|  |  |
| --- | --- |
| **Conseil 2021 Consultation virtuelle des Conseillers, 8-18 juin 2021** |  |
|  |  |
|  |  |
| **Point de l'ordre du jour: PL 1.04** | **Document C21/82-F** |
| **25 mai 2021** |
| **Original: anglais** |
| Note du Secrétaire général | |
| Contribution de l'Australie, du Canada, de la République tchèque, de la France, de la RoUmanie et du Royaume-Uni de grande-bretagne et d'Irlande du nord  lignes directrices relatives à l'utilisation  du Programme mondial cybersécurité | |

J'ai l'honneur de transmettre aux États Membres du Conseil une contribution soumise par l'**Australie, le Canada, la République tchèque, la France, la Roumanie et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord**.

Houlin ZHAO  
 Secrétaire général

Contribution de l'Australie, du Canada, de la République tchèque, de la France, de la Roumanie et du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

lignes directrices relatives à l'utilisation   
du Programme mondial cybersécurité

|  |
| --- |
| Résumé  Nous sommes d'avis que les Lignes directrices relatives à l'utilisation du Programme mondial cybersécurité (GCA) devraient constituer un document de référence succinct et bien ciblé qui tienne compte des travaux que mène actuellement l'Union internationale des télécommunications (UIT) sur les questions liées à la cybersécurité, eu égard notamment à la Résolution 130 de la Conférence de plénipotentiaires, à la Résolution 50 de l'Assemblée mondiale de normalisation des télécommunications (AMNT), à la Résolution 45 de la Conférence mondiale de développement des télécommunications (CMDT), aux travaux de la Commission d'études 17 (CE 17) du Secteur de la normalisation des télécommunications de l'UIT (UIT-T) et d'autres initiatives et programmes menés par le Secteur du développement des télécommunications de l'UIT (UIT‑D).  Suite à donner  Le présent document **est soumis** au Conseil, afin qu'il l'examine.  \_\_\_\_\_\_\_\_\_\_\_\_  Références  [*https://www.itu.int/en/action/cybersecurity/Pages/default.aspx*](https://www.itu.int/en/action/cybersecurity/Pages/default.aspx)  *[Document C21/36](https://www.itu.int/md/S21-CL-C-0036/en)* |

# 1 Introduction

Nous nous félicitons qu'il soit possible de soumettre des observations complémentaires concernant le projet de Lignes directrices relatives à l'utilisation du Programme GCA et sommes bien conscients que de gros efforts ont été faits pour établir la version actuelle du projet de Lignes directrices que le Secrétaire général a soumis au Conseil à des fins d'examen.

Nous avons conscience que le Programme GCA est un dispositif important composé de cinq piliers (Mesures juridiques, Mesures techniques et de procédure, Structures administratives, Renforcement des capacités et Coopération internationale), et qu'il s'agit en substance d'un document de référence pour la coopération et la collaboration multipartites avec et entre tous les acteurs concernés, dans le prolongement des initiatives en cours, l'objectif étant d'éviter la répétition des tâches.

En outre, nous tenons à souligner que l'UIT utilise déjà le Programme GCA de manière efficace et rationnelle, dans l'intérêt de tous ses membres, comme indiqué dans la contribution soumise au Conseil par le Secrétaire général.

Conscients du mandat de l'Union et des activités et programmes qu'elle mène en matière de cybersécurité, et de la nécessité pour l'UIT et ses membres de bien comprendre l'objectif, le public cible et l'idée maîtresse des Lignes directrices, nous avons le plaisir de proposer de faire des Lignes directrices un document concis, bien ciblé et circonscrit aux activités simplifiées de chacun des piliers du Programme GCA exposées ci-dessous.

Pilier 1: Mesures juridiques

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

b) L'UIT devrait continuer à travailler avec les partenaires compétents, dans le cadre de son mandat, pour élaborer et tenir à jour des ressources sur la législation relative à la cybersécurité, afin d'aider les États Membres à comprendre les aspects juridiques de la cybersécurité, tout en soutenant l'échange de données d'expériences et de connaissances entre les États Membres pour les aider à élaborer des cadres dans ce domaine.

c) L'UIT, en collaboration avec toutes les parties prenantes, devrait s'attacher à dégager une idée commune précise du terme "technologies émergentes" et des possibilités et des difficultés liées à ces technologies, et faciliter l'échange d'études de cas et de bonnes pratiques sur les mesures juridiques susceptibles de s'appliquer aux niveaux national, régional et international.

