|  |  |
| --- | --- |
| **Conférence de plénipotentiaires (PP-22)Bucarest, 26 septembre – 14 octobre 2022** |  |
|  |  |
|  |  |
| SÉANCE PLÉNIÈRE | **Addendum 5 auDocument 68-F** |
|  | **18 août 2022** |
|  | **Original: russe** |
|  |
| États Membres de l'UIT, membres de la RCC |
| Proposition de révision de la résolution 130: |
| Renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'informationet de la communication |
|  |

|  |
| --- |
| RésuméLes travaux actuellement menés par l'UIT en vue de définir un Indice mondial de cybersécurité (GCI) à l'usage des États Membres contribuent largement à la protection des intérêts des utilisateurs des réseaux et des systèmes d'infocommunication. Dans le même temps, il apparaît que les pays en développement rencontrent certaines difficultés pour interpréter les résultats de l'Indice mondial de cybersécurité et prendre des décisions sur l'amélioration future de l'indice GCI, sur la base des données disponibles.Par conséquent, il serait opportun de renforcer les activités de l'UIT visant à promouvoir les calculs liés à l'Indice GCI et à mener à bien diverses activités pour faciliter la mise en œuvre des recommandations concrètes formulées par les experts de l'UIT. L'organisation à intervalles réguliers de séances visant à obtenir des retours d'informations à ce sujet permettrait à l'UIT d'évaluer l'efficacité de ses activités et de jeter les bases des améliorations futures à apporter aux méthodes de calcul de l'Indice GCI.Il est aussi proposé de remplacer les termes "sécurité informatique", dans le texte de la résolution, par le terme "cybersécurité".À l'heure actuelle, les termes "sécurité informatique" ne font pas l'objet d'une définition exclusive et s'appliquent à tous les domaines des technologies de l'information et de la communication (TIC) (groupes de serveurs, réseaux pour l'Internet des objets, plates-formes en nuage, etc.).L'un des aspects de l'utilisation sécurisée des TIC est l'utilisation de signatures numériques. Les mécanismes de confiance actuels liés à l'utilisation de signatures électroniques diffèrent considérablement d'un pays à l'autre. À titre d'exemple, l'autorisation des justificatifs d'un entrepreneur peut, dans certains pays, être accordée au moyen d'un certificat fourni à l'entrepreneur en tant que personne morale et, dans d'autres, en tant que personne physique, tandis que dans d'autres pays encore, il faut un certificat d'autorisation (certificat d'attribut) en plus de la signature électronique de la personne. Les différences importantes que l'on constate entre les pays quant à la manière d'instaurer la confiance au moyen d'une infrastructure de clé publique sont sources de difficultés considérables dans les activités commerciales.Une solution possible serait de tenir un registre général des autorités de certification accréditées, en mettant à disposition les informations pertinentes. La tenue d'un registre général répertoriant ces autorités de certification accréditées et donnant des informations sur leurs domaines d'activité, les algorithmes de chiffrement et les identificateurs qu'elles utilisent, ainsi que les types de certificats qu'elles émettent, contribuerait grandement à simplifier les interactions entre les entités commerciales dans différents pays.Compte tenu de ce qui précède, les pays membres de la RCC proposent d'apporter des modifications à la Résolution 130.Suite à donnerLa Conférence de plénipotentiaires est invitée à examiner la présente proposition et à apporter les modifications nécessaires à la Résolution 130 de la PP, 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".\_\_\_\_\_\_\_\_\_\_\_\_Références*-* |

MOD RCC/68A5/1

RÉSOLUTION 130 (RÉV. bucarest, 2022)

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

La Conférence de plénipotentiaires de l'Union internationale des télécommunications (Bucarest, 2022),

rappelant

*a)* la Résolution 68/198 de l'Assemblée générale des Nations Unies sur l'utilisation des technologies de l'information et de la communication (TIC) au service du développement;

*b)* la Résolution 71/199 de l'Assemblée générale des Nations Unies intitulée "Le droit à la vie privée à l'ère du numérique";

*c)* la Résolution 68/243 de l'Assemblée générale des Nations Unies intitulée "Progrès de l'informatique et des télécommunications et sécurité internationale";

*d)* la Résolution 57/239 de l'Assemblée générale des Nations Unies intitulée "Création d'une culture mondiale de la cybersécurité";

*e)* la Résolution 64/211 de l'Assemblée générale des Nations Unies, intitulée "Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infrastructures essentielles";

*f)* la Déclaration du SMSI+10 sur la mise en œuvre des résultats du SMSI et la Vision du SMSI pour l'après‑2015, adoptées lors de la Manifestation de haut niveau du SMSI+10 coordonnée par l'UIT (Genève, 2014) et organisée sur la base de la plate-forme préparatoire multi-parties prenantes (MPP), conjointement avec d'autres institutions des Nations Unies et ouverte à toutes les parties prenantes du SMSI, approuvées par la Conférence de plénipotentiaires (Busan, 2014) et soumises à l'examen d'ensemble de l'Assemblée générale des Nations Unies;

*g)* la Résolution 70/125 de l'Assemblée générale des Nations Unies, intitulée "Document final de la réunion de haut niveau de l'Assemblée générale sur l'examen d'ensemble de la mise en œuvre des textes issus du Sommet mondial sur la société de l'information (SMSI)";

*h)* la Résolution 174 (Rév. Busan, 2014) de la Conférence de plénipotentiaires sur le rôle de l'UIT concernant les questions de politiques publiques internationales ayant trait aux risques d'utilisation des TIC à des fins illicites;

