

RÉSOLUTION 45 (Rév. Bakou, 2025)

Mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam

La Conférence mondiale de développement des télécommunications (Bakou, 2025),

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)* la Résolution 50 (Rév. New Delhi, 2024) de l'Assemblée mondiale de normalisation des télécommunications (AMNT) relative à la cybersécurité;
- f)* la Résolution 52 (Rév. New Delhi, 2024) de l'AMNT relative à la lutte contre le spam;
- g)* la Résolution 58 (Rév. New Delhi, 2024) de l'AMNT, sur l'action à mener pour encourager la création et le renforcement d'équipes nationales d'intervention en cas d'incident informatique (CIRT), en particulier pour les pays en développement¹;
- h)* la Résolution 69 (Rév. Bakou, 2025) de la présente Conférence, sur la manière de faciliter la création d'équipes CIRT, en particulier pour les pays en développement, et la coopération entre ces équipes;
- i)* la Résolution 67 (Rév. Bakou, 2025) de la présente Conférence sur le rôle du Secteur du développement des télécommunications de l'UIT (UIT-D) dans la protection en ligne des enfants;

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.

- j)* la Résolution 214 (Bucarest, 2022) de la Conférence de plénipotentiaires relative aux technologies fondées sur l'intelligence artificielle (IA) et sur les télécommunications/TIC, qui définit le cadre dans lequel le Directeur du Bureau de développement des télécommunications (BDT) peut appuyer les travaux de l'UIT-D visant à relever les défis et à saisir les possibilités que représente l'IA en tant que technologie nouvelle et émergente, appliquée à la cybersécurité et à la lutte contre le spam;
- k)* les avis pertinents du sixième Forum mondial des politiques de télécommunication qui relèvent du mandat de l'UIT-D;
- l)* les nobles principes, buts et objectifs énoncés dans la Charte des Nations Unies et dans la Déclaration universelle des droits de l'homme;
- m)* que l'UIT joue le rôle de coordonnateur principal de 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);
- n)* les dispositions de l'Engagement de Tunis et de l'Agenda de Tunis du SMSI relatives à la cybersécurité;
- o)* les priorités thématiques énoncées dans le Plan stratégique de l'Union en vigueur;
- p)* la Déclaration de principes de Genève adoptée par le SMSI, qui indique au paragraphe 37 que "le spam est un problème important et qui ne cesse de s'aggraver pour les utilisateurs, les réseaux et l'Internet dans son ensemble et que les questions relatives au spam et à la cybersécurité devraient être traitées aux niveaux national et international appropriés";
- q)* la Question 3/2 de l'UIT-D, intitulée "Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité";
- r)* le rapport du Président du Groupe d'experts de haut niveau pour le Programme mondial cybersécurité (GCA), établi par le Secrétaire général de l'UIT en application de la grande orientation C5 du SMSI, "Établir la confiance et la sécurité dans l'utilisation des TIC", et conformément à la Résolution 140 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires sur le rôle de l'UIT en tant que coordonnateur principal pour la grande orientation C5 du SMSI ainsi qu'à la Résolution 58 (Rév. New Delhi, 2024) de l'AMNT, sur l'action à mener pour encourager la création et le renforcement d'équipes CIRT nationales, en particulier pour les pays en développement;

s) que le Conseil de l'UIT a approuvé, à sa session de 2022, des lignes directrices relatives à l'utilisation du Programme GCA par l'UIT dans le cadre de ses travaux;

t) que l'UIT et l'Office des Nations Unies contre la drogue et le crime ont signé un Mémoire d'accord, afin de renforcer la sécurité dans l'utilisation des TIC;

u) le Pacte numérique mondial, adopté en tant qu'Annexe I de la Résolution 79/1 de l'Assemblée générale des Nations Unies, dans lequel sont définis des objectifs, des principes, des engagements et des mesures en lien avec la transformation numérique²,

