ITUPublications
Résolutions

Union internationale des télécommunications
Secteur de la normalisation

ASSEMBLÉE MONDIALE DE NORMALISATION DES TÉLÉCOMMUNICATIONS
New Delhi, 15-24 octobre 2024

Résolution 50 – Cybersécurité

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

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. 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;

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 64/211 de l'Assemblée générale des Nations Unies, relative à la création d'une culture mondiale de la cybersécurité et à l'évaluation des efforts nationaux visant à protéger les infostructures essentielles;

h) 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;

i) la Résolution 76/19 de l'Assemblée générale des Nations Unies, intitulée "Progrès de l'informatique et des télécommunications et sécurité internationale, et promotion du comportement responsable des États dans l'utilisation du numérique";

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. Kigali, 2022) 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. New Delhi, 2024) de la présente Assemblée, intitulée "Lutter contre le spam";

m) la Résolution 58 (Rév. New Delhi, 2024) de la présente Assemblée, "Encourager la création et le renforcement d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement[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 Sommet mondial sur la société de l'information (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 télécommunications/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 toutes les télécommunications/TIC;

j) qu'il est essentiel de garantir la sûreté et la sécurité des télécommunications/TIC émergentes pour assurer la sécurité du cyberespace, d'où la nécessité d'élaborer des normes de sécurité pour ces technologies;

---

[1] Par pays en développement, on entend 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.

k) 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;

l) 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), et dans le cadre du Plan d'action de Kigali, adopté par la CMDT (Kigali, 2022);

m) 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 *k)* du *considérant* de la présente Résolution,

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;

b) que la Recommandation UIT-T X.805 établit un cadre systématique pour déterminer les failles de sécurité 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 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, 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;

d) qu'il importe de considérer que la sécurité dans le cadre de l'utilisation des télécommunications/TIC est un processus continu et itératif, intégré aux produits dès le départ et se poursuivant à chaque étape de leur cycle de vie;

e) qu'une approche itérative fondée sur les risques et intégrant à la fois des facteurs propres aux technologies, aux processus et à l'humain est essentielle pour renforcer la sécurité et la résilience en ce qui concerne l'utilisation des télécommunications/TIC, en ce qu'elle permet d'élaborer et d'appliquer des pratiques en matière de cybersécurité selon les besoins, afin de faire face à l'évolution constante des menaces et des vulnérabilités, tout en favorisant également l'innovation et les télécommunications/TIC émergentes,

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 de l'Union 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 en priorité à offrir une infrastructure, des services et des applications de télécommunication/TIC accessibles à tous, de qualité, interopérables et sûrs, à un coût abordable;

c) que les normes sont une composante essentielle du Pilier 2 (Mesures techniques et de procédure) du Programme mondial cybersécurité (GCA) de l'UIT, qui 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 télécommunications/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 télécommunications/TIC,

reconnaissant en outre

a) que des cyberattaques, dont l'ampleur et la diversité ne cessent de croître, telles que l'hameçonnage, le détournement d'adresses, le balayage/l'intrusion, les dénis de services distribués, le détournement de sites web et l'accès non autorisé, apparaissent, évoluent et ont d'importantes conséquences;

b) que plusieurs vecteurs peuvent être 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;

e) que la sécurisation des données est un élément essentiel de la cybersécurité dans la mesure où les données sont souvent la cible des cyberattaques;

f) que la cybersécurité est un élément fondamental qui permet d'instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC;

g) la généralisation croissante de l'accès aux télécommunications/TIC dans le monde entier, en particulier à l'Internet, et de leur utilisation par des personnes mineures,

notant

a) l'activité et l'intérêt marqués pour l'élaboration de normes et de Recommandations UIT-T sur la sécurité des télécommunications/TIC au sein de la Commission d'études 17 de l'UIT-T, 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;

b) 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;

c) qu'en plus des autres menaces de cybersécurité, les aspects de cybersécurité liés à la protection des données et aux informations d'identification personnelle (PII) revêtent désormais une grande importance pour les États Membres;

d) 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 télécommunications/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 télécommunications/TIC aux niveaux national, régional et international;

