comportements illégaux, comme les discours de haine, sur les réseaux sociaux. De nouvelles initiatives ont vu le jour pour traiter de ces questions, comme le partenariat du [Forum Internet mondial de lutte contre le terrorisme](https://www.gifct.org/about/) entre les Nations Unies et les entreprises du secteur des technologies Facebook, Microsoft, Twitter et YouTube.

c) L'Internet des objets (IoT)

Les technologies intelligentes changent la façon dont la population mondiale vit, interagit et travaille[[15]](#footnote-15).Dernièrement, l'infrastructure web à travers le monde a été à maintes reprises la cible d'attaques par un botnet de dispositifs connectés piratés, allant de webcams à des routeurs. L'avènement de nouvelles technologies comme la 5G et l'omniprésence des dispositifs interconnectés étant devenus une réalité, il est probable que les risques augmentent.

d) L'intelligence artificielle (IA)

La transparence algorithmique, y compris la traçabilité des actions entreprises, est un facteur très important pour établir la responsabilité des décisions prises par des systèmes partiellement ou entièrement automatisés, et ainsi garantir la confiance dans les applications et services des TIC. Les experts ont constaté que pour plusieurs types de techniques d'IA, comme l'apprentissage profond, il est difficile de déterminer comment les résultats sont obtenus. À mesure que les

processus décisionnels automatisés se généralisent dans les applications et services destinés aux consommateurs et aux entreprises, la nécessité d'une plus grande clarté sur les aspects juridiques concernant l'obligation de rendre des comptes et la responsabilité pour les analyses et les décisions que ces processus fournissent deviendra de plus en plus importante[[16]](#footnote-16).

e) Abus et exploitation sexuels d'enfants

La [Convention des Nations Unies relative aux droits de l'enfant](https://www.ohchr.org/FR/ProfessionalInterest/Pages/CRC.aspx) (CRC) a été adoptée en 1989. L'article 34 de la Convention oblige les États parties à prendre des mesures appropriées pour protéger les enfants contre toutes les formes d'exploitation et d'abus sexuels. En 2002, un [Protocole facultatif de la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants](https://www.ohchr.org/fr/ProfessionalInterest/Pages/OPSCCRC.aspx) est entré en vigueur. Les contenus en ligne à caractère pédopornographique se sont répandus avec la croissance de l'Internet et des réseaux sociaux. Des experts ont préconisé une approche globale pour la prévention de ces abus[[17]](#footnote-17). Il s'agit notamment de mesures visant à empêcher le développement et l'accès aux sites web qui comportent des contenus à caractère pédopornographique, y compris le blocage, le filtrage ou toute autre technologie similaire. En mars 2021, le Comité des droits de l'enfant a adopté son [observation générale N° 25 (2021) sur les droits de l'enfant dans le contexte de l'environnement numérique](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en), qui explique comment les États parties doivent mettre en œuvre la Convention relative aux droits de l'enfant dans l'environnement numérique et fournit des orientations sur les mesures législatives et politiques, notamment, qui s'imposent.

**2.8 Droit procédural – Principes généraux**

L'adoption du droit procédural nécessaire pour établir les pouvoirs et les procédures de poursuite des comportements criminels dans le cyberespace a été considérée comme une mesure juridique essentielle pour la prévention, les enquêtes et les poursuites au niveau mondial en matière de cybercriminalité et pour garantir la cybersécurité. Toutefois, certains experts ont noté que ces pouvoirs et procédures pourraient également être nécessaires pour la poursuite d'autres infractions pénales commises au moyen d'un système informatique, et que des règlements pourraient s'appliquer à la collecte de preuves sous forme électronique de toutes les infractions pénales[[18]](#footnote-18). L'ensemble du droit procédural devrait être conforme aux obligations et aux normes du droit international des droits de l'homme. À cet égard, sachant que le principe de la souveraineté des États s'applique dans le cyberespace, des demandes ont été formulées et des discussions ont également eu lieu sur l'étude des mécanismes susceptibles de faciliter l'accès légal au contenu des communications lorsque le chiffrement de bout en bout a été mis en œuvre, tout en garantissant la protection des droits fondamentaux et de la sécurité des citoyens[[19]](#footnote-19).Certaines parties prenantes ont attiré l'attention sur le fait que ces mécanismes risquaient d'affaiblir la sécurité de l'Internet et d'exposer à des risques accrus l'économie mondiale, les services essentiels – dont beaucoup dépendent – et la vie des personnes.

**2.9** À la lumière de ces considérations, il est évident que les pays devraient continuer de prendre les mesures juridiques qui conviennent pour protéger leurs infrastructures essentielles de communication et d'information (et tout actif, système ou partie de celui-ci) qui sont indispensables au maintien de fonctions vitales de la société comme la santé, la sûreté, la sécurité, le bien-être économique ou social des personnes, et pour prévenir toute perturbation ou destruction susceptible d'avoir des incidences importantes sur ces infrastructures essentielles et d'entraîner leur dysfonctionnement.

Lignes directrices pour l'utilisation du Pilier 1 – Mesures juridiques

**2.10** Comme nous l'avons indiqué précédemment, les cinq Piliers du Programme GCA sont tous interdépendants, celui des mesures juridiques les recouvrant tous.