considérant

a) le rôle que jouent les télécommunications/TIC en tant qu'outils efficaces pour promouvoir la paix, le développement économique, la sécurité et la stabilité et pour renforcer la démocratie, la cohésion sociale, la bonne gouvernance et la primauté du droit, ainsi que la nécessité de faire face efficacement aux difficultés et aux menaces toujours plus nombreuses résultant de l'utilisation abusive de ces technologies, notamment à des fins criminelles et terroristes, tout en respectant les droits de l'homme (voir également le paragraphe 15 de l'Engagement de Tunis);

b) qu'il est nécessaire d'instaurer un climat de confiance et de sécurité dans l'utilisation des télécommunications/TIC en renforçant les bases de cette confiance (paragraphe 39 de Agenda de Tunis) et qu'il est nécessaire que les gouvernements, en coopération avec les autres parties prenantes, dans la limite de leurs rôles respectifs, élaborent la législation nécessaire leur permettant de mener des enquêtes et de poursuivre en justice les auteurs de cybercrimes, au niveau national, et coopèrent aux niveaux régional et international, compte tenu des cadres existants;

c) que l'existence d'un ordinateur quantique pertinent dans le domaine du chiffrement constituerait une menace pour certains systèmes de chiffrement utilisés dans les réseaux de télécommunication/TIC;

d) que, par sa Résolution 64/211, l'Assemblée générale des Nations Unies invite les États Membres à utiliser, si et quand ils le jugent opportun, la méthode d'auto-évaluation volontaire des efforts nationaux décrite dans l'annexe de cette Résolution;

² Notant que certains États Membres n'ont pas approuvé le Pacte numérique mondial.

- e) qu'il est nécessaire que les États Membres élaborent des programmes nationaux en matière de cybersécurité fondés sur un plan national, des partenariats public-privé, des bases juridiques solides, des moyens de gestion des incidents, de veille, d'alerte, d'intervention et de rétablissement, et une culture de la sensibilisation, en s'appuyant sur les différentes ressources mises au point et/ou mises à disposition par l'UIT, les membres de l'Union et ses partenaires, s'il y a lieu;
- f) qu'une approche itérative et fondée sur les risques en matière de cybersécurité permet d'élaborer et d'appliquer les pratiques de cybersécurité nécessaires pour faire face à l'évolution constante des menaces et des vulnérabilités, et que la cybersécurité 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;
- g) 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 que constituent les incidents de cybersécurité, y compris ceux liés à l'utilisation inappropriée des télécommunications/TIC à des fins malveillantes dans le monde, alarment tous les pays développés et les pays en développement du monde, sans exception;
- h) les motifs qui ont présidé à l'adoption de la Résolution 37 (Rév. Bakou, 2025) de la présente Conférence relative à la réduction de la fracture numérique, compte tenu de l'importance de la mise en œuvre multi-parties prenantes au plan international et des grandes orientations visées au paragraphe 108 de l'Agenda de Tunis, notamment celle intitulée "Établir la confiance et la sécurité dans l'utilisation des TIC";
- i) les résultats de plusieurs activités de l'UIT dans le domaine de la cybersécurité, plus précisément, sans toutefois s'y limiter, celles coordonnées par le BDT, pour que l'UIT puisse s'acquitter de son mandat en tant que coordonnateur pour la mise en œuvre de la grande orientation C5;
- j) que plusieurs organisations issues de tous les secteurs de la société travaillent en collaboration pour renforcer la cybersécurité des services et des technologies de télécommunication/TIC et instaurer la confiance dans ces services et ces technologies;
- k) que toutes les parties prenantes concernées peuvent jouer un rôle précieux dans la sensibilisation aux questions de cybersécurité, en particulier auprès des femmes, des enfants, des personnes handicapées, des personnes ayant des besoins particuliers ainsi que des personnes présentant un handicap lié à l'âge;

l) que le fait, entre autres, que les infrastructures essentielles des télécommunications/TIC sont interconnectées au niveau mondial signifie qu'un faible niveau de sécurité des infrastructures dans un pays pourrait entraîner une vulnérabilité et des risques accrus dans d'autres pays;

m) que de nombreux États Membres connaissent une importante pénurie de personnel qualifié dans le secteur de la cybersécurité et que cette pénurie de professionnels de la cybersécurité formés constitue un frein majeur pour la cybersécurité et qu'il importe d'encourager davantage de personnes à choisir une carrière dans le domaine de la cybersécurité;

