|  |  |  |
| --- | --- | --- |
|  | Assemblée mondiale de normalisation des télécommunications (AMNT-24)New Delhi, 15-24 octobre 2024 |  |
|  |
|  |  |
| SÉANCE PLÉNIÈRE | Addendum 10 auDocument 37-F |
|  | 22 septembre 2024 |
|  | Original: anglais |
|  |
| Administrations des pays membres de la Télécommunauté Asie-Pacifique |
| PROPOSITION DE MODIFICATION DE LA RÉSOLUTION 50 |
|  |
|  |

|  |  |
| --- | --- |
| **Résumé:** | Le présent document contient la proposition de modification de la Résolution 50 de l'AMNT intitulée "Cybersécurité". |
| **Contact:** | M. Masanori KondoSecrétaire généralTélécommunauté Asie-Pacifique | Courriel: aptwtsa@apt.int |

Introduction

La sécurité revêt une importance croissante pour l'infrastructure actuelle des télécommunications/TIC. L'UIT-T a un rôle à jouer dans l'élaboration de Recommandations techniques essentielles visant à renforcer la confiance et la sécurité dans l'utilisation des TIC. Garantir la sécurité au moyen des TIC et assurer la sécurité des TIC sont deux grands sujets d'étude.

La sécurité devrait être prise en considération dans toutes les étapes du cycle de vie d'un système, d'un réseau ou d'une application. À défaut, ce système ou réseau ou cette application présentera de nombreuses failles de sécurité exigeant bon nombre de correctifs.

Étant donné que les activités de normalisation dans le domaine de la sécurité contribuent à prévenir les incidents dus à des cyberactivités malveillantes, il y a lieu de poursuivre les travaux en matière de sécurité. De plus, les commissions d'études de l'UIT-T, en particulier la CE 17, devraient étudier les nouvelles technologies de sécurité qui ont été identifiées, notamment la sécurité de l'intelligence artificielle (IA), la sécurité du métavers, la sécurité zéro confiance, la sécurité des chaînes d'approvisionnement des logiciels, etc.

L'objectif principal des modifications proposées est de préciser et de renforcer le rôle de la CE 17 en tant que commission d'études directrice pour la sécurité.

Proposition

Compte tenu de ce qui précède, les Administrations des pays membres de l'APT proposent que l'AMNT‑24 envisage de réviser la Résolution 50 "Cybersécurité" de l'AMNT.

MOD APT/37A10/1

RÉSOLUTION 50 (Rév. New Delhi, 2024)

Cybersécurité

(Florianópolis, 2004; Johannesburg, 2008; Dubaï, 2012; Hammamet, 2016; Genève, 2022; New Delhi, 2024)

L'Assemblée mondiale de normalisation des télécommunications (New Delhi, 2024),

rappelant

*a)* la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires, sur le 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 (TIC);

*b)* la Résolution 174 (Rév. Dubaï, 2018) 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;

*c)* la Résolution 179 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires, sur le rôle de l'UIT dans la protection en ligne des enfants;

*d)* la Résolution 181 (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;

*e)* les Résolutions 55/63 et 56/121 de l'Assemblée générale des Nations Unies, par lesquelles a été établi le cadre juridique pour la lutte contre l'exploitation des technologies de l'information à des fins criminelles;

*f)* la Résolution 57/239 de l'Assemblée générale des Nations Unies, relative à la création d'une culture mondiale de la cybersécurité;

*g)* la Résolution 58/199 de l'Assemblée générale des Nations Unies, relative à la création d'une culture mondiale de la cybersécurité et à la protection des infrastructures essentielles de l'information;

*h)* la Résolution 68/167 de l'Assemblée générale des Nations Unies, relative au droit à la vie privée à l'ère du numérique, dans laquelle l'Assemblée, entre autres dispositions, affirme que "les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne, y compris le droit à la vie privée";

*i)* la Résolution 41/65 de l'Assemblée générale des Nations Unies, relative aux principes concernant la télédétection de la Terre depuis l'espace extra-atmosphérique;

*j)* la Résolution 70/125 de l'Assemblée générale des Nations Unies – "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";

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

*l)* la Résolution 52 (Rév. Hammamet, 2016) de l'Assemblée mondiale de normalisation des télécommunications, "Lutter contre le spam";

*m)* la Résolution 58 (Rév. Genève, 2022) de la présente Assemblée, "Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement[[1]](#footnote-1)1";