**2.11** Depuis le lancement du Programme GCA, l'UIT s'est consacrée essentiellement aux domaines de la cybersécurité qui correspondent à son mandat de base et à ses connaissances spécialisées, notamment le domaine technique et celui du développement, à l'exclusion de ceux qui concernent l'application par les États Membres de principes juridiques ou politiques se rapportant à la défense et la sécurité nationales, à la cybercriminalité et aux contenus, qui relèvent de leurs droits souverains. En conséquence, concernant les activités au titre du Pilier 1, l'UIT s'est principalement attachée à faciliter la collaboration, au moyen de mécanismes comme des protocoles d'accord, avec d'autres organisations internationales et parties prenantes (comme INTERPOL et l'ONUDC) qui peuvent avoir un mandat principal dans ce domaine pour fournir une assistance aux pays. Il s'agit notamment 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 et le recueil sur la cybercriminalité de l'ONUDC](http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html). Des travaux ont aussi été menés pour aider les États Membres des Caraïbes, de l'Afrique subsaharienne et des îles du Pacifique à harmoniser les réglementations et les législations en matière de TIC, y compris les cadres juridiques relatifs à la cybercriminalité.

|  |
| --- |
| **2.12** 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 sont présentées ci-dessous:  **a)** L'UIT devrait poursuivre ses efforts pour faciliter les discussions et la collaboration multipartites sur les difficultés liées au traitement de la question de la cybersécurité et, en particulier, renforcer ses relations avec les partenaires et autres parties prenantes pour fournir une assistance aux États Membres à cet égard.  **b)** L'UIT devrait continuer de collaborer avec des partenaires, dans le cadre de son mandat, pour élaborer et tenir à jour des ressources, comme les ressources sur la législation relative à la cybercriminalité, pour aider les États Membres à mieux cerner les aspects juridiques de la cybersécurité, 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, notamment en matière de législation.  **c)** L'UIT, en collaboration avec des partenaires appropriés, devrait favoriser une meilleure compréhension des difficultés et des risques liés à la cybersécurité que présentent les technologies émergentes pour les mesures juridiques existantes et faciliter l'échange d'études de cas et de bonnes pratiques aux niveaux national, régional et international. |
| **d)** Toutes les parties prenantes concernées doivent également prendre des mesures juridiques appropriées pour mettre en œuvre des programmes efficaces visant à prévenir ou à interdire la diffusion de matériel en ligne concernant la violence sexuelle visant des enfants et l'exploitation sexuelle des enfants, notamment en prenant des mesures préventives pour détecter, désorganiser et démanteler les réseaux, organisations ou structures utilisés pour la production et/ou la diffusion de matériel en ligne concernant la violence sexuelle visant des enfants et l'exploitation sexuelle des enfants, et pour mettre en place des mécanismes permettant de détecter et de poursuivre les auteurs d'infractions tout en identifiant et en protégeant les victimes. À cet égard, 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, d'activités et de résultats sur tous les aspects, y compris les mesures juridiques qui peuvent faciliter et soutenir l'action des pays sur cette question essentielle. | |

# Section 3 Pilier 2: Mesures techniques et de procédure

Introduction

**3.1** Le Programme GCA a guidé l'élaboration et la mise en œuvre de diverses initiatives, contribuant ainsi à la maturité du débat sur la cybersécurité aux niveaux international, régional et national. Une difficulté de taille reste de répondre d'une façon cohérente au besoin de mesures de cybersécurité efficaces et efficientes, que ce soit au niveau stratégique ou opérationnel.

**3.2** Aujourd'hui, il peut sembler que les dimensions identifiées par les Piliers 1, 3, 4 et 5 du Programme GCA prennent de plus en plus d'importance dans le domaine de la cyberdiplomatie et du dialogue international, et l'emportent souvent sur le Pilier 2. Cependant, les questions techniques peuvent souvent être à l'origine de tous les autres Piliers. La gestion des cyberrisques à l'aide de mesures technologiques et de procédure (par exemple les mesures d'ordre administratif et opérationnel ou de gestion) reste d'une importance primordiale, notamment dans le contexte des infrastructures essentielles. Compte tenu du rôle qu'elle joue depuis longtemps, en tant qu'institution spécialisée des Nations Unies et organisation mondiale de normalisation, l'UIT est bien placée pour faire progresser le domaine des normes et des mesures techniques liées à la sécurité.

Évolution de l'environnement des mesures techniques et de procédure depuis 2008

**3.3** Les technologies (actuelles et émergentes) et les pratiques numériques qui en découlent sont en constante évolution. Cette dimension technique dynamique est quelque peu indépendante des autres Piliers du Programme GCA et évolue largement de façon autonome, en tenant compte de manière limitée des besoins et des incidences sur le sujet des quatre autres Piliers.

**3.4** Pour que toutes les infrastructures, applications et services fonctionnent, il est fondamental d'élaborer et de mettre en œuvre des normes. En outre, il est important que, lors de l'élaboration des normes, les obligations pertinentes en matière de droits de l'homme soient également prises en considération.

**3.5** L'UIT, qui compte diverses parties prenantes parmi ses membres, offre une tribune mondiale unique en son genre permettant d'élaborer des normes mondiales relatives aux TIC, que les États membres de l'UIT peuvent adopter sur une base volontaire. Au sein de l'UIT, la CE 17 de l'UIT-T est la principale Commission d'études chargée de l'examen des normes de sécurité − puisqu'elle a publié plus de 200 normes axées sur la sécurité. Elle étudie actuellement divers domaines technologiques émergents, notamment la sécurité des technologies financières, la sécurité de l'IoT (y compris la sécurité de l'Internet industriel), la sécurité des systèmes de transport intelligents, la technologie des registres distribués, la distribution de clés quantiques, l'apprentissage machine pour lutter contre le spam, la sécurité de la 5G, l'informatique en périphérie, la protection des informations d'identification personnelle, l'informatique multipartite et les lignes directrices pour la création, l'exploitation et l'automatisation des centres de cyberdéfense, entre autres. En mettant en œuvre les recommandations du Rapport du Groupe HLEG de 2008 sur la "collaboration" (par exemple les recommandations 2.1, 2.6, 2.7, 2.10, 2.12, 2.16), la CE 17 recueille et tient à jour une base de données des normes de sécurité des TIC[[20]](#footnote-20) accessible au public, qui comprend 2 600 normes de sécurité existantes et en cours d'élaboration émanant de 13 organisations de normalisation de premier plan, dont le 3GPP, ATIS, l'ETSI, l'IEEE, l'IETF, l'ISO/CEI JTC 1, l'UIT, OASIS, OneM2M, etc.