n) que le développement des compétences humaines et le renforcement des capacités sont essentiels pour améliorer la cybersécurité, et qu'il est nécessaire de sensibiliser le public et de promouvoir des mesures élémentaires de sécurité en matière de cyberhygiène, que tout un chacun, y compris les femmes, les enfants, les personnes handicapées, les personnes ayant des besoins particuliers et les personnes présentant un handicap lié à l'âge, devrait prendre pour se prémunir contre les risques de cybersécurité;

o) que des organisations nationales et régionales ainsi que d'autres organisations internationales concernées, selon leur rôle respectif, mettent à la disposition des États Membres diverses informations, données, bonnes pratiques et ressources financières, selon qu'il convient;

p) que le Programme GCA 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;

q) que la cybersécurité et la cyberrésilience sont devenues fondamentales aux niveaux national, régional et international pour le développement numérique durable, et que l'UIT-D peut, dans le cadre de son mandat, continuer de contribuer à l'action menée pour instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC,

reconnaissant

a) les défis auxquels les États, en particulier les pays en développement, sont confrontés pour instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC;

b) que les mesures prises pour garantir la stabilité et la sécurité des réseaux de télécommunication/TIC et pour assurer la protection contre les cybermenaces/la cybercriminalité et le spam doivent protéger et respecter les dispositions relatives à la vie privée et à la liberté d'expression qui figurent dans les parties pertinentes de la Déclaration universelle des droits de l'homme (voir également le paragraphe 42 de l'Agenda de Tunis) et le Pacte international relatif aux droits civils et politiques;

c) que l'Assemblée générale des Nations Unies, dans sa Résolution 75/176 sur le droit à la vie privée à l'ère du numérique, affirme notamment "que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne, y compris le droit à la vie privée, et qu'une attention particulière doit être accordée à la protection des enfants";

d) la nécessité de prendre des mesures appropriées, notamment préventives, déterminées par la loi, pour empêcher les utilisations abusives des télécommunications/TIC, comme indiqué dans la Déclaration de principes et le Plan d'action de Genève du SMSI au chapitre des dimensions éthiques de la société de l'information (paragraphe 43 de l'Agenda de Tunis), la nécessité de lutter contre le terrorisme sous toutes ses formes et dans toutes ses manifestations sur les réseaux de télécommunication/TIC, dans le respect des droits de l'homme et conformément à d'autres obligations au regard du droit international, comme indiqué au point 81 du dispositif de la Résolution 60/1 de l'Assemblée générale des Nations Unies ("Document final du Sommet mondial de 2005"), l'importance de la sécurité, de la continuité et de la stabilité de l'Internet et la nécessité de protéger l'Internet et les réseaux TIC contre les menaces et les risques de vulnérabilité (paragraphe 45 de l'Agenda de Tunis), tout en garantissant le respect de la vie privée et la protection des informations et des données personnelles, et ce par différents moyens: adoption de législations, mise en œuvre de cadres de coopération, élaboration de bonnes pratiques et mise au point de mesures techniques et d'autoréglementation par les entreprises et les utilisateurs (paragraphe 46 de l'Agenda de Tunis);

e) la nécessité de remédier efficacement aux problèmes et aux menaces résultant de l'utilisation des télécommunications/TIC, par exemple 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, et de coopérer pour prévenir l'utilisation abusive des ressources et technologies de l'information, tout en respectant les droits de l'homme;

f) le rôle que jouent les télécommunications/TIC dans la protection et l'épanouissement de l'enfant, et la nécessité de renforcer l'action menée pour protéger les enfants et les jeunes contre tout abus et défendre leurs droits dans le contexte des télécommunications/TIC, en insistant sur le fait que l'intérêt supérieur de l'enfant doit être une considération primordiale;