*n)* que l'UIT joue le rôle de coordonnateur principal pour la grande orientation C5 de l'Agenda de Tunis pour la société de l'information (Établir la confiance et la sécurité dans l'utilisation des TIC) adopté par le SMSI;

*o)* les dispositions des résultats du SMSI relatives à la cybersécurité,

considérant

*a)* l'importance cruciale que revêt l'infrastructure des télécommunications/TIC et ses applications pour pratiquement toutes les formes d'activités sociales et économiques;

*b)* que le réseau téléphonique public commuté traditionnel présente un certain niveau de sécurité intrinsèque du fait de sa structure hiérarchisée et de ses systèmes de gestion intégrés;

*c)* que les réseaux utilisant le protocole Internet (IP) n'assurent qu'une séparation réduite entre les éléments utilisateurs et les éléments réseaux si on n'accorde pas le soin voulu à la conception et à la gestion de la sécurité;

*d)* que les réseaux traditionnels et les réseaux IP post-convergence sont donc potentiellement plus vulnérables à l'intrusion si on n'accorde pas le soin voulu à la conception et à la gestion de la sécurité de ces réseaux;

*e)* que la question de la cybersécurité est intersectorielle, et que l'environnement de la cybersécurité est complexe et diversifié, et compte de nombreuses parties prenantes différentes aux niveaux national, régional et mondial chargées d'identifier, d'examiner et de résoudre les problèmes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

*f)* que les pertes considérables et toujours plus importantes que les utilisateurs de systèmes de télécommunication/TIC ont subies en raison du problème toujours plus préoccupant de la cybercriminalité alarment tous les pays développés et les pays en développement du monde, sans exception;

*g)* que le fait, notamment, que les infrastructures essentielles des télécommunications/TIC sont interconnectées au niveau mondial signifie qu'une sécurité insuffisante des infrastructures dans un pays pourrait entraîner une vulnérabilité et des risques accrus dans d'autres pays, d'où l'importance de la coopération;

*h)* que le nombre de cybermenaces et de cyberattaques et les méthodes correspondantes sont en augmentation, tout comme la dépendance à l'égard de l'Internet et d'autres réseaux qui sont essentiels pour accéder aux services et à l'information;

*i)* que les normes peuvent prendre en compte les aspects liés à la sécurité de l'Internet des objets (IoT) et des villes et des communautés intelligentes, y compris les aspects liés à la sécurité des technologies nouvelles et émergentes;

*j)* que, pour protéger les infrastructures mondiales de télécommunication/TIC contre les menaces et les risques liés à l'évolution de l'environnement de la cybersécurité, il est nécessaire de prendre des mesures concertées au niveau national, régional et international, pour la prévention, la préparation, l'intervention et le rétablissement en cas d'incidents liés à la cybersécurité;

*k)* les travaux déjà entrepris et en cours à l'UIT, notamment au sein de la Commission d'études 17 du Secteur de la normalisation des télécommunications de l'UIT (UIT-T) et de la Commission d'études 2 du Secteur du développement des télécommunications (UIT-D), y compris le rapport final de la Commission d'études 1 de l'UIT-D au titre de la Question 22/1, et dans le cadre du Plan d'action de Dubaï, adopté par la CMDT (Dubaï, 2014);

*l)* que l'UIT-T a un rôle à jouer dans le cadre de son mandat et de ses compétences en ce qui concerne le point *j)* du *considérant*,

considérant en outre

*a)* que la Recommandation UIT-T X.1205 établit une définition, une description des technologies et les principes de protection des réseaux en matière de cybersécurité;

*b)* que la Recommandation UIT-T X.805 établit un cadre systématique pour déterminer les failles de sécurité, que la Recommandation UIT-T X.509 traite du cadre général des certificats de clé publique et d'attribut et que la Recommandation UIT-T X.1500 donne un modèle d'échange d'informations sur la cybersécurité (CYBEX) et porte sur les techniques qui pourraient être utilisées pour faciliter l'échange d'informations sur la cybersécurité;

*c)* que la Recommandation UIT-T X.1060 établit un cadre permettant aux organisations de mettre en place et de gérer un centre de cyberdéfense (CDC) pour garantir leur propre sécurité, d'évaluer l'efficacité de ce centre pour la mise en œuvre des services de sécurité et de remédier aux risques associés en matière de cybersécurité;