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

Pilier 2: Mesures techniques et de procédure

a) Les Commissions d'études de l'UIT devraient, conformément à leurs compétences essentielles et mandat respectifs, s'attacher à préciser davantage ce qu'on entend par "technologies émergentes", afin de mener des études et de proposer des lignes directrices appropriées en matière de cybersécurité aux fins de l'utilisation de ces technologies, et recommander aux États Membres d'appliquer rapidement ces lignes directrices à titre volontaire.

b) Un mécanisme de coordination étroite devrait être établi entre les différentes Commissions d'études de l'UIT-T concernant l'étude des questions liées à la cybersécurité, la CE 17 jouant à cet égard un rôle de coordination ou de direction.

c) Une coordination et une collaboration étroites entre l'UIT et des organisations de normalisation relevant du secteur privé 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 poursuivre ses efforts en vue d'élaborer des Recommandations d'application volontaire sur les mesures techniques en matière de cybersécurité dans les domaines relevant de son mandat, en incitant ses membres à renforcer leur participation aux activités de normalisation connexes de l'UIT, en établissant des partenariats stratégiques et en consultant les organisations de normalisation relevant du secteur privé.

Pilier 3: Structures administratives

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

b) Pour éviter tout chevauchement d'activité, l'UIT devrait continuer d'encourager une collaboration ouverte et inclusive entre les diverses organisations nationales, régionales ou internationales participant à la mise en place de structures administratives nationales durables.

c) L'UIT devrait poursuivre ses efforts pour mesurer les engagements institutionnels des États Membres, en s'appuyant sur des outils comme l'Indice mondial de cybersécurité (GCI).

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

Pilier 4: Renforcement des capacités

a) Continuer de favoriser une collaboration et une coordination ouvertes et inclusives entre les diverses organisations nationales, régionales ou internationales engagées dans le renforcement des capacités en matière de cybersécurité, afin de garantir l'efficacité et d'éviter tout chevauchement d'activité.

b) Continuer de soutenir les pays en développement, les pays les moins avancés et les PEID dans leurs efforts 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) Continuer d'aider les pays en développement, les pays les moins avancés et les PEID, en collaboration avec les partenaires intéressés et les communautés de développement des capacités, à élaborer des stratégies, des plans, des politiques et des capacités d'intervention en cas d'incident en matière de cybersécurité au niveau national.

d) Renforcer et faciliter les échanges de bonnes pratiques des États Membres afin d'aider les pays en retard dans le domaine de la cybersécurité à améliorer leur position en matière de cybersécurité et à réduire l'écart en matière de capacités.

e) Continuer de faire évoluer les activités de renforcement des capacités, en tenant compte de la nécessité d'acquérir de nouvelles compétences pour s'adapter aux possibilités offertes et aux difficultés posées par les technologies émergentes.

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

g) Continuer d'utiliser l'Indice GCI, outil de renforcement des capacités et de sensibilisation.

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

i) Diffuser des outils, des ressources et des bonnes pratiques aux États Membres, au secteur privé et aux autres parties prenantes dans le but de soutenir leurs efforts pour renforcer la capacité des micro, petites et moyennes entreprises (MPME) à instaurer la confiance dans l'utilisation des TIC, et continuer de promouvoir une culture de la cybersécurité.

Pilier 5: Coopération internationale

a) L'UIT devrait continuer de jouer un rôle moteur dans les domaines relevant de son mandat pour favoriser la coopération, le dialogue et la coordination entre tous les pays, ainsi qu'avec le secteur privé et d'autres parties prenantes, sur les questions de cybersécurité mondiale.

b) S'il convient de continuer à encourager les débats bilatéraux et multilatéraux entre les principaux acteurs, étant donné la nature mondiale de la cybersécurité, il est également nécessaire de faciliter des échanges plus larges entre des groupes plus nombreux, y compris le secteur privé, le milieu universitaire, la société civile et d'autres parties prenantes.

c) L'UIT devrait continuer à explorer 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.

d) L'UIT devrait continuer à collaborer avec d'autres institutions clés du système des Nations Unies pour appuyer les initiatives internes du Secrétariat de l'ONU et rationaliser ses programmes et activités en matière de cybersécurité et ainsi servir plus efficacement la communauté internationale.

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