g) la volonté et la détermination de toutes les parties concernées d'édifier une société de l'information à dimension humaine, inclusive, sûre et privilégiant le développement, conformément aux buts et aux principes de la Charte des Nations Unies, au droit international et au multilatéralisme et tout en respectant pleinement et en soutenant la Déclaration universelle des droits de l'homme, afin que chacun puisse, partout, créer, obtenir, utiliser et partager l'information et le savoir en toute sécurité pour réaliser ainsi l'intégralité de son potentiel et pour atteindre les buts et les objectifs de développement arrêtés à l'échelle internationale, notamment les Objectifs de développement durable (ODD);

h) les dispositions des paragraphes 4, 5 et 55 de la Déclaration de principes de Genève et le fait que la liberté d'expression et la libre circulation des informations, des idées et du savoir favorisent le développement;

i) que la phase de Tunis du SMSI a constitué une occasion unique de faire prendre conscience des avantages que les télécommunications/TIC peuvent apporter à l'humanité et de la façon dont elles peuvent transformer les activités, les relations et la vie des personnes et, par conséquent, renforcer la confiance dans l'avenir, à condition que leur utilisation soit sécurisée, comme l'a démontré la mise en œuvre des résultats du SMSI;

j) que le spam est un problème mondial, qui présente des caractéristiques différentes selon les régions, et qu'une démarche de coopération multipartite est nécessaire pour y répondre;

k) que la manipulation de la façon dont les informations sur l'appelant sont présentées lorsqu'un utilisateur reçoit un appel constitue un problème important dans le cadre du spam vocal qui peut découler de vulnérabilités en matière de cybersécurité et qui peut nécessiter l'application de mesures appropriées et une coopération internationale continue entre toutes les parties prenantes;

l) la nécessité de traiter efficacement le problème préoccupant du spam, comme indiqué dans le paragraphe 41 de l'Agenda de Tunis, ainsi que les cyberattaques et les incidents de cybersécurité;

m) que des mécanismes antispam complets sont essentiels pour protéger les utilisateurs des télécommunications/TIC, en particulier dans les pays en développement,

notant

a) la nécessité d'assurer une coordination efficace au sein de l'UIT-D;

- b)* le travail accompli en permanence par la Commission d'études 17 (Sécurité) du Secteur de la normalisation des télécommunications de l'UIT (UIT-T) et d'autres organisations de normalisation sur différents aspects de la sécurité des télécommunications/TIC;
- c)* que le spam est un problème important et continue de représenter une menace pour les utilisateurs, les réseaux et l'Internet dans son ensemble, et que la question de la cybersécurité, devrait être traitée aux niveaux national, régional et international selon qu'il convient;
- d)* que la coopération et la collaboration entre les États Membres, les Membres de Secteur et les parties prenantes concernées contribuent à créer et à entretenir une culture de la cybersécurité;
- e)* le travail accompli en permanence par le secteur privé, les établissements universitaires, la communauté technique et toutes les autres parties prenantes concernées pour promouvoir la cybersécurité dans le secteur des télécommunications/TIC;
- f)* que les pays peuvent être confrontés à d'importants nouveaux défis et bénéficier de nouvelles perspectives considérables dans les domaines de la cybersécurité et de la lutte contre le spam, à mesure que les services et les technologies de télécommunication/TIC nouveaux et émergents continuent de se développer;
- g)* que les aspects de la cybersécurité liés à la protection des données et aux informations d'identification personnelle (PII) revêtent une grande importance;
- h)* qu'il est nécessaire de promouvoir d'une part le développement et le perfectionnement d'une main-d'œuvre diversifiée et qualifiée dans le domaine de la cybersécurité, capable de faire face aux risques de cybersécurité et de les atténuer, et d'autre part l'importance des compétences requises et des perspectives de carrière professionnelle,

décide

- 1 de continuer à faire de la cybersécurité l'une des activités prioritaires de l'UIT, compte tenu des services et des technologies de télécommunication/TIC nouveaux et émergents, et à examiner, dans son domaine de compétence principal, la question du renforcement de la confiance et de la sécurité dans l'utilisation des télécommunications/TIC, en sensibilisant davantage l'opinion, en échangeant des bonnes pratiques, en fournissant une assistance sur l'application de mesures techniques et en élaborant des outils et du matériel didactique approprié, afin de promouvoir une culture de la cybersécurité;