*i)* la Résolution 179 (Rév. Dubaï, 2018) de la présente Conférence sur le rôle de l'UIT dans la protection en ligne des enfants;

*j)* la Résolution 181 (Rév. Guadalajara, 2010) de la Conférence de plénipotentiaires sur les définitions et termes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

*k)* la Résolution 196 (Rév. Dubaï, 2018) de la présente Conférence sur la protection des utilisateurs/consommateurs de services de télécommunication;

*l)* la Résolution 45 (Rév. Dubaï, 2014) de la Conférence mondiale de développement des télécommunications (CMDT) relative aux mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam;

*m)* la Résolution 140 (Rév. Dubaï, 2018) de la présente Conférence sur le rôle de l'UIT dans la mise en œuvre des résultats du SMSI et dans l'examen d'ensemble de leur mise en œuvre par l'Assemblée générale des Nations Unies;

n) la Résolution 58 (Rév. Dubaï, 2012) de l'Assemblée mondiale de normalisation des télécommunications (AMNT), intitulée "Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement[[1]](#footnote-1)1";

*o)* la Résolution 67 (Rév. Buenos Aires, 2017) de la CMDT, sur le rôle du Secteur du développement des télécommunications de l'UIT (UIT-D) dans la protection en ligne des enfants;

*p)* la Résolution 69 (Rév. Buenos Aires, 2017) de la CMDT sur la création d'équipes nationales d'intervention en cas d'incident informatique (CIRT), en particulier pour les pays en développement, et la coopération entre ces équipes;

*q)* que, dans la Résolution 1305 qu'il a adoptée à sa session de 2009, le Conseil de l'UIT a défini la sécurité, la sûreté, la continuité, la durabilité et la solidité de l'Internet comme autant de questions de politiques publiques qui relèvent du mandat de l'UIT,

considérant

*a)* que la Manifestation de haut niveau SMSI+10 coordonnée par l'UIT a réaffirmé qu'il importait d'instaurer la confiance et la sécurité dans l'utilisation des TIC, comme indiqué dans les paragraphes pertinents des documents finals du SMSI+10 (Genève, 2014);

*b)* l'importance cruciale des infrastructures de l'information et de la communication et de leurs applications dans la quasi‑totalité des formes d'activités sociales et économiques;

*c)* les dispositions de l'Engagement de Tunis et de l'Agenda de Tunis relatives à la cybersécurité et le document final de la réunion de haut niveau de l'Assemblée générale des Nations Unies sur l'examen d'ensemble de la mise en œuvre des textes issus du SMSI;

*d)* que, du fait de l'utilisation et du développement des TIC, de nouvelles menaces, d'origines diverses, sont apparues, qui ont nui à la confiance et à la sécurité dans l'utilisation des TIC par tous les États Membres, les Membres des Secteurs et les autres parties prenantes, y compris tous les utilisateurs des TIC, et qui ont nui également au maintien de la paix ainsi qu'au développement socio‑économique de tous les États Membres; que, par ailleurs, ces menaces pesant sur les infrastructures, les réseaux et les dispositifs, et la vulnérabilité de ceux-ci, continuent de poser à tous les pays, en particulier aux pays en développement, des problèmes de sécurité croissants qui dépassent le cadre du territoire national, tout en notant dans ce contexte le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des TIC et la nécessité d'intensifier la coopération internationale et de promouvoir le renforcement des capacités et de développer les mécanismes nationaux, régionaux et internationaux existants appropriés (par exemple, accords, bonnes pratiques, mémorandums d'accord, etc.);

*e)* que le Secrétaire général de l'UIT a été invité à appuyer d'autres projets mondiaux ou régionaux en matière de cybersécurité, le cas échéant, et que tous les pays, en particulier les pays en développement, ont été invités à participer aux activités qui s'y rapportent et présentent un intérêt pour l'UIT;

*f)* le Programme mondial cybersécurité (GCA) de l'UIT, qui encourage la coopération internationale dans la recherche de stratégies et de solutions pour accroître la confiance et la sécurité dans l'utilisation des télécommunications/TIC;

*g)* que, pour protéger ces infrastructures et traiter ces problèmes et ces menaces, il faut que des mesures coordonnées soient prises aux niveaux national, régional et international, en matière de prévention, de préparation, de réaction et de rétablissement en cas d'incidents liés à la cybersécurité, par les autorités nationales (y compris la création d'équipes nationales CIRT) et sous‑nationales, par le secteur privé, et par les particuliers et les utilisateurs; une coopération et une coordination internationales et régionales sont également nécessaires et l'UIT a un rôle prééminent à jouer dans le cadre de son mandat et de ses compétences en la matière;

*h)* qu'une approche itérative et fondée sur les risques en matière de cybersécurité permet d'élaborer et d'appliquer les pratiques de cybersécurité qui s'imposent pour faire face à l'évolution constante des menaces et des vulnérabilités, et que la sécurité est un processus continu et itératif qui doit être intégré dans le développement et le déploiement des technologies et de leurs applications dès leur conception et maintenu tout au long de leur cycle de vie;

*i)* la nécessité d'une évolution permanente des nouvelles technologies pour appuyer la détection rapide des événements ou incidents compromettant la cybersécurité et la réaction concertée et dans les délais à de tels événements ou incidents, ou d'incidents de sécurité des réseaux informatiques qui pourraient compromettre la disponibilité, l'intégrité et la confidentialité des infrastructures essentielles des États Membres de l'UIT, et la nécessité d'adopter des stratégies qui réduiront au minimum les répercussions de tels incidents et atténueront les risques et les menaces croissants auxquels ces plates-formes sont exposées;