*d)* que l'UIT-T et le Comité technique mixte pour les technologies de l'information (JTC 1) de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI), ainsi que plusieurs consortiums et entités de normalisation comme le World Wide Web consortium (W3C), l'Organization for Advancement of Structured Information Standards (OASIS), l'Alliance FIDO (Fast IDentity Online), le Groupe de travail sur l'ingénierie Internet et l'Institut des ingénieurs en électricité et en électronique, notamment, disposent déjà d'un important volume de documents publiés et ont des travaux en cours qui se rapportent directement à ce sujet, dont il faut tenir compte;

*e)* l'importance des travaux en cours sur une architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique,

reconnaissant

*a)* le paragraphe du dispositif de la Résolution 130 (Rév. Bucarest, 2022) chargeant le Directeur du TSB d'intensifier les travaux menés au sein des Commissions d'études existantes de l'UIT-T;

*b)* que, par sa Résolution 71 (Rév. Bucarest, 2022), la Conférence de plénipotentiaires a adopté le Plan stratégique pour la période 2024-2027, qui comprend le But stratégique 1 (Connectivité universelle: favoriser et encourager l'accès universel, à un coût abordable, à des télécommunications/TIC sûres et de qualité), au titre duquel l'Union s'emploiera à offrir une infrastructure, des services et des applications de télécommunication/technologies de l'information et des communications (TIC) accessibles à tous, de qualité, interopérables et sûrs, à un coût abordable;

*c)* que le Programme mondial cybersécurité (GCA) de l'UIT encourage la coopération internationale dans le but de proposer des stratégies en vue de l'élaboration de solutions propres à accroître la confiance et la sécurité dans l'utilisation des TIC, compte tenu des aspects liés à la sécurité à toutes les étapes du processus d'élaboration des normes;

*d)* les problèmes auxquels les États, en particulier ceux des pays en développement, sont confrontés pour instaurer la confiance et la sécurité dans l'utilisation des TIC, et la Résolution 44 (Rév. Genève, 2022) de l'AMNT relative à la réduction de l'écart en matière de normalisation entre pays en développement et pays développés;

*e)* les difficultés que les États Membres, en particulier les pays en développement, connaissent pour créer des infrastructures et des applications de télécommunication/TIC fiables et sûres pour les aspects techniques et opérationnels de la protection des données et des informations d'identification personnelle (PII),

reconnaissant en outre

*a)* que des cyberattaques, telles que le hameçonnage, le spam, le détournement d'adresses, le balayage/l'intrusion, les dénis de services distribués, les menaces persistantes avancées, le détournement de sites web, l'accès non autorisé, les logiciels malveillants, l'empoisonnement des données, l'usurpation d'identité, etc., apparaissent et ont de graves conséquences;

*b)* que des réseaux zombis sont utilisés pour distribuer des logiciels malveillants et mener des cyberattaques;

*c)* que l'origine des attaques est parfois difficile à identifier;

*d)* que les menaces très importantes qui pèsent sur la cybersécurité des logiciels et des matériels nécessiteront peut‑être une gestion des failles en temps voulu, l'actualisation des logiciels ou des matériels en temps utile et l'attribution des droits d'accès appropriés, pour prévenir les attaques contre les dispositifs terminaux;

*e)* que le nombre d'attaques par rançongiciel continue de croître;

*f)* que l'application des nouvelles technologies combinée à l'évolution permanente des infrastructures mondiales de télécommunication/TIC pose de nouveaux défis et nécessite des exigences plus élevées concernant la sécurité des télécommunications/TIC et les aspects techniques et opérationnels de la protection des données et des informations PII, ce qui peut avoir des incidences sur l'architecture de sécurité du réseau;

*g)* l'évolution des technologies utilisées pour gérer les menaces de cybersécurité et assurer la protection des télécommunications/TIC;

*h)* qu'il est nécessaire de renforcer les capacités de sécurité, y compris les capacités du personnel en matière de gestion des risques de sécurité et des technologies de sécurité;

*i)* que la sécurisation des données et de l'infrastructure des mégadonnées est un élément essentiel de la cybersécurité dans la mesure où les données sont souvent la cible des cyberattaques, tandis que le large champ d'application de la technologie des mégadonnées en fait une cible permanente compte tenu du comportement des réseaux à l'heure actuelle;

*j)* que la cybersécurité est un élément essentiel pour instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC;

*k)* que la sécurité occupe une place importante tout au long du cycle de vie des systèmes, réseaux, applications ou données;