2 de continuer à renforcer la collaboration, la coopération et l'échange d'informations entre toutes les organisations internationales ou régionales compétentes sur les initiatives relatives à la cybersécurité, y compris la cyberrésilience, dans les domaines de compétence de l'UIT, compte tenu de la nécessité de fournir une assistance aux pays en développement;

3 d'inviter les organismes de financement nationaux et internationaux à privilégier davantage la fourniture d'une assistance financière importante, y compris en octroyant des crédits à des conditions favorables, aux formations et programmes nationaux sur les compétences techniques en matière de cybersécurité des pays en développement qui ne disposent pas des compétences techniques appropriées en matière de cybersécurité, en accordant la priorité aux jeunes, aux femmes et aux personnes handicapées;

4 de continuer à encourager les partenariats pour le renforcement des capacités en matière de cybersécurité, afin de permettre à l'UIT-D de collaborer avec d'autres parties prenantes et organisations concernées ayant les compétences spécialisées et les connaissances nécessaires dans ce domaine;

5 de continuer à intégrer les considérations relatives à la cybersécurité dans toutes les initiatives et tous les projets de développement numérique de l'UIT-D,

charge le Directeur du Bureau de développement des télécommunications

1 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;

2 de continuer d'organiser, en collaboration avec les organisations compétentes, selon qu'il conviendra, compte tenu des contributions des membres, et en coopération avec le Directeur du Bureau de la normalisation des télécommunications (TSB), des réunions des États Membres, des Membres de Secteur et d'autres parties prenantes intéressées, pour réfléchir aux moyens d'améliorer la cybersécurité, y compris la lutte contre le spam;

3 de continuer, en collaboration avec les organisations et les parties prenantes intéressées, de mener des études sur le renforcement de la cybersécurité et de la cyberrésilience dans les pays en développement, aux niveaux régional et international, sur la base d'une évaluation précise des besoins de ces pays, notamment en ce qui concerne l'utilisation des télécommunications/TIC, y compris la lutte contre le spam, et les services et les technologies de télécommunication/TIC nouveaux et émergents, ainsi que la protection en ligne des enfants et des jeunes et des personnes vulnérables et les aspects relatifs à la cybersécurité de la protection des données et des informations PII;

- 4 d'examiner les résultats des travaux relatifs à l'Indice mondial de cybersécurité (GCI), pour fournir des orientations au BDT concernant les initiatives relatives à la cybersécurité, en tenant compte notamment des lacunes recensées dans le cadre du processus lié à l'Indice GCI;
- 5 de continuer de présenter les résultats du GCI de façon que les pays soient représentés par niveaux, plutôt que selon un classement individuel, afin de rendre compte plus précisément du niveau de développement de la cybersécurité dans les États Membres;
- 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 ils sont confrontés;
- 7 de soutenir les initiatives des États Membres, en particulier des pays en développement, concernant les mécanismes propres à renforcer la coopération dans le domaine de la cybersécurité, y compris la lutte contre le spam;
- 8 d'aider les États Membres à recenser les mesures élémentaires de cybersécurité qui ont trait à la cyberhygiène et que chacun devrait prendre pour se prémunir contre les risques de cybersécurité et le spam, et d'encourager et d'aider les membres de l'UIT et les autres parties prenantes à faire connaître ces mesures au public;
- 9 d'aider les États Membres, en particulier les pays en développement, en fournissant des orientations et des bonnes pratiques sur les difficultés et les possibilités liés à la cybersécurité et à la lutte contre le spam qui découlent des services et des technologies de télécommunication/TIC nouveaux et émergents;
- 10 de contribuer à mener des campagnes de sensibilisation et de pédagogie sur la nécessité de préparer la migration, au niveau national, vers la cryptographie post-quantique dans les réseaux de télécommunication/TIC, dans le cadre du mandat et des compétences spécialisées de l'UIT, et d'encourager les membres à échanger des bonnes pratiques et des données d'expérience nationales à cet égard;
- 11 de diffuser auprès des pays en développement des informations concernant les lignes directrices, les recommandations, les rapports techniques et les bonnes pratiques concernant la cybersécurité qui ont été élaborés par les commissions d'études de l'UIT-T, en particulier par la Commission d'études 17 de l'UIT-T, en tant que commission d'études directrice pour la sécurité, en collaboration avec le Directeur du TSB;