*j)* que l'Assemblée générale des Nations Unies, dans sa Résolution 70/125, intitulée "Document final de la réunion de haut niveau de l'Assemblée générale sur l'examen d'ensemble de la mise en œuvre des textes issus du SMSI", a reconnu les défis auxquels les États, en particulier les pays en développement, sont confrontés dans le cadre de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, et a demandé de se concentrer davantage sur le renforcement des capacités, l'éducation, le partage des connaissances et les pratiques réglementaires, ainsi que sur la promotion de la collaboration multi-parties prenantes à tous les niveaux et la sensibilisation des utilisateurs des TIC, en particulier les plus pauvres et les plus vulnérables;

*k)* que les cybermenaces et les cyberattaques sont de plus en plus nombreuses et que la dépendance à l'égard de l'Internet et d'autres réseaux qui sont essentiels pour avoir accès à des services et à l'information est de plus en plus grande;

*l)* que le Secteur de la normalisation des télécommunications de l'UIT (UIT-T) a adopté près de 300 normes sur l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

*m)* le rapport final sur la Question 3/2 "Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité" de l'UIT-D;

*n)* que par sa nature même, l'environnement des normes en matière de cybersécurité appelle une coopération entre l'UIT et d'autres organisations nationales, régionales, mondiales ou sectorielles;

*o)* qu'un grand nombre de pays en développement élaborent ou mettent en œuvre actuellement des stratégies nationales en matière de cybersécurité;

*p)* que la cybersécurité est devenue une question très importante au niveau international et que le rôle et la participation de l'ONU et de ses institutions spécialisées, par exemple l'UIT, en vue d'instaurer la confiance et la sécurité dans l'utilisation des TIC sont dès lors importants;

*q)* que toutes les parties prenantes remplissent des rôles différents et assument des responsabilités différentes pour ce qui est d'assurer la confiance et la sécurité dans l'utilisation des TIC;

*r)* que certaines petites et moyennes entreprises (PME) se heurtent à des difficultés supplémentaires lorsqu'il s'agit de mettre en œuvre les pratiques relatives à la cybersécurité,

reconnaissant

*a)* que la cybersécurité est un élément fondamental de la sécurisation des infrastructures de télécommunication/TIC et constitue une base essentielle du développement socio-économique;

*b)* que le développement des TIC a été et continue d'être déterminant pour la croissance et le développement de l'économie mondiale, y compris de l'économie numérique, étayés par la sécurité et la confiance;

*c)* que le SMSI a affirmé l'importance qu'il y a à établir la confiance et la sécurité dans l'utilisation des TIC, ainsi que la grande importance d'une mise en œuvre multi-parties prenantes au niveau international, et a défini la grande orientation C5 (Établir la confiance et la sécurité dans l'utilisation des TIC), l'UIT ayant été désignée dans l'Agenda de Tunis comme coordonnateur/modérateur pour cette grande orientation, et que l'Union s'est acquittée de cette tâche ces dernières années, par exemple dans le cadre du Programme GCA;

*d)* que la CMDT-17 a adopté le Plan d'action de Buenos Aires et son Objectif 2, en particulier le produit 2.2 relatif à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, qui identifie la cybersécurité comme une activité prioritaire du Bureau de développement des télécommunications (BDT) et définit les principaux domaines de travail que celui-ci doit entreprendre; et que la CMDT-14 a adopté la Résolution 45 (Rév. Dubaï, 2014) relative aux mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam, dans laquelle le Secrétaire général est prié de porter cette résolution à l'attention de la prochaine Conférence de plénipotentiaires pour examen et suite à donner, et de présenter un rapport sur les résultats de ces principaux domaines de travail au Conseil et à la Conférence de plénipotentiaires de 2018, selon qu'il conviendra; ainsi que la Résolution 69 (Rév. Buenos Aires, 2017) relative à la création d'équipes nationales CIRT, en particulier pour les pays en développement, et à la coopération entre ces équipes;

*e)* que dans la Déclaration de Buenos Aires qu'elle a adoptée, la CMDT-17 déclare: "que le renforcement de la confiance et de la sécurité dans l'utilisation des télécommunications/TIC ainsi que la protection des données personnelles sont des priorités, qui appellent une coopération et une coordination internationales entre les gouvernements, les organisations concernées, les entreprises et les entités du secteur privé dans le domaine du renforcement des capacités et de l'échange de bonnes pratiques, en vue de l'élaboration de politiques publiques connexes et de mesures juridiques, réglementaires et techniques tenant compte, notamment, de la protection des données personnelles, et que les parties prenantes devraient œuvrer ensemble pour assurer la fiabilité et la sécurité des réseaux et services TIC";

*f)* que, pour appuyer la création d'équipes nationales CIRT dans les États Membres où de telles équipes sont nécessaires et n'existent pas actuellement, l'AMNT-16 a adopté la Résolution 58 (Rév. Dubaï, 2012), dans laquelle elle encourage la création d'équipes nationales CIRT, en particulier pour les pays en développement, et la CMDT-17 a adopté la Résolution 69 (Rév. Buenos Aires, 2017), relative à la création d'équipes nationales CIRT, y compris d'équipes CIRT chargées de la coopération entre les gouvernements, en particulier pour les pays en développement, à la coopération entre ces équipes et à l'importance d'assurer une coordination entre toutes les organisations concernées;