*l)* que l'architecture et le cadre de sécurité sont importants et que l'on pourrait considérer que c'est sur cette base que devraient être conçues les architectures de sécurité pour les différents systèmes, réseaux, applications et données,

notant

*a)* l'activité et l'intérêt marqués pour l'élaboration de normes et de Recommandations sur la sécurité des télécommunications/TIC au sein de la Commission d'études 17, qui est la commission d'études directrice pour la sécurité et la gestion d'identité, et au sein d'autres organismes de normalisation, y compris le Groupe de collaboration pour la normalisation mondiale (GSC);

*b)* qu'il conviendrait d'évaluer les aspects liés à l'interopérabilité et à la sécurité en ce qui concerne l'évolution de l'infrastructure de réseau et l'accélération de l'innovation en matière de développement de l'infrastructure de réseau ouvert;

*c)* qu'en plus des autres menaces de cybersécurité, les aspects techniques et opérationnels de la protection des données et des informations PII revêtent désormais une grande importance pour les États Membres;

*d)* qu'il est nécessaire d'harmoniser les stratégies et initiatives nationales, régionales et internationales dans toute la mesure du possible pour éviter les doubles emplois et optimaliser l'utilisation des ressources;

*e)* les efforts de collaboration importants déployés par et entre les gouvernements, le secteur privé, la société civile, les milieux techniques et universitaires, dans le cadre de leurs rôles et de leurs responsabilités, pour instaurer la confiance et la sécurité dans l'utilisation des TIC,

décide

1 de continuer d'accorder à ces travaux un rang de priorité élevé à l'UIT-T, 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 que toutes les commissions d'études de l'UIT-T doivent continuer à évaluer les Recommandations existantes et les nouvelles Recommandations en cours d'élaboration, conformément à leurs mandats définis dans la Résolution 2 (Rév. Genève, 2022) de l'AMNT et en tenant compte des aspects de sécurité tout au long du processus d'élaboration des normes de l'UIT‑T, quant à la robustesse de leur conception et de leur utilisation et aux risques d'une exploitation par des acteurs malveillants, et tenir compte des services et des technologies de télécommunication/TIC nouveaux et émergents qui seront pris en charge par l'infrastructure mondiale des télécommunications/TIC (y compris, mais non exclusivement, par exemple, l'informatique en nuage et l'Internet des objets (IoT), qui sont fondés sur les réseaux de télécommunication/TIC);

3 que l'UIT-T, dans le cadre de son mandat et de ses compétences, doit continuer à sensibiliser l'opinion à l'échelle mondiale sur la sécurité des TIC en élaborant des Recommandations et des rapports techniques à l'appui des procédures, des politiques techniques et des cadres relatifs à la cybersécurité, et sur la nécessité de renforcer et de défendre les systèmes d'information et de télécommunication contre les cybermenaces et les cyberactivités malveillantes, à renforcer les capacités du personnel en matière de sécurité et à promouvoir la coopération entre les organisations internationales et régionales appropriées afin de renforcer l'échange d'informations techniques dans le domaine de la sécurité des réseaux d'information et de télécommunication;

4 que l'UIT-T devrait sensibiliser l'opinion à l'échelle mondiale en ce qui concerne la sécurité des TIC, en élaborant des Recommandations et des rapports techniques pour appuyer les procédures, les politiques techniques et les cadres en matière de cybersécurité, dans le but de mieux gérer les risques de cybersécurité et de protéger les réseaux d'information et de télécommunication;

5 que l'UIT-T devrait travailler en collaboration avec l'UIT-D, en particulier dans le contexte de la Question 3/2 de l'UIT-D (Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité);

6 que les commissions d'études concernées de l'UIT-T devront suivre le rythme de l'évolution des technologies nouvelles et émergentes, compte tenu de leurs mandats, pour appeler l'attention de la CE 17 sur les domaines dans lequel il peut y avoir lieu d'élaborer de nouvelles Recommandations et de nouveaux Suppléments et rapports techniques permettant de traiter les enjeux que posent ces technologies sur le plan de la sécurité ainsi que les aspects techniques et opérationnels de la protection des données et des informations PII;

7 que l'UIT-T doit poursuivre ses travaux sur l'élaboration et l'amélioration des termes et définitions relatifs à l'instauration de la confiance (notamment via la protection des données et des informations d'identification personnelle) et de la sécurité dans l'utilisation des télécommunications/TIC, y compris en ce qui concerne la cybersécurité;