**3.6** Si la CE 17 de l'UIT-T reste la principale Commission d'études pour les normes de sécurité, la plupart – sinon toutes – des autres commissions d'études traitent également des aspects liés à la sécurité dans leurs domaines d'étude respectifs, par exemple la CE 20 sur l'IoT et ses applications (y compris les villes et communautés intelligentes), la CE 13 sur les réseaux de prochaine génération ou la CE 16 sur le codage, les systèmes et les applications multimédias, entre autres. Les différents groupes spécialisés sur les technologies émergentes, comme l'IA et la santé, l'apprentissage machine et la 5G, les technologies des registres numériques, les technologies de l'information quantique pour les réseaux, notamment, abordent aussi les problèmes de sécurité. Il importe d'instaurer 'une coopération étroite entre les différents groupes, la CE 17 jouant un rôle de coordination ou de direction, pour que le plus haut degré possible de sécurité de bout en bout soit maintenu tout au long du processus de normalisation du cycle de mise au point des produits et services liés aux TIC.

Multiplication des initiatives de normalisation et nécessité d'une coopération accrue

**3.7** La normalisation au niveau international concernant la cybersécurité est difficile en raison de la diversité des technologies et de l'arrivée d'acteurs divers issus de tous les secteurs, et est particulièrement ardue pour les pays en développement, qui manquent parfois des capacités opérationnelles et des compétences techniques nécessaires en matière de cybersécurité.

**3.8** A cet égard, la Recommandation 2.1 du Rapport du groupe HLEG de 2008 reste plus que jamais d'actualité: "En ce qui concerne les possibilités de renforcer la collaboration avec les travaux existants en matière de cybersécurité en dehors de l'UIT, l'UIT devrait travailler avec les centres de compétence externes existants pour identifier, soutenir et encourager l'adoption de procédures et de mesures techniques de sécurité renforcées"[[21]](#footnote-21).

**3.9** De plus, comme précisé dans la Recommandation 2.2 du Rapport du groupe HLEG de 2008, l'UIT est désignée comme étant "le centre d'excellence mondial"[[22]](#footnote-22) pour s'occuper du processus de normalisation internationale et des normes relatives aux mesures techniques et de procédure. Pour y parvenir, les pays technologiquement les plus avancés et leur secteur privé devraient être encouragés à participer aux activités de l'UIT et à collaborer à l'élaboration de normes techniques et de procédure, y compris celles liées à la sécurité.

**3.10** Il est essentiel de continuer à renforcer la coordination et la collaboration avec les autres organisations de normalisation, sur une base de réciprocité, afin d'assurer la sécurité de bout en bout, la sécurité dès la conception, l'évaluation des risques et l'interopérabilité tout au long du cycle de vie du produit.

**3.11** Le Rapport du groupe HLEG de 2008 a souligné l'importance des "principales mesures permettant de remédier aux vulnérabilités des produits logiciels (systèmes, protocoles et normes d'accréditation)"[[23]](#footnote-23). À cet égard, l'UIT devrait continuer à adapter ses travaux, en tenant compte des nouvelles technologies et exigences. Pour chacune de ces technologies ou chacun de ces domaines, les exigences suivantes devraient être prises en considération:

• nécessité de la sécurité dès la conception ou de la sécurité par défaut dans chaque élément et chaque interface dans un écosystème des TIC hétérogène au stade de la conception;

• nécessité de paramètres appropriés pour déceler le niveau de sécurité au moment de la mise en œuvre; et

• nécessité de processus d'évaluation et de certification périodiques pour certifier le niveau de sécurité d'un ensemble de données/produit/système/service tout au long de son cycle de vie après déploiement.

Lignes directrices pour l'utilisation du Pilier 2 – Mesures techniques et de procédure

|  |
| --- |
| **3.12** Toutes les recommandations relatives au Pilier 2 figurant dans le Rapport du groupe HLEG de 2008 restent valables. Compte tenu de ce qui précède, 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, afin d'étudier et de formuler des lignes directrices en matière de sécurité pour l'utilisation de technologies connexes, et recommander aux États Membres d'adopter ces lignes directrices à titre volontaire et en temps utile, afin de faire face à l'évolution et à la progression des cybermenaces.  **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 sécurité, 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. Les autres organisations de normalisation et les groupes du secteur privé sont encouragés à soumettre leurs normes sur les mesures techniques et de procédure à l'UIT-T pour adoption en tant que Recommandations de l'UIT-T.  **e)** L'UIT devrait poursuivre ses efforts en vue de devenir "le centre mondial d'excellence" pour l'élaboration de Recommandations sur les mesures techniques et de procédure en matière de cybersécurité dans les domaines relevant de son mandat (comme indiqué dans le Rapport du groupe HLEG de 2008), notamment en incitant ses membres à renforcer leur participation aux activités de normalisation connexes de l'UIT et en établissant des partenariats stratégiques.  **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 systèmes de certification internationaux à l'échelle mondiale en matière de cybersécurité, sur la base de normes harmonisées. |

# Section 4 Pilier 3: Structures administratives

Introduction

**4.1** Les structures administratives au niveau de la coordination nationale, régionale et internationale peuvent être analysées selon que l'objectif de leur coopération est stratégique ou opérationnel. Dans une structure stratégique, les organisations mettent davantage l'accent sur l'établissement d'une relation de collaboration que sur la réalisation d'opérations conjointes en cas de cyberincident. En revanche, dans une structure opérationnelle, les organisations forment des systèmes de partage de renseignements efficaces pour échanger rapidement des informations afin de réagir rapidement aux cyberincidents. Cette distinction peut être utile pour comparer les différentes structures administratives dans le monde.

**4.2** Il faut mettre en place des mécanismes et des structures institutionnelles efficaces au niveau national pour se préparer et faire face en toute fiabilité aux cybermenaces et aux cyberincidents. L'absence de telles institutions et le manque de capacités nationales posent des problèmes pour répondre de manière adéquate et efficace aux cyberattaques. Les équipes nationales d'intervention en cas d'incident informatique (CIRT) jouent un rôle essentiel dans l'amélioration de l'état de préparation et de la résilience au niveau national.