*g)* le paragraphe 15 de l'Engagement de Tunis, libellé en ces termes: "Reconnaissant les principes de l'accès universel et non discriminatoire aux TIC pour toutes les nations, la nécessité de prendre en compte le niveau de développement social et économique de chaque pays, dans le respect des aspects de la société de l'information qui privilégient le développement, nous insistons sur le fait que les TIC sont des outils efficaces pour promouvoir la paix, la sécurité et la stabilité, pour renforcer la démocratie, la cohésion sociale, la bonne gouvernance et la primauté du droit, à l'échelle nationale, régionale et internationale. Les TIC peuvent servir à promouvoir la croissance économique et le développement des entreprises. Pour atteindre ces objectifs, il est capital de développer les infrastructures, de renforcer les capacités humaines et de sécuriser l'information et les réseaux. Nous sommes par ailleurs conscients de la nécessité de faire face efficacement aux enjeux et aux menaces résultant de l'utilisation des TIC à des fins qui sont incompatibles avec les objectifs de maintien de la stabilité et de la sécurité internationales et qui risquent de nuire à l'intégrité des infrastructures nationales, au détriment de la sécurité des États. Il est nécessaire de prévenir toute utilisation abusive des ressources et technologies de l'information à des fins criminelles et terroristes, tout en respectant les droits de l'homme", et que les problèmes créés par cette utilisation abusive des ressources TIC n'ont fait que croître depuis la tenue du SMSI;

*h)* que la Manifestation de haut niveau SMSI+10, coordonnée par l'UIT, a identifié plusieurs problèmes qui subsistent dans la mise en œuvre des grandes orientations du SMSI et qui devront être réglés après 2015;

*i)* que, dans l'élaboration de mesures législatives appropriées et efficaces concernant la protection contre les cybermenaces aux niveaux national, régional et international, les États Membres, en particulier les pays en développement, peuvent avoir besoin de l'aide de l'UIT pour mettre en place des mesures techniques et de procédure visant à sécuriser les infrastructures nationales des TIC, à la demande de ces États Membres, tout en notant qu'un certain nombre d'initiatives régionales et internationales peuvent aider ces pays à élaborer de telles mesures législatives;

*j)* l'Avis 4 (Lisbonne, 2009) du Forum mondial des politiques de télécommunication/TIC sur les stratégies de collaboration propres à instaurer la confiance et la sécurité dans l'utilisation des TIC;

*k)* les résultats pertinents de l'AMNT-16, et en particulier:

i) la Résolution 50 (Rév. Hammamet, 2016) sur la cybersécurité;

ii) la Résolution 52 (Rév. Hammamet, 2016) intitulée "Lutter contre et combattre le spam";

*l)* que des réseaux sûrs et fiables renforceront la confiance et favoriseront l'échange et l'utilisation d'informations et de données;

*m)* que la valorisation des compétences humaines et le renforcement des capacités sont essentiels pour améliorer la protection des réseaux d'information;

*n)* que les États Membres s'efforcent d'améliorer les cadres institutionnels;

*o)* que l'évaluation et l'analyse des risques permettent de mieux comprendre les risques liés à la cybersécurité auxquels font face les organisations ainsi que les moyens de les atténuer,

consciente du fait

*a)* que l'UIT et d'autres organisations internationales examinent actuellement, dans le cadre de diverses activités, des questions liées à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, notamment la stabilité, ainsi que des mesures visant à combattre le spam, les logiciels malveillants, etc., et à protéger les données personnelles et la confidentialité;

*b)* que la Commission d'études 17 de l'UIT‑T et les Commissions d'études 1 et 2 de l'UIT-D et d'autres commissions d'études compétentes de l'UIT poursuivent leurs travaux sur les moyens techniques permettant d'assurer la sécurité des réseaux d'information et de communication, conformément aux Résolutions 50 et 52 (Rév. Hammamet, 2016) et aux Résolutions 45 (Rév. Dubaï, 2014) et 69 (Rév. Buenos Aires, 2017);

*c)* que l'UIT a un rôle fondamental à jouer pour instaurer la confiance et la sécurité dans l'utilisation des TIC;

*d)* que la Commission d'études 2 de l'UIT‑D continue d'effectuer les études demandées au titre de la Question 3/2 de l'UIT-D (Sécurisation des réseaux d'information et de communication: meilleures pratiques pour créer une culture de la cybersécurité), qui a été reflétée dans la Résolution 64/211 de l'Assemblée générale des Nations Unies;

*e)* que l'UIT fournit aussi une assistance aux pays en développement pour l'instauration de la confiance et de la sécurité dans l'utilisation des TIC et qu'elle appuie la création d'équipes CIRT, y compris d'équipes CIRT chargées de la coopération entre les gouvernements, et qu'il importe d'assurer une coordination entre toutes les organisations concernées;

*f)* que, dans la Résolution 1336 qu'il a adoptée à sa session de 2011, le Conseil a créé un Groupe de travail du Conseil sur les questions de politiques publiques internationales relatives à l'Internet (GTC-Internet), qui a pour mandat d'identifier, d'étudier et d'approfondir les thèmes liés aux questions de politiques publiques internationales relatives à l'Internet, notamment les questions recensées dans la Résolution 1305 du Conseil (2009) telles que la sécurité, la sûreté, la continuité, la durabilité et la robustesse de l'Internet;

*g)* que la CMDT-17 a adopté la Résolution 80 (Buenos Aires, 2017) intitulée "Établir et promouvoir des cadres de l'information sécurisés dans les pays en développement afin de faciliter et d'encourager les échanges d'informations économiques par voie électronique entre partenaires économiques";