2 que les commissions d'études de l'UIT-T doivent, conformément à leurs mandats définis dans la Résolution 2 (Rév. New Delhi, 2024) de la présente Assemblée, continuer à évaluer les Recommandations UIT-T existantes et les Recommandations UIT-T en cours d'élaboration et soumettre à la Commission d'études 17 de l'UIT-T, pour examen, les questions de sécurité touchant à la robustesse de conception et de fonctionnement, 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 assurés par l'infrastructure mondiale des télécommunications/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 en ce qui concerne la sécurité des télécommunications/TIC en élaborant des Recommandations UIT-T et des rapports techniques à l'appui des procédures, des politiques techniques et des cadres normatifs liés à la cybersécurité, et en ce qui concerne l'importance que revêt la protection des télécommunications/TIC contre les cybermenaces et les cyberactivités malveillantes, afin de renforcer les capacités du personnel des organisations en matière de sécurité, et 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 télécommunications/TIC, dans le but de gérer les risques de cybersécurité et de protéger les télécommunications/TIC;

4 que l'UIT-T devrait prendre en compte les besoins des utilisateurs et des développeurs lors de l'élaboration de produits pouvant être utilisés pour promouvoir la cybersécurité des technologies émergentes liées aux télécommunications/TIC;

5 que l'UIT-T devrait tenir compte de l'importance du renforcement des capacités pour faciliter l'adoption de normes permettant de promouvoir la cybersécurité, en particulier pour les pays en développement, mais pas uniquement;

6 que l'UIT-T devrait travailler en coordination et en collaboration avec l'UIT-D à cet égard, tant 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) que dans celui des activités de renforcement des capacités menées par le Bureau de développement des télécommunications (BDT);

7 que les commissions d'études concernées de l'UIT-T devront suivre le rythme de l'évolution des technologies et services de télécommunication/TIC nouveaux et émergents, compte tenu de leurs mandats, pour informer la Commission d'études 17 de l'UIT-T des domaines qui pourraient nécessiter de nouvelles Recommandations UIT-T, de nouveaux Suppléments et de nouveaux rapports techniques en vue de surmonter les difficultés relatives à la cybersécurité et à ses aspects concernant la protection des données et des informations PII;

8 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 et de la sécurité dans l'utilisation des télécommunications/TIC, y compris en ce qui concerne le terme "cybersécurité";

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

10 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 télécommunications/TIC;

11 que les aspects liés à la sécurité devront être pris en considération tout au long du processus d'élaboration des normes de l'UIT-T;

12 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;

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

charge la Commission d'études 17 du Secteur de la normalisation des télécommunications de l'UIT

1 d'encourager les études relatives à la cybersécurité, notamment en ce qui concerne les aspects liés à la protection des données et des informations PII des services et technologies de télécommunication/TIC 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 UIT-T, 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 cybersécurité et à ses aspects concernant la protection des données et des informations PII, ainsi que le Recueil sur la sécurité, qui devrait comprendre la liste des Recommandations UIT-T ainsi que des termes et des définitions, et de les communiquer, en sa qualité de commission d'études directrice de l'UIT-T pour la sécurité, aux commissions d'études concernées du Secteur des radiocommunications de l'UIT et de l'UIT-D;

3 de diriger des activités conjointes de coordination sur la confiance et la sécurité entre toutes les commissions d'études de l'UIT et les autres organisations de normalisation, selon qu'il conviendra;