Évolution de l'environnement des structures administratives depuis 2008

**4.3** Des progrès considérables ont été accomplis au cours de la dernière décennie en ce qui concerne le Pilier 3. De nombreuses organisations nationales, régionales et internationales ont été mises en place pour s'attaquer au problème de la cybersécurité.

**4.4** Parmi les exemples d'initiatives nationales et régionales, citons AFRIPOL, AMERIPOL, GCCPOL, le Centre de cybersécurité d'Océanie (OCSC), le Centre de cybersécurité australien (ACSC), le Centre européen de lutte contre la cybercriminalité (EC3), le Centre de coordination sur la cybercriminalité de l'Inde (I4C) et le portail de signalement de la cybercriminalité, Le Centre national de préparation aux incidents et de stratégie pour la cybersécurité et le Centre de lutte contre la cybercriminalité du Japon (JC3), l'Agence nationale de cybersécurité de Malaisie (NACSA), l'Agence nationale de la sécurité des systèmes d'information de France (ANSSI), le Centre national de cybersécurité de Lituanie (NCSC), le Centre national pour la cybersécurité de Suisse, le Centre national de cybersécurité du Royaume-Uni (NCSC), la Cellule de coordination internationale de la cybercriminalité des États-Unis (IC4), le Centre national de coordination des incidents informatiques de Russie, ainsi que le Centre consultatif de coordination des interventions en cas d'incident informatique de l'Organisation du traité de sécurité collective (CCC CSTO), le Comité interaméricain contre le terrorisme (CICTE) et le Programme de cybersécurité de l'OEA, l'Autorité nationale de cybersécurité (NCA) d'Arabie saoudite et l'Autorité nationale du Rwanda en matière de cybersécurité.

**4.5** Malgré l'investissement croissant des États Membres dans les équipes CIRT et le rayonnement régional et international indépendant de ces équipes nationales, 85 pays n'ont toujours pas d'équipe CIRT nationale − une situation très préoccupante compte tenu de la nature mondiale des cybermenaces[[24]](#footnote-24).

**4.6** L'UIT, par l'intermédiaire de son Bureau de développement, travaille avec les États Membres, des partenaires et des organisations régionales ou internationales pour renforcer les capacités aux niveaux national et régional, déployer des moyens et aider à la création et au renforcement d'équipes CIRT nationales. À ce jour, plus de 80 évaluations de l'état de préparation des équipes CIRT ont été menées par l'UIT pour aider les pays à évaluer leur état de préparation national en matière de cybersécurité et leurs capacités d'intervention en cas d'incident[[25]](#footnote-25). L'UIT a apporté son aide à la création ou au renforcement de 22 projets CIRT nationaux pour les États Membres concernés[[26]](#footnote-26). Pour procéder à ces évaluations des pays, l'UIT collabore avec des partenaires comme le Forum pour les des équipes d'intervention et de sécurité en cas d'incident (FIRST) et le Centre mondial des capacités de cybersécurité, entre autres.

**4.7** En ce qui concerne les organisations internationales, plusieurs initiatives ont été prises, dont voici quelques exemples:

• Le [Centre mondial des capacités de cybersécurité](https://www.oxfordmartin.ox.ac.uk/cyber-security/) (GCSCC) est un centre international de recherche sur le renforcement efficace et effectif des capacités en matière de cybersécurité, et a collaboré avec l'UIT à l'élaboration du [Guide d'élaboration d'une stratégie nationale en matière de cybersécurité](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx) (NCS), qui est actuellement utilisé pour fournir des exercices pratiques sur ces stratégies, ainsi qu'une formation sur les bonnes pratiques pour les pays sur l'élaboration d'un cadre efficace de stratégie nationale en matière de cybersécurité.

• Le [Forum mondial sur la cyberexpertise](https://thegfce.org/) (GFCE), créé en 2015, a pour objectif d'échanger les bonnes pratiques et de fournir des compétences spécialisées sur le renforcement des cybercapacités aux pays, aux organisations internationales et au secteur privé. Le GFCE et l'UIT sont les cofondateurs de [l'initiative sur la maturité des équipes CSIRT](https://cybilportal.org/projects/csirt-maturity-initiative-3/) et ont collaboré sur des activités de cybersécurité comme le "[Kit pratique de lutte contre la cybercriminalité](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf)".

• Le [Complexe mondial INTERPOL pour l'innovation](https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2014/Le-Complexe-mondial-INTERPOL-pour-l-innovation-ouvre-ses-portes) (IGCI), inauguré en 2015 à Singapour, fournit aux services nationaux d'application de la législation un soutien opérationnel et une formation spécialisés pour faire face à l'évolution de la criminalité. En 2018, l'UIT et INTERPOL ont signé un accord de coopération visant à établir un cadre officiel pour que ces deux organisations coopèrent dans leur intérêt mutuel et dans le cadre de leurs mandats et ressources respectifs afin d'instaurer la confiance et la sécurité dans l'utilisation des TIC.

• Le WEF a lancé un nouveau [Centre mondial pour la cybersécurité](https://www.weforum.org/centre-for-cybersecurity/) en 2018 dans le but d'établir une plate-forme mondiale pour les gouvernements, les entreprises, les experts et les organismes d'application de la loi afin de collaborer sur les défis de la cybersécurité. La même année, l'UIT et le WEF sont convenus de coopérer à la promotion de projets et d'initiatives de cybersécurité visant à atténuer les cybermenaces et d'explorer d'autres possibilités de coopération pour soutenir la cybersécurité.