*h)* que l'Article 6 relatif à la sécurité et à la robustesse des réseaux et l'Article 7 relatif aux communications électroniques non sollicitées envoyées en masse du Règlement des télécommunications internationales ont été adoptés par la Conférence mondiale des télécommunications internationales (Dubaï, 2012),

notant

*a)* que, en tant qu'organisation intergouvernementale aux travaux de laquelle participe le secteur privé, l'UIT est bien placée pour jouer un rôle important, de même que d'autres instances et organisations internationales compétentes, pour parer aux menaces et remédier aux vulnérabilités qui ont une incidence sur les efforts entrepris pour instaurer la confiance et la sécurité dans l'utilisation des TIC;

*b)* les paragraphes 35 et 36 de la Déclaration de principes de Genève et le paragraphe 39 de l'Agenda de Tunis, sur le renforcement de la confiance et de la sécurité dans l'utilisation des TIC;

*c)* que, bien qu'il n'existe pas de définitions universellement acceptées du spam et d'autres termes connexes, le spam a été décrit par la Commission d'études 2 de l'UIT‑T, à sa réunion de juin 2006, comme étant un terme couramment employé pour désigner l'envoi en masse de messages électroniques non sollicités, par courriel ou par messagerie mobile (SMS ou MMS), habituellement dans le but de faire vendre des produits ou services commerciaux;

*d)* l'initiative prise par l'Union concernant la coopération avec le Forum des équipes et de sécurité en cas d'incident,

ayant à l'esprit

les travaux de l'UIT établis par les Résolutions 50 et 52 (Rév. Hammamet, 2016) et la Résolution 58 (Rév. Dubaï, 2012), la Résolution 45 (Rév. Dubaï, 2014) et la Résolution 69 (Rév. Buenos Aires, 2017), l'Objectif 2 du Plan d'action de Buenos Aires, les Questions pertinentes de l'UIT-T sur les aspects techniques de la sécurité des réseaux d'information et de communication et la Question 3/2 de l'UIT‑D,

décide

1 de continuer d'accorder à ces travaux un rang de priorité élevé à l'UIT, conformément à ses compétences et à ses connaissances spécialisées, notamment en favorisant une compréhension commune, entre les gouvernements et les autres parties prenantes, de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC aux niveaux national, régional et international;

2 d'accorder un rang de priorité élevé aux travaux de l'UIT décrits dans le texte du *ayant à l'esprit* ci‑dessus, conformément à ses compétences et à ses domaines de spécialisation, et de continuer de collaborer étroitement, selon qu'il conviendra, avec d'autres organismes ou institutions concernés du système des Nations Unies et d'autres organismes internationaux concernés, compte tenu des mandats et des domaines de compétence spécifiques des différentes institutions, tout en gardant à l'esprit la nécessité d'éviter tout chevauchement des travaux entre les organisations et entre les Bureaux ou le Secrétariat général;

3 que l'UIT doit consacrer essentiellement des ressources et des programmes aux domaines de la cybersécurité à l'échelle nationale, régionale et internationale 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. Toutefois, cela n'empêche pas l'UIT de s'acquitter de son mandat, qui consiste à élaborer des recommandations techniques destinées à réduire les vulnérabilités de l'infrastructure des TIC, et de fournir toute l'assistance qui a été décidée à la CMDT‑17, y compris dans le cadre de l'Objectif 2 et des activités au titre de la Question 3/2;

4 de promouvoir une culture dans laquelle la sécurité est perçue comme un processus continu et itératif, intégré aux produits dès leur conception et maintenu tout au long de leur cycle de vie, et est accessible et compréhensible pour les utilisateurs;

5 de sensibiliser davantage les membres de l'UIT aux activités menées au sein de l'Union et d'autres entités compétentes qui s'emploient à améliorer la cybersécurité, y compris en ce qui concerne le renforcement des capacités, et de sensibiliser ces entités aux défis particuliers auxquels font face les pays en développement pour ce qui est d'instaurer la confiance et la sécurité dans l'utilisation des TIC;

6 de contribuer à renforcer encore la confiance et le cadre de sécurité, conformément au rôle de l'UIT en tant que coordonnateur principal pour la grande orientation C5 du SMSI, compte tenu de la Résolution 140 (Rév. Dubaï, 2018);

7 de continuer de tenir à jour, compte tenu de la base d'informations associée à la "Feuille de route pour la normalisation de la sécurité des TIC" et des efforts entrepris par l'UIT-D dans le domaine de la cybersécurité, et avec le concours d'autres organisations compétentes, un inventaire des initiatives et activités nationales, régionales et internationales, pour promouvoir l'élaboration d'approches communes dans le domaine de la cybersécurité;

8 de procéder à des études de cas sur les accords institutionnels liées à la cybersécurité, en coopération avec les membres et les organisations concernées;

9 d'étudier les problèmes particuliers que rencontrent les PME en matière de cybersécurité et de tenir compte de ces problèmes dans le cadre des activités que mène l'UIT pour instaurer la confiance et la sécurité dans l'utilisation des TIC;

10 de prendre en considération les incidences du déploiement de technologies émergentes sur la cybersécurité et d'en tenir compte dans les activités que mène l'UIT pour instaurer la confiance et la sécurité dans l'utilisation des TIC;

11 d'appuyer le développement de l'infrastructure qui sous-tend le processus en cours de transformation numérique de l'économie mondiale, en instaurant la confiance et la sécurité dans l'utilisation des TIC, en particulier pour lutter contre les menaces actuelles et futures, dans le cadre du mandat de l'UIT;