8 que l'adoption de procédures mondiales, cohérentes et interopérables pour échanger des informations sur les mesures prises en cas d'incident doit être encouragée;

9 que les commissions d'études de l'UIT-T doivent continuer d'assurer la liaison avec les organisations de normalisation et d'autres organismes travaillant dans ce domaine et 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;

10 que des réseaux et des services de télécommunication/TIC sécurisés, résilients et fiables devront être conçus et exploités afin de renforcer la confiance dans l'utilisation des télécommunications/TIC;

11 qu'il est nécessaire que la Commission d'études 17 procède à une analyse de la cybersécurité fondée sur la coopération et élabore des cadres de gestion des incidents;

12 que la résilience des réseaux et des systèmes TIC devra être considérée comme une priorité dans le développement des réseaux, des infrastructures et des applications de télécommunication/TIC,

charge la Commission d'études 17

1 d'encourager les études relatives à la cybersécurité, notamment en ce qui concerne la sécurité et les aspects techniques et opérationnels des données et des informations PII pour les services et les technologies nouveaux et émergents, afin de lutter contre les failles liées à l'utilisation de l'infrastructure mondiale des télécommunications/TIC moyennant l'élaboration de Recommandations, de Suppléments et de rapports techniques, selon qu'il conviendra;

2 d'aider le Directeur du TSB à tenir à jour la "Feuille de route relative aux normes de sécurité des TIC", qui devrait comprendre des sujets d'étude visant à faire progresser les travaux de normalisation relatifs à la sécurité et les aspects techniques et opérationnels de la protection des données et des informations PII, ainsi que le registre sur la sécurité, qui devrait comprendre une liste de Recommandations et de termes et définitions, et de les communiquer, en sa qualité de commission d'études directrice pour la sécurité, aux commissions d'études concernées du Secteur des radiocommunications de l'UIT (UIT-R) et de l'UIT-D;

3 d'encourager les activités conjointes de coordination sur la confiance et la sécurité entre toutes les commissions d'études et tous les groupes spécialisés concernés de l'UIT et les autres organisations de normalisation, y compris l'Activité conjointe de coordination sur la protection en ligne des enfants et son analyse des lacunes;

4 de collaborer étroitement avec toutes les autres commissions d'études de l'UIT-T, d'élaborer un plan d'action visant à examiner les Recommandations UIT-T existantes, en cours d'élaboration ou nouvelles, pour lutter contre les menaces et les failles de sécurité en constante évolution, afin de garantir la résilience des réseaux de TIC contre les cyberattaques et de continuer de faire rapport périodiquement sur la sécurité des télécommunications/TIC au Groupe consultatif de la normalisation des télécommunications;

5 de continuer de définir un ensemble commun ou général de capacités de sécurité pour chaque étape du cycle de vie des systèmes d'information, réseaux ou applications, y compris concernant le développement des capacités du personnel en matière de sécurité, afin que la sécurité au stade de la conception (capacités et fonctionnalités de sécurité prévues dès la conception) soit assurée pour les systèmes, réseaux ou applications dès le premier jour;

6 de poursuivre la conception d'un ou de plusieurs cadres ou d'architectures de référence dotés d'éléments fonctionnels de sécurité, compte tenu notamment de la collaboration entre différents types de systèmes à des fins de sécurité, qui pourraient être considérés comme les bases de la conception d'architectures de sécurité pour différents systèmes, réseaux ou applications, afin d'améliorer la qualité des Recommandations relatives à la sécurité, et de fournir des références en matière de conception de sécurité pour les applications possibles des technologies émergentes dans l'infrastructure mondiale des télécommunications/TIC;

7 de prendre en considération l'évolution constante des technologies et des activités commerciales dans le domaine des TIC, d'examiner régulièrement les Recommandations relatives à la sécurité des réseaux et de réviser les Recommandations existantes afin de les adapter aux nouvelles exigences de sécurité et de répondre aux nouvelles menaces qui pèsent sur la sécurité des réseaux;