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

|  |
| --- |
| **4.8** 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 à mettre en place des équipes CIRT nationales et d'autres unités/organisations techniques connexes.  **b)** L'UIT devrait donner la priorité aux pays où des structures administratives appropriées en matière de cybersécurité n'ont pas encore été mises en place.  **c)** L'UIT devrait encourager une collaboration plus ouverte et inclusive ainsi que la coordination entre les diverses organisations nationales, régionales ou internationales participant à la mise en place de structures administratives nationales durables pour assurer un soutien efficace et éviter tout chevauchement d'activité.  **d)** 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, pour promouvoir la cybersécurité en tant que catalyseur intersectoriel des efforts qu'ils déploient en faveur de la transformation numérique.  **e)** Pour les structures nationales en particulier, l'UIT devrait aider les États Membres à élaborer des stratégies pour mettre en place 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.  **f)** 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 Pilier 4: Renforcement des capacités

Introduction

**5.1** Le renforcement et le déploiement de compétences appropriées, d'une culture de la cybersécurité et de bonnes pratiques parmi toutes les parties prenantes est un enjeu majeur.

**5.2** Tous les pays et toutes les organisations sont confrontés à la nécessité de disposer des ressources humaines et des compétences suffisantes pour:

• mettre en œuvre des mesures de cybersécurité stratégiques et opérationnelles;

• procéder à des évaluations des risques en matière de cybersécurité au niveau national;

• gérer les crises liées aux incidents de cybersécurité;

• renforcer la robustesse et la résilience des infrastructures et des services numériques; et

• définir des processus, des compétences et des pratiques homogènes.

**5.3** Il importe aussi de relever que, compte tenu des progrès rapides des TIC et des problèmes d'accès et de connectivité déjà existants, il arrive souvent que les utilisateurs finals − et en particulier les populations comme les femmes, les enfants, les personnes âgées, les personnes handicapées et les personnes ayant des besoins particuliers − soient plus vulnérables aux menaces et aux incidents de cybersécurité. Les programmes d'éducation en matière de cybersécurité, outre la sensibilisation aux menaces de cybersécurité qui touchent les utilisateurs finals vulnérables, pourraient donc être essentiels pour réduire les risques de cybersécurité pour la société dans son ensemble.

Évolution de l'environnement du renforcement des capacités depuis 2008

**5.4** La cybersécurité ayant une dimension mondiale et traitant d'un large éventail de questions − comme l'utilisation ou la mauvaise utilisation des TIC, les mesures techniques, les questions économiques, juridiques et politiques − il importe d'élaborer une culture mondiale de la cybersécurité pour améliorer le niveau de compréhension de chaque acteur de la chaîne de la cybersécurité. Lors de la définition d'une culture de la cybersécurité, l'un des principaux défis consiste à cerner correctement les problèmes mondiaux et internationaux et les besoins locaux spécifiques, les cultures reposant principalement sur des facteurs locaux et temporels. Les normes techniques internationales peuvent contribuer à recenser les principaux problèmes mondiaux et génériques liés à la dimension technique et procédurale d'une culture de la cybersécurité.

**5.5** Une action collective est importante pour protéger les infrastructures numériques. Ceci est d'autant plus urgent que l'évolution technologique va dans le sens d'une interconnectivité accrue et permanente grâce aux TIC[[27]](#footnote-27). Tout ce qui peut être connecté pourrait être altéré. De plus, la miniaturisation des composants grâce aux nanotechnologies, notamment divers types de puces intelligentes et autonomes, a conduit à intégrer ces puces dans des technologies qui touchent à l'ensemble de nos activités.

**5.6** Le Programme GCA a servi de cadre interdisciplinaire novateur et efficace pour les mesures de renforcement des capacités, à partir duquel les acteurs concernés peuvent continuer de définir une action mondiale programmable et concrète, afin de pouvoir collaborer efficacement. Le cadre du Programme GCA vise à relever le défi de l'édification d'une société de l'information sûre et inclusive.

**5.7** Les recommandations formulées à cet égard dans le Rapport du groupe HLEG de 2008 restent d'actualité. Compte tenu des travaux menés par l'UIT, en particulier depuis la publication de la première édition du "[Guide de cybersécurité pour les pays en développement](https://www.itu.int/pub/D-STR-SECU-2006/fr)" en 2006, et sur la base du cadre du Programme GCA et du Rapport du groupe HLEG de 2008, des travaux approfondis ont été menés dans les États Membres sur le renforcement des capacités − y compris des activités de formation, de sensibilisation et d'éducation aux niveaux national, régional et international.

**5.8** En utilisant le cadre du Programme GCA, l'UIT continue d'aider les pays, notamment en renforçant les capacités et les compétences humaines nécessaires, en définissant leur stratégie nationale de cybersécurité, en contribuant à développer les compétences nécessaires à la gestion des équipes d'intervention en cas d'incident informatique (CIRT) et en mettant au point des ressources pour la protection en ligne des enfants.

**5.9** Par exemple, pour ce qui est de la sensibilisation, il importe de reconnaître la contribution de [l'Indice mondial de cybersécurité](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI). Depuis son lancement en 2015, le GCI − qui mesure l'engagement des États membres en matière de cybersécurité − a été publié trois fois grâce à la forte demande des États Membres, du secteur privé, des établissements universitaires et d'autres acteurs. Grâce à son engagement pour sensibiliser le public, le GCI continue d'aider les États Membres à améliorer leur situation en matière de cybersécurité en partageant les bonnes pratiques pour une mise en œuvre efficace de la cybersécurité. Le GCI s'est révélé être un outil de sensibilisation inestimable et devrait continuer à être exploité et renforcé.

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

**5.10** Des mesures concrètes devraient être prises au niveau national pour renforcer ou améliorer les capacités de cybersécurité des différentes parties prenantes afin de pouvoir traiter les questions de cybersécurité nationales et internationales. Les activités de renforcement des capacités se déroulant principalement au niveau national, des ressources appropriées devraient être allouées aux acteurs nationaux[[28]](#footnote-28).

**5.11** En outre, dans une perspective mondiale, l'autonomisation des ressources humaines nécessite un cadre éducatif général, modulaire et souple en matière de cybersécurité pour répondre aux besoins d'une sensibilisation accrue du public et de fournir un programme d'études adapté à des professionnels spécifiques. Une attention particulière devrait être accordée à l'écart entre les hommes et les femmes dans ce domaine. Il y a beaucoup de capital humain inexploité qui peut être mis à contribution dans le domaine de la cybersécurité, notamment les femmes qui ne représentent encore que 20% de la main-d'œuvre dans ce domaine[[29]](#footnote-29).