12 d'utiliser le cadre qu'offre le Programme 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 TIC,

charge le Secrétaire général et les Directeurs des Bureaux

1 de continuer d'examiner:

i) les travaux effectués à ce jour au sein des trois Secteurs, dans le cadre du Programme GCA de l'UIT et par d'autres organisations compétentes, ainsi que les initiatives visant à assurer et à renforcer la protection contre les menaces existantes et futures, afin d'instaurer la confiance et la sécurité dans l'utilisation des TIC;

ii) les progrès réalisés dans la mise en œuvre de la présente résolution, l'UIT continuant de jouer un rôle de premier plan en tant que modérateur/coordonnateur pour la grande orientation C5, avec l'aide des groupes consultatifs, conformément aux dispositions de la Constitution de l'UIT et de la Convention de l'UIT;

iii) les résultats des travaux menés à ce jour pour aider notamment les pays en développement à renforcer les capacités et les compétences en matière de cybersécurité, afin de veiller à ce que l'UIT mobilise efficacement ses ressources pour relever les défis liés au développement;

2 conformément à la Résolution 45 (Rév. Dubaï, 2014), de faire rapport au Conseil sur les activités menées par l'UIT et d'autres organisations et entités concernées pour améliorer la coopération et la collaboration, aux niveaux régional et mondial, pour renforcer l'instauration de la confiance et de la sécurité des États Membres dans l'utilisation des TIC, en particulier des pays en développement, compte tenu des informations fournies par les États Membres, notamment des informations relatives à des situations qui sont de leur ressort et qui sont susceptibles d'avoir une incidence sur cette coopération;

3 conformément à la Résolution 45 (Rév. Dubaï, 2014), de soumettre un rapport sur les mémorandums d'accord entre les pays, ainsi que sur les formes de coopération existantes, comportant une analyse de leur état d'avancement, de leur portée et des applications de ces mécanismes de coopération, dans le but de renforcer la cybersécurité et de lutter contre les cybermenaces, afin de permettre aux États Membres de déterminer si des mémorandums ou des mécanismes supplémentaires sont nécessaires;

4 de mieux faire connaître les activités menées au sein de l'UIT et d'autres entités compétentes qui s'emploient à renforcer la cybersécurité, y compris en ce qui concerne le renforcement des capacités, et les défis particuliers auxquels les pays en développement font face concernant l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, conformément au point 5 du *décide*;

5de faciliter, dans les limites du budget disponible, l'accès aux outils et aux ressources nécessaires pour renforcer la confiance et la sécurité dans l'utilisation des TIC pour tous les États Membres, conformément aux dispositions adoptées par le SMSI en ce qui concerne la mise en place d'un accès universel et non discriminatoire aux TIC pour tous les pays;

6 de continuer d'échanger des informations et des connaissances sur les initiatives nationales, régionales et internationales qui sont ou seront prises dans le monde en matière de cybersécurité, via la page web de l'UIT consacrée à la cybersécurité, et d'encourager toutes les parties prenantes à contribuer à ces activités, en tenant compte des portails existants;

7 de faire rapport chaque année au Conseil sur ces activités et de formuler des propositions, selon qu'il conviendra;

8 d'améliorer encore la coordination entre les commissions d'études et les programmes concernés,

charge le Directeur du Bureau de la normalisation des télécommunications

1 d'intensifier les travaux menés au sein des commissions d'études existantes de l'UIT-T pour:

i) faire face aux menaces et aux vulnérabilités existantes ou futures qui nuisent aux efforts visant à instaurer la confiance et la sécurité dans l'utilisation des TIC, compte tenu des nouveaux services et des nouvelles applications reposant sur les réseaux de télécommunication/TIC, en élaborant des rapports ou des recommandations, selon qu'il conviendra, en vue de mettre en œuvre les résolutions de l'AMNT, en particulier les Résolutions 50 et 52 (Rév. Hammamet, 2016) et la Résolution 58 (Rév. Dubaï, 2012), en permettant le commencement des travaux avant qu'une Question ne soit approuvée;

ii) rechercher des moyens de promouvoir l'échange d'informations techniques dans ces domaines, d'encourager l'adoption de protocoles et de normes qui permettent d'accroître la sécurité et de promouvoir la coopération internationale entre les entités concernées;

iii) faciliter des projets issus des résultats de l'AMNT-16, en particulier de:

• la Résolution 50 (Rév. Hammamet, 2016) relative à la cybersécurité;

• la Résolution 52 (Rév. Dubaï, 2012), intitulée "Lutter contre et combattre le spam";

2 d'envisager de promouvoir, au sein de l'UIT-T, une culture dans laquelle la sécurité est perçue comme un processus continu et itératif, et de soumettre, s'il y a lieu, des propositions au Conseil;

3 de poursuivre la collaboration avec les organisations compétentes, afin d'échanger des informations sur les bonnes pratiques et de diffuser l'information, par exemple dans le cadre de formations et d'ateliers communs, d'activités conjointes de coordination et, sur invitation, de contributions écrites soumises par les organisations compétentes,

charge le Directeur du Bureau de développement des télécommunications

1 conformément aux résultats de la CMDT-17 et en application des Résolutions 45 (Rév. Dubaï, 2014) et 69 (Rév. Buenos Aires, 2017), de la Résolution 80 (Buenos Aires, 2017) et de l'Objectif 2 du Plan d'action de Buenos Aires, d'appuyer les projets mondiaux ou régionaux en cours en matière de cybersécurité et d'encourager tous les pays à prendre part à ces activités;