8 de proposer des bonnes pratiques pour l'évaluation et l'amélioration de la sécurité ainsi que des aspects techniques et opérationnels de la protection des données et des informations PII, compte tenu de l'évolution de l'infrastructure des télécommunications/TIC,

charge le Directeur du Bureau de la normalisation des télécommunications

1 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 télécommunications/TIC" et des efforts consacrés par l'UIT-D à la cybersécurité, et avec l'assistance d'autres organisations compétentes, un inventaire des initiatives et activités nationales, régionales et internationales pour promouvoir, dans toute la mesure possible, l'harmonisation à l'échelle mondiale des stratégies et méthodologies dans ce domaine d'une importance cruciale, notamment par l'élaboration d'approches communes dans le domaine de la cybersécurité;

2 de contribuer à l'élaboration des rapports annuels à l'intention du Conseil de l'UIT sur l'instauration de la confiance et de la sécurité dans l'utilisation des télécommunications/TIC, comme indiqué dans la Résolution 130 (Rév. Bucarest, 2022);

3 de soumettre au Conseil un rapport sur l'état d'avancement des activités menées au titre de la "Feuille de route pour la normalisation de la sécurité des télécommunications/TIC";

4 de continuer de reconnaître le rôle que jouent d'autres organisations possédant une expérience et des compétences dans le domaine des normes relatives à la sécurité, à la protection des données et aux informations PII et d'assurer une coordination avec ces organisations, selon qu'il conviendra;

5 de continuer d'assurer la mise en œuvre et le suivi des activités pertinentes du SMSI relatives à l'instauration de la confiance et de la sécurité dans l'utilisation des télécommunications/TIC, en collaboration avec les autres Secteurs de l'UIT et en coopération avec les parties prenantes compétentes, en vue de partager des informations et des bonnes pratiques au plan mondial sur les initiatives en matière de cybersécurité nationales, régionales et internationales, et non discriminatoires;

6 de coopérer avec le Programme mondial cybersécurité (GCA) du Secrétaire général et d'autres projets de portée mondiale ou régionale dans le domaine de la cybersécurité, selon qu'il conviendra, pour encourager le renforcement des capacités et nouer des relations et des partenariats avec diverses organisations et initiatives régionales ou internationales liées à la cybersécurité selon qu'il conviendra, et d'inviter tous les États Membres, en particulier les pays en développement, à participer à ces activités et à assurer une coordination et une coopération entre ces différentes activités;

7 d'apporter un appui au Directeur du Bureau de développement des télécommunications (BDT), en vue d'aider les États Membres à mettre en place un cadre approprié entre les pays en développement, permettant de réagir rapidement à des incidents majeurs et de proposer un plan d'action destiné à renforcer leur protection, compte tenu des mécanismes et des partenariats, selon le cas;

8 d'appuyer les activités menées par les commissions d'études concernées de l'UIT‑T pour ce qui est du renforcement et de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

9 de diffuser auprès de toutes les parties prenantes des informations sur la cybersécurité et d'améliorer leur compréhension de ce domaine, en organisant des programmes de formation, des forums, des ateliers, des séminaires, etc., selon qu'il convient, sur les Recommandations UIT-T et les lignes directrices relatives à la mise en œuvre, à l'intention des décideurs, des régulateurs, des opérateurs et d'autres parties prenantes, en particulier dans les pays en développement;

10 d'envisager, chaque fois que cela est possible, de sensibiliser l'opinion en organisant des ateliers en même temps que les réunions des groupes régionaux concernés des commissions d'études de l'UIT-T, ou en tenant des manifestations parallèlement à ces réunions, en coordination et en collaboration avec le Directeur du BDT et les bureaux régionaux de l'UIT,

invite les États Membres, les Membres de Secteur, les Associés et les établissements universitaires, selon qu'il conviendra

1 à travailler en étroite collaboration en vue de renforcer la coopération aux niveaux régional et international, en tenant compte de la Résolution 130 (Rév. Bucarest, 2022), en vue de renforcer la confiance et la sécurité dans l'utilisation des télécommunications/TIC, de façon à réduire les risques et faire face aux menaces;

2 à coopérer et à participer activement à la mise en œuvre de la présente Résolution et des mesures connexes;

3 à participer aux activités menées par les commissions d'études concernées de l'UIT-T pour élaborer des normes et des lignes directrices en matière de cybersécurité, afin d'instaurer la confiance et la sécurité dans l'utilisation des TIC;

4 à utiliser les Recommandations, les rapports techniques et les Suppléments pertinents de l'UIT-T;

5 à continuer de contribuer aux travaux de la Commission d'études 17 concernant les méthodes de gestion des risques de cybersécurité et de la cyberdéfense.

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

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