**5.12** La qualité de l'instruction au niveau scolaire ou universitaire et de la sensibilisation du grand public dépend dans une certaine mesure de la qualité, de la maturité et de la pertinence de la recherche.

**5.13** De plus, il importe de veiller à renforcer les capacités des micro, petites et moyennes entreprises (MPME), qui figurent désormais au nombre des acteurs clés de l'économie numérique en pleine croissance, en leur permettant d'identifier et de gérer les cyberrisques et d'utiliser les actifs TIC (y compris le large bande et l'Internet) de manière sûre et durable.

|  |
| --- |
| **5.14** 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 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, en collaboration avec les partenaires intéressés et d'autres 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.  **d)** 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.  **e)** Renforce la promotion 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.  **f)** 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 besoins de sécurité des technologies émergentes. À cet égard, il convient de favoriser une plus grande collaboration avec les établissements universitaires, le secteur privé et les États Membres.  **g)** 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 âgées − dans les efforts de renforcement des capacités.  **h)** Continue de développer et de renforcer le GCI en tant qu'outil de renforcement des capacités et de sensibilisation. |

|  |
| --- |
| **i)** Élabore un "Guide relatif à l'élaboration et à la mise en œuvre du programme d'éducation à la cybersécurité", dans le but d'aider les États Membres à élaborer/adopter des cours sur la cybersécurité 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 dans tous les domaines et auprès de tous les futurs professionnels.  **j)** Continue de faciliter le recensement des activités de recherche liées à la cybersécurité ou les dialogues entre les différentes parties prenantes, en particulier dans les domaines des technologies émergentes, en tirant parti de la participation des membres de l'UIT issus des milieux universitaires et du secteur privé, comme cela a été fait, par exemple, dans le cadre du Sommet mondial annuel de l'UIT sur l'intelligence artificielle au service du bien social.  **k)** 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 relever les défis en matière de sécurité et d'instaurer la confiance dans l'utilisation des TIC.  **l)** Continue de favoriser une culture de la cybersécurité. |

# Section 6 Pilier 5: Coopération internationale

Introduction

**6.1** Il ressort clairement de la dernière décennie qu'aucune entité ou organisation ne peut à elle seule relever l'ensemble des défis actuels et qui se font jour en matière de cybersécurité. Ces défis peuvent être relevés grâce à des partenariats fondés sur une collaboration et une coordination étroites entre toutes les parties prenantes, afin de contribuer à la mise en place d'un écosystème des TIC universellement disponible, ouvert, sûr et digne de confiance.

**6.2** Le Pilier 5 sur la Coopération internationale est donc un pilier intersectoriel du Programme GCA – il forme la base de tous les aspects liés à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC. Dans le Rapport du groupe HLEG de 2008, ce Pilier visait à élaborer une stratégie pour la coopération, le dialogue et la coordination internationaux face aux cybermenaces.

Évolution de l'environnement de la coopération internationale depuis 2008

Dialogues mondiaux de haut niveau

**6.3** Les débats sur les divers aspects de la cybersécurité − y compris les aspects techniques, la cybercriminalité, la vie privée, la protection des données et autres – ont lieu dans le cadre de nombreux forums et processus. Certains d'entre eux ont été organisés par diverses institutions spécialisées des Nations Unies, notamment l'UIT ou d'autres organisations internationales, et d'autres ont été lancés par d'autres parties prenantes, ainsi que diverses autres instances internationales et régionales.

**6.4** Si tous les forums et processus font un bon travail de sensibilisation et d'amélioration de la compréhension, il importe d'identifier les synergies entre ces différents efforts pour que la communauté internationale puisse se réunir et trouver des solutions.

**6.5** L'Organisation des Nations Unies, avec son importante capacité de rassemblement, est bien placée pour favoriser la coopération, le dialogue et la coordination au niveau international entre les parties prenantes de tous les pays pour relever les défis liés au cyberespace. Comme indiqué dans le Rapport du groupe HLEG de 2008, l'UIT, compte tenu de sa position au sein du système des Nations Unies en tant qu'institution spécialisée dans les TIC, peut continuer à jouer un rôle important, dans le cadre de son mandat, dans les domaines connexes.

**6.6** Alors qu'une "Conférence mondiale" était proposée dans la Recommandation 1.15 du Rapport du groupe HLEG de 2008[[30]](#footnote-30), des conférences, forums et processus actuels découlant du processus du SMSI et qui se sont ensuite renforcés – le [Forum du SMSI](https://www.itu.int/net4/wsis/forum/2020/fr) sur les questions liées au développement et l'[IGF](https://www.intgovforum.org/multilingual/fr/) sur la gouvernance – pourraient aussi être mieux utilisés à cet égard. Le Forum du SMSI, le plus grand rassemblement annuel des acteurs des TIC au service du développement (ICT4D) offre plusieurs mécanismes pour rassembler la communauté mondiale afin de débattre et de recenser des solutions concrètes aux défis du développement concernant le renforcement de la confiance et de la sécurité dans l'utilisation des TIC (grande orientation C5), y compris, entre autres, la partie des coordonnateurs des grandes orientations, les dialogues de haut niveau et des séances ciblées pour les parties prenantes.

**6.7**Une évolution importante au cours de la dernière décennie a été la reconnaissance de l'importance essentielle de la cybersécurité au plus haut niveau politique des gouvernements nationaux. Cela se traduit par l'adoption, par de nombreux pays, d'une stratégie en faveur de la transformation numérique qui adopte une approche faisant intervenir toutes les entités publiques et crée des mécanismes de coordination centrale intersectorielle qui relèvent généralement directement des chefs d'État ou de gouvernement.

**6.8** Une autre évolution connexe a été le nombre élevé de débats bilatéraux entre des pays et régions avancés sur le plan technologique.