2 d'appuyer, sur demande, les efforts déployés par les États Membres de l'UIT pour renforcer les capacités en facilitant l'accès des États Membres aux ressources élaborées par d'autres organisations internationales compétentes qui s'intéressent aux législations nationales en matière de lutte contre la cybercriminalité; en appuyant les efforts déployés par les États Membres de l'UIT sur les plans national et régional pour renforcer les capacités aux fins de la protection contre les cybermenaces/la cybercriminalité, en collaboration entre eux; conformément à la législation nationale des États Membres dont il est question plus haut, en aidant les États Membres, en particulier les pays en développement, à élaborer des mesures juridiques appropriées et réalisables en matière de protection contre les cybermenaces aux niveaux national, régional et international; en établissant des mesures techniques et liées aux procédures visant à sécuriser les infrastructures TIC nationales, en tenant compte des travaux accomplis par les commissions d'études concernées de l'UIT-T et, les cas échéant, par d'autres organisations concernées; et en établissant des structures organisationnelles, telles que des équipes CIRT, pour identifier et gérer les cybermenaces et pour y réagir, ainsi que des mécanismes de coopération aux niveaux régional et international;

3 de fournir l'appui administratif et financier nécessaire à ces projets, dans les limites des ressources existantes, et de rechercher des ressources additionnelles (en espèces ou en nature) pour mettre en œuvre ces projets dans le cadre d'accords de partenariat;

4 d'assurer la coordination des travaux liés à ces projets dans le contexte des activités générales entreprises par l'UIT en sa qualité de modérateur/coordonnateur pour la grande orientation C5 du SMSI, et d'éliminer tout double emploi avec les activités du Secrétariat général et de l'UIT-T concernant ce thème important;

5 de coordonner les travaux liés à ces projets avec ceux des commissions d'études de l'UIT‑D sur cette question et avec les activités correspondantes au titre des programmes ainsi qu'avec le Secrétariat général;

6 de poursuivre la collaboration avec les organisations concernées, afin d'échanger des données sur les bonnes pratiques et de diffuser l'information grâce, par exemple, à des sessions de formation et à des ateliers communs;

7 d'appuyer les travaux de la Commission d'études 17 et des autres commissions d'études de l'UIT-T, en encourageant et facilitant la mise en œuvre par les États Membres et les Membres des Secteurs de l'UIT, en particulier dans les pays en développement, des Recommandations UIT-T approuvées qui ont trait à la sécurité;

8 d'aider les États Membres de l'UIT à élaborer leurs stratégies de cybersécurité nationales ou régionales en vue de renforcer les capacités nationales de lutte contre les cybermenaces, selon les principes de la coopération internationale, conformément à l'Objectif 2 du Plan d'action de Buenos Aires;

9 de fournir aux membres un appui en ce qui concerne le développement des compétences humaines et le renforcement des capacités afin d'améliorer la cybersécurité;

10 d'apporter un appui aux membres concernant les activités d'évaluation des risques se rapportant à la cybersécurité;

11 de faire rapport chaque année au Conseil sur ces activités et de formuler des propositions, selon qu'il conviendra,

charge en outre le Directeur du Bureau de la normalisation des télécommunications et le Directeur du Bureau de développement des télécommunications

dans les limites de leurs responsabilités respectives,

1 de mettre en œuvre les résolutions pertinentes de l'AMNT-16 et de la CMDT-17, y compris le Produit 2.2 de l'Objectif 2 du Plan d'action de Buenos Aires, en mettant l'accent en particulier sur les besoins des pays en développement dans le cadre des efforts qu'ils déploient pour améliorer la cybersécurité et instaurer la confiance et la sécurité dans l'utilisation des TIC;

2 de déterminer s'il existe des informations sur l'instauration de la confiance et de la sécurité dans l'utilisation des TIC et de favoriser la disponibilité de telles informations, y compris celles qui se rapportent aux infrastructures TIC, pour les États Membres, les Membres des Secteurs et les organisations concernées;

3 de continuer de définir, sans répéter les travaux accomplis au titre de la Question 3/2 de l'UIT‑D, de bonnes pratiques liées à la Question 3/2, notamment en ce qui concerne l'établissement d'équipes CIRT, et d'examiner le guide de référence à l'intention des États Membres et, selon qu'il conviendra, de contribuer à l'étude de la Question 3/2;

4 de coopérer avec les organisations concernées et d'autres experts internationaux et nationaux compétents, selon qu'il conviendra, afin de définir de bonnes pratiques relatives à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, notamment en ce qui concerne l'établissement d'équipes CIRT;

5 de prendre des mesures afin que de nouvelles Questions soient examinées par les commissions d'études des Secteurs relativement à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

6 de déterminer et de répertorier les mesures concrètes susceptibles d'aider les pays en développement à renforcer leurs capacités et leurs compétences en matière de cybersécurité, compte tenu des défis particuliers auxquels ces pays sont confrontés;

7 de tenir compte des problèmes que rencontrent toutes les parties prenantes, en particulier dans les pays en développement, pour instaurer la confiance et la sécurité dans l'utilisation des TIC, et de déterminer les mesures qui peuvent contribuer à trouver des solutions à ces problèmes;

8 de promouvoir la mise à disposition d'informations sur les autorités nationales de certification et leurs domaines d'activité, ainsi que sur les algorithmes et identifiants qu'elles utilisent, à l'usage des États Membres, des Membres de Secteur et des organisations concernées;

9 de déterminer et de répertorier les mesures concrètes propres à renforcer la sécurité dans l'utilisation des TIC au niveau international, eu égard au concept selon lequel la sécurité est perçue comme un processus continu et itératif, sur la base de pratiques, de lignes directrices et de recommandations largement reconnues, que les États Membres et d'autres parties prenantes pourront choisir d'appliquer pour être mieux à même de lutter contre les cybermenaces et les cyberattaques, notamment en faisant appel à une approche dynamique, itérative et fondée sur les risques qui tienne compte du caractère évolutif des menaces et des vulnérabilités, et de renforcer la coopération internationale pour instaurer la confiance et la sécurité dans l'utilisation des TIC, en tenant compte du Programme GCA de l'UIT, et dans les limites des ressources financières disponibles;