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 promouvoir la résilience des réseaux de télécommunication/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 au cours de chaque étape du cycle de développement, notamment les prescriptions, la conception, la mise en œuvre, la vérification, la commercialisation et la maintenance, des produits de type systèmes d'information, réseaux, applications ou services, y compris le renforcement des capacités du personnel des organisations 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 continuer de concevoir un ou plusieurs cadres de sécurité ou architectures de référence dotés d'éléments fonctionnels de sécurité, y compris en tenant compte de l'interopérabilité en matière de sécurité des différents types de systèmes, 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 UIT-T relatives à la sécurité, et de fournir des références en matière de conception de la sécurité pour des applications éventuelles dans l'infrastructure mondiale des télécommunications/TIC;

7 de continuer d'élaborer et de promouvoir l'analyse de la cybersécurité fondée sur la coopération et les outils de gestion des incidents, afin de soutenir les travaux des équipes nationales d'intervention en cas d'incident informatique (CIRT), en particulier dans les pays en développement;

8 d'envisager de répondre aux exigences, au fur et à mesure qu'elles seront établies, afin d'élaborer des normes techniques à l'appui des efforts visant à renforcer la cybersécurité des mineurs;

9 de prendre en considération l'évolution constante des télécommunications/TIC, d'examiner régulièrement et de réviser les Recommandations UIT-T existantes relatives à la sécurité des réseaux, afin de les adapter aux nouvelles exigences de sécurité et de répondre aux nouvelles menaces qui pèsent sur la sécurité des réseaux;

10 de proposer des bonnes pratiques pour l'évaluation et l'amélioration de la cybersécurité, y compris ses aspects concernant la protection des données et des informations PII, compte tenu de l'évolution de l'infrastructure des télécommunications/TIC;

11 de procéder à une évaluation des incidences des télécommunications/TIC nouvelles et émergentes, sous l'angle de la cybersécurité, en recensant les lacunes en la matière et en prônant des stratégies en vue de leur adoption et leur utilisation en toute sécurité,

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 de cybersécurité, y compris, entre autres, les aspects de la cybersécurité concernant la protection des données et des 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 d'autres organisations et toutes 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 BDT, en vue de superviser l'élaboration de Recommandations UIT-T et éventuellement d'autres outils que les États Membres, en particulier les pays en développement, peuvent utiliser pour se préparer à réagir rapidement en cas d'incidents majeurs et d'aider ces organismes à proposer des plans d'action au moyen d'un cadre approprié, selon le cas et sur demande, afin de renforcer leur protection, compte tenu des mécanismes et des partenariats;

8 d'appuyer les activités menées par la Commission d'études 17 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 télécommunications/TIC, et de coordonner ces activités avec celles des commissions d'études de l'UIT-D ainsi qu'avec les activités menées au titre des programmes pertinents;

9 de diffuser auprès de toutes les parties prenantes des informations sur la cybersécurité et de renforcer la compréhension des parties prenantes en la matière, en organisant des programmes de formation, des forums, des ateliers, des séminaires, etc., selon qu'il conviendra, sur les Recommandations UIT-T et les directives de mise en œuvre, à l'intention des décideurs, des régulateurs, des opérateurs et d'autres parties prenantes, en particulier dans les pays en développement, afin d'accroître la sensibilisation et de recenser les besoins, en collaboration avec le Directeur du BDT;

10 de collaborer avec les organisations régionales de télécommunication pour diffuser plus efficacement des connaissances et des compétences spécialisées auprès d'un public plus large;

11 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, le cas échéant,

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 et le soutien 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 à 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 télécommunications/TIC;

4 à utiliser les Recommandations UIT-T, rapports techniques et Suppléments pertinents;

5 à continuer de contribuer aux travaux de la Commission d'études 17 de l'UIT-T concernant les méthodes de gestion des risques de cybersécurité et de la cyberdéfense, dans le cadre des attributions de l'UIT;

6 à continuer de prendre part aux initiatives visant à encourager la participation active des femmes aux activités et aux fonctions de direction de l'UIT-T relatives à la cybersécurité;

7 à adopter et à appuyer la mise en œuvre de mesures de cybersécurité pour les télécommunications/TIC nouvelles et émergentes dans leur juridiction respective, en promouvant un environnement sûr et résilient pour tous les utilisateurs.