Partenariats multi-parties prenantes internationaux

**6.9** L'UIT a connu certains succès dans le soutien à la coopération internationale de par son rôle de coordonnateur unique de la grande orientation C5 du SMSI.

**6.10** L'UIT a mis en place une série de partenariats multi-parties prenantes, que ce soit par:

• des mécanismes formels comme des protocoles d'accord ou des arrangements similaires (par exemple avec FIRST, Interpol, l'ONUDC, le WEF et d'autres);

• des initiatives comme la protection en ligne des enfants[[31]](#footnote-31), en partenariat avec plus de 80 entités de tous les groupes de parties prenantes; ou

• de mécanismes comme les Groupes spécialisés, par exemple les Groupes spécialisés sur les technologies de registres numériques, les technologies quantiques, l'IA et la santé, etc., qui donnent à toutes les parties prenantes la possibilité d'examiner des questions relatives à la confiance dans les nouvelles technologies.

**6.11** L'UIT a considérablement accru le nombre de ses parties prenantes au cours de la dernière décennie, en particulier parmi les entreprises du secteur privé et les établissements universitaires. Elle compte 193 États Membres et près de 900 entreprises du secteur privé, établissements universitaires et organisations internationales ou régionales, ce qui reflète l'évolution rapide de la société numérique.

Amélioration de la coordination au sein du système des Nations Unies

**6.12** Comme indiqué précédemment aux § 2.4 et 2.5 du présent document, un certain nombre de processus des Nations Unies ont été établis par l'Assemblée générale des Nations Unies pour aider à relever les défis consistant à garantir la sécurité internationale dans le cyberespace. Il s'agit notamment des travaux du Groupe d'experts gouvernementaux (GGE) et du groupe de travail à composition non limitée (OEWG). Dans son [rapport de fond final](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf) (2019-2021), l'OWEG a notamment conclu que le futur dialogue institutionnel régulier ne devrait pas faire double emploi avec les missions, les mesures et les activités actuelles de l'ONU consacrés aux dimensions numériques d'autres questions, et que tout mécanisme futur de dialogue institutionnel régulier sous l'égide de l'ONU devrait être un processus tourné vers l'action, assorti d'objectifs précis et reposant sur les résultats obtenus, et être inclusif, transparent, axé sur la recherche du consensus et fondé sur les résultats. Compte tenu de ce qui précède, il est important que les travaux de l'UIT complètent ceux qui sont actuellement menés au sein du système des Nations Unies dans ce domaine, en particulier les processus susmentionnés mis en place par l'Assemblée générale des Nations Unies.

**6.13** L'articulation complexe du mandat du système des Nations Unies peut parfois entraver une approche harmonisée pragmatique et efficace. Il est donc impératif que la famille des Nations Unies continue à travailler à l'harmonisation de ses efforts, notamment en rationalisant les programmes et les activités en matière de cybersécurité afin d'être plus efficace.

**6.14** En conséquence, il importe d'œuvrer à l'établissement d'une communauté de vues au sein des Nations Unies sur les besoins et exigences à remplir pour établir correctement des programmes et des initiatives qui appuieraient efficacement les efforts entrepris par les gouvernements, le secteur privé et toutes les autres parties prenantes concernées.

**6.15** 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. En collaboration avec l'Office des Nations Unies contre la drogue et le crime (ONUDC) et 33 autres institutions des Nations Unies, l'UIT a mené un effort de deux ans 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 Conseil des Chefs de secrétariat des organismes des Nations Unies pour la coordination (CCS) en novembre 2013.

**6.16** Bien qu'il s'agisse d'une étape clé, d'autres changements systémiques sont nécessaires afin d'assurer une coordination efficace. La priorité accordée à la coopération numérique par le Secrétaire général des Nations Unies[[32]](#footnote-32) offre la possibilité d'aborder la nécessité pour la famille des Nations Unies dans son ensemble de continuer d'améliorer la coordination et la coopération internes en ayant recours à divers mécanismes interorganisations, y compris le CCS.

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

|  |
| --- |
| **6.17** 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:  **a)** 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. L'UIT, 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), devrait continuer à jouer un rôle de premier plan en la matière, dans les domaines relevant de son mandat.  **b)** Sur la base du processus du SMSI et compte tenu des efforts du Groupe de haut niveau du Secrétaire général des Nations Unies sur la coopération numérique – en particulier la Recommandation 4 (Engagement mondial en faveur de la confiance et de la sécurité), l'UIT devrait contribuer à renforcer les efforts de facilitation en réunissant les différents acteurs. Ces efforts pourraient être déployés par l'intermédiaire des mécanismes offerts dans le cadre des processus liés à la grande orientation C5 par le biais du Forum du SMSI, ainsi que par ceux offerts par l'IGF, entre autres.  **c)** S'il convient de continuer à encourager les débats bilatéraux et multilatéraux entre les principaux acteurs, étant donné la nature mondiale des cybermenaces, il importe également de faciliter des échanges plus larges entre des groupes plus nombreux, y compris le secteur privé et d'autres parties prenantes. L'UIT pourrait, dans les domaines relevant de son mandat, jouer un rôle de coordonnateur à cet égard – en travaillant avec des partenaires pour aider à réunir toutes les parties prenantes dans le contexte mondial plus large des Nations Unies.  **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 jouer un rôle actif, avec d'autres institutions clés du système des Nations Unies, pour harmoniser les initiatives internes prises par le secrétariat des Nations Unies et pour 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