10 d'appuyer les stratégies, l'organisation, la sensibilisation, la coopération, l'évaluation et le perfectionnement des compétences;

11 de fournir l'appui technique et financier nécessaire, dans les limites des ressources budgétaires existantes, conformément à la Résolution 58 (Rév. Dubaï, 2012);

12 d'encourager la participation d'experts aux activités de l'UIT dans le domaine de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

13 de mobiliser des ressources extrabudgétaires appropriées, en dehors du budget ordinaire de l'Union, pour la mise en œuvre de la présente résolution, en vue d'aider les pays en développement;

14 d'aider les pays en développement à promouvoir et à faciliter la mise en œuvre des recommandations UIT-T relatives à la sécurité;

15 d'aider les États Membres à évaluer et à adapter les cadres législatifs et réglementaires en tirant le meilleur parti du rapport sur l'Indice mondial de cybersécurité (GCI) de l'UIT;

16 d'organiser chaque année des séances visant à solliciter des retours d'informations auprès des administrations autorisées des États Membres, afin d'analyser et d'améliorer le processus de calcul de l'Indice GCI,

charge le Secrétaire général

dans le cadre de l'initiative qu'il a prise sur cette question:

1 de soumettre un rapport au Conseil, en tenant compte des activités des trois Secteurs, sur la mise en œuvre et l'efficacité du plan d'action visant à renforcer le rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

2 de coopérer avec les organisations internationales concernées, y compris par le biais de l'adoption de mémorandums d'accord, sous réserve de l'approbation du Conseil à cet égard, conformément à la Résolution 100 (Minneapolis, 1998) de la Conférence de plénipotentiaires,

prie le Conseil de l'UIT

d'inclure le rapport du Secrétaire général dans les documents qui seront envoyés aux États Membres, conformément au numéro 81 de la Convention,

invite les États Membres

1 à envisager de participer à des initiatives internationales et régionales appropriées visant à renforcer les cadres législatifs nationaux qui ont trait à la sécurité des réseaux d'information et de communication;

2 à collaborer étroitement au renforcement de la coopération régionale et internationale, en tenant compte de la Résolution 45 (Rév. Dubaï, 2014), afin d'améliorer la confiance et la sécurité dans l'utilisation des TIC et d'atténuer les risques et les menaces;

3 à appuyer les initiatives de l'UIT en matière de cybersécurité, y compris l'Indice mondial de cybersécurité (GCI), afin de promouvoir les stratégies gouvernementales et de diffuser des informations concernant les mesures prises dans l'ensemble des entreprises et des secteurs;

4 à informer le Secrétaire général des activités menées au titre de la présente résolution concernant la confiance et la sécurité dans l'utilisation des TIC;

5 à exploiter les ressources, l'appui et les bonnes pratiques disponibles dans le cadre des initiatives nationales, régionales et internationales prises dans le monde en matière de cybersécurité au moyen de la page web de l'UIT consacrée à la cybersécurité;

6 à collaborer avec les organisations compétentes, en échangeant de bonnes pratiques sur l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, notamment sur la création et la mise en place d'équipes nationales CIRT;

7 à continuer de mener des activités de sensibilisation pour faire connaître les bonnes pratiques et les politiques qui ont été mises en œuvre, afin d'être mieux à même d'élaborer des politiques adaptées visant à assurer la protection des utilisateurs, de façon à renforcer la confiance dans l'utilisation des télécommunications/TIC,

invite les États Membres, les Membres des Secteurs et les Associés

1 à contribuer aux travaux sur cette question menés par les commissions d'études compétentes de l'UIT ainsi qu'à toute autre activité dont l'Union est responsable;

2 à contribuer à instaurer la confiance et la sécurité dans l'utilisation des TIC aux niveaux national, régional et international, en menant à bien les activités visées dans les documents finals du SMSI, la Déclaration du SMSI+10 sur la mise en œuvre des résultats du SMSI et la Vision du SMSI+10 pour l'après-2015, ainsi que dans le document final de la réunion de haut niveau de l'Assemblée générale sur l'examen d'ensemble de la mise en œuvre des textes issus du SMSI, et à contribuer à la préparation et à la mise en œuvre de ces activités;

3 à mieux faire connaître auprès de toutes les parties prenantes, y compris les organisations et les utilisateurs individuels, l'importance que revêt le renforcement de la cybersécurité, notamment la mise en œuvre de garanties fondamentales;

4 à promouvoir l'élaboration de programmes d'enseignement et de formation pour sensibiliser davantage les utilisateurs aux risques dans le cyberespace et aux mesures qu'ils peuvent prendre pour se protéger;

5 à prendre en considération une approche itérative fondée sur les risques pour faire face à l'évolution des menaces et des vulnérabilités et à promouvoir une culture dans laquelle la sécurité est perçue comme un processus continu et itératif devant être intégré dans le développement et le déploiement des technologies et de leurs applications, dès leur conception et maintenu tout au long de leur cycle de vie, dans le cadre des efforts qu'ils déploient pour instaurer la confiance et la sécurité dans l'utilisation des TIC;

6 à collaborer, s'il y a lieu, afin de résoudre et de prévenir les problèmes qui nuisent à la confiance et à la sécurité dans l'utilisation des télécommunications/TIC.

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

1. 1 Par pays en développement, on entend aussi les pays les moins avancés, les petits Etats insulaires en développement, les pays en développement sans littoral et les pays dont l'économie est en transition. [↑](#footnote-ref-1)