12 de contribuer à la diffusion des Recommandations techniques de l'UIT-T et des ressources d'information pertinentes élaborées par d'autres organisations susceptibles d'aider les pays en développement à identifier et à mettre en œuvre des mesures permettant de prévenir, de détecter et de limiter le spam vocal résultant de vulnérabilités en matière de cybersécurité et d'encourager la coopération internationale entre toutes les parties prenantes;

13 d'aider les pays en développement à améliorer leur état de préparation afin d'assurer un niveau de cybersécurité élevé et efficace, y compris la cyberrésilience, pour leurs infrastructures essentielles de télécommunication/TIC, notamment en organisant des séminaires, des ateliers et des formations pour promouvoir la cyberhygiène ainsi que d'autres manifestations au titre des piliers du GCA, en particulier en ce qui concerne les mesures organisationnelles et techniques et le renforcement des capacités, en collaboration avec le Directeur du TSB, selon qu'il conviendra;

14 d'aider les États Membres à mettre en place un cadre approprié entre les pays en développement, permettant de détecter rapidement des incidents majeurs et d'y réagir sans tarder, notamment en encourageant l'échange volontaire d'informations entre les administrations intéressées, et de proposer un plan d'action destiné à accroître leur protection et à renforcer la cyberrésilience, compte tenu des mécanismes et des partenariats, selon le cas;

15 de recueillir auprès des États Membres et d'échanger, dans le cadre des travaux relevant de la Question 3/2 de la Commission d'études 2 de l'UIT-D, des informations sur les réglementations, les politiques et les autres approches adoptées par les autorités nationales de régulation des télécommunications et les autres organisations de parties prenantes pour instaurer un climat de confiance et de sécurité dans l'utilisation des télécommunications/TIC;

16 d'encourager toutes les parties concernées à participer et/ou à contribuer aux activités des centres de formation de l'Académie de l'UIT à des fins de formation, d'éducation et de sensibilisation aux questions de cybersécurité, dans le cadre du GCA;

17 d'aider les États Membres en améliorant l'échange d'informations actualisées sur les questions de cybersécurité et les bonnes pratiques à envisager;

18 de présenter à la prochaine conférence mondiale de développement des télécommunications un rapport sur les résultats de la mise en œuvre de la présente Résolution;

19 de continuer de consulter les membres au sujet de l'amélioration du processus lié à l'Indice GCI, notamment dans le cadre du débat relatif aux méthodes, aux indicateurs, à la structure, à la pondération et aux questions, en faisant appel au Groupe d'experts, selon qu'il conviendra, compte tenu des incidences financières;

20 de continuer de soutenir le Réseau de femmes (NoW) à l'UIT-D et les autres initiatives visant à encourager la participation active des femmes aux activités et aux fonctions de direction de l'UIT-D relatives à la cybersécurité;

21 de tenir à jour, d'étoffer et de promouvoir un recueil de bonnes pratiques sur les mesures propres à aider et à encourager les personnes, en particulier les femmes et les jeunes filles, à opter pour une carrière dans le secteur de la cybersécurité,

invite le Secrétaire général, en coordination avec les Directeurs du Bureau des radiocommunications, du Bureau de la normalisation des télécommunications et du Bureau de développement des télécommunications

1 à soumettre un rapport sur les Mémoires d'accord entre les pays, ainsi que sur les formes de coopération existantes, comportant une analyse de leur état d'avancement et de leur champ d'application ainsi que de l'application de ces mécanismes de coopération pour renforcer la cybersécurité et lutter contre les cybermenaces, afin de permettre aux États Membres de déterminer si des Mémoires ou des mécanismes supplémentaires sont nécessaires;

2 à appuyer les initiatives mondiales et régionales en matière de cybersécurité, et à inviter tous les pays, en particulier les pays en développement, à y participer;

3 à continuer de mobiliser les compétences spécialisées de l'