|  |
| --- |
| **7.1** 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)
4. Plus de renseignements sur la procédure et sur les observations des États Membres et d'autres parties prenantes sont disponibles à l'adresse <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. Documents finals du SMSI, 2005, disponibles à l'adresse <https://www.itu.int/net/wsis/outcome/booklet.pdf>. [↑](#footnote-ref-5)
6. Juge Stein Schjolber: Rapport du président du Groupe d'experts de haut niveau, 2008, disponible à l'adresse <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-6)
7. Les recommandations du Rapport du groupe HLEG de 2008 sont présentées avec un résumé annoté des points de vue exprimés et des discussions qui ont eu lieu pendant la réunion au sujet de chaque recommandation. Bien que les membres du groupe HLEG ne soient pas parvenus à un consensus complet sur chaque recommandation, la plupart des experts du groupe HLEG étaient néanmoins largement d'accord sur de nombreuses recommandations. [↑](#footnote-ref-7)
8. La [Directive du Parlement européen et du Conseil de l'Union européenne du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la Décision-cadre du Conseil (2005)](https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32013L0040) définit une infrastructure critique comme suit: un point, un système ou une partie de celui-ci, situé dans des États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État Membre du fait de la défaillance de ces fonctions. [↑](#footnote-ref-8)
9. Nombre d'utilisateurs actifs par mois de Facebook dans le monde au 4ème trimestre 2020, disponible à l'adresse <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>. [↑](#footnote-ref-9)
10. Mark Zuckerberg: L'Internet a besoin de nouvelles règles. Commençons dans les quatre domaines suivants, Washington Post, 30 mars 2019, disponible à l'adresse <https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html>. [↑](#footnote-ref-10)
11. Groupe d'experts gouvernementaux, disponible à l'adresse <https://www.un.org/disarmament/group-of-governmental-experts/>. [↑](#footnote-ref-11)
12. Groupe de travail à composition non limitée, disponible à l'adresse <https://www.un.org/disarmament/open-ended-working-group/>. [↑](#footnote-ref-12)
13. Pour plus de renseignements, veuillez vous référer aux documents suivants:

    – Rapport annuel sur l'activité de l'Union présenté au Conseil de l'UIT, concernant le renforcement de la confiance et de la sécurité dans l'utilisation des TIC, disponible à l'adresse <https://www.itu.int/en/council/2021/Pages/default.aspx>.

    – Rapport au Conseil, à sa session de 2021, sur l'utilisation du Programme GCA par l'UIT, disponible à l'adresse <https://www.itu.int/md/S21-CL-C-0036/en>. [↑](#footnote-ref-13)
14. Stein Schjolberg, *The History of Cybercrime* (3ème édition, février 2020). [↑](#footnote-ref-14)
15. La Commission de l'Union européenne a lancé un programme appelé [Horizon 2020](https://ec.europa.eu/programmes/horizon2020/en) pour développer le potentiel de l'Internet des objets et le programme de travail 2016-2017 pour soutenir l'expérimentation et l'innovation. Des propositions sont sollicitées sur plusieurs sujets, dont: sécurité de l'IoT et vie privée, concepts avancés pour la sécurité de bout en bout dans des environnements IoT très répartis, hétérogènes et dynamiques. Les méthodes doivent être globales et inclure l'identification et l'authentification, la protection des données et la prévention contre les cyberattaques au niveau des dispositifs et des systèmes. Elles doivent aborder les éléments de sécurité et de protection de la vie privée pertinents comme la confidentialité, la sensibilisation et le contrôle des données des utilisateurs, l'intégrité, la résilience et l'autorisation (voir la Décision C (2015) 6776 de la Commission européenne du 13 octobre 2015). [↑](#footnote-ref-15)
16. T. Ballell, *Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact*, Uniform Law Review, Volume 24, Issue 2, juin 2019, pages 302‑314, disponible à l'adresse <https://doi.org/10.1093/ulr/unz018>. [↑](#footnote-ref-16)
17. Un cadre juridique modèle peut être la [Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011](https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201192eu_en) relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants et la pédopornographie. [↑](#footnote-ref-17)
18. Juge Stein Schjolberg, 2018 et Juge Stein Schjolberg, 2019, disponible à l'adresse <https://www.cybercrimelaw.net/Cybercrimelaw.html>. [↑](#footnote-ref-18)
19. Par exemple, https://www.justice.gov/olp/lawful-access. [↑](#footnote-ref-19)
20. L'environnement des normes de l'UIT, disponible à l'adresse <https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance>. [↑](#footnote-ref-20)
21. Rapport du groupe HLEG, 2008, § 2.1, page 9, *id.* à 6. [↑](#footnote-ref-21)
22. Rapport du groupe HLEG, 2008, § 2.2, page 9, *id.* à 6. [↑](#footnote-ref-22)
23. Rapport du groupe HLEG, 2008, § 2, page 9, *id.* à 6. [↑](#footnote-ref-23)
24. Équipes CIRT nationales, UIT, disponible à l'adresse <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx>. [↑](#footnote-ref-24)
25. *Ibid*. [↑](#footnote-ref-25)
26. *Ibid*. [↑](#footnote-ref-26)
27. Tim Berners-Lee, 30 years on, what's next #ForTheWeb?, 12 mars 2019 (disponible à l'adresse <https://webfoundation.org/2019/03/web-birthday-30/>), à l'occasion du trentième anniversaire du web, dans une lettre ouverte, a déclaré que le web avait certes créé des possibilités, donné une voix aux groupes marginalisés et rendu notre vie quotidienne plus facile, mais avait aussi créé des possibilités pour les escrocs, donné une voix à ceux qui répandent la haine et rendu toutes sortes de crimes plus faciles à commettre. [↑](#footnote-ref-27)
28. S. Ghernaouti, *Cyberpower, Crime, Conflict and Security in Cyberspace*, Presses de l'EPFL, 2013. [↑](#footnote-ref-28)
29. Laurence Bradford, *Cybersecurity needs women: Here’s why,* 18 octobre 2018, disponible à l'adresse[*https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#5a7a3cc447e8*](https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#5a7a3cc447e8). [↑](#footnote-ref-29)
30. Rapport du groupe HLEG de 2008, § 1.15, page 9, *id.* à 6. [↑](#footnote-ref-30)
31. On trouvera davantage de renseignements à l'adresse <https://www.itu.int/en/cop/Pages/partners.aspx>. [↑](#footnote-ref-31)
32. De plus amples informations sont disponibles à l'adresse [https://www.un.org/en/digital-cooperation-panel/](https://www.un.org/fr/digital-cooperation-panel/index.html). [↑](#footnote-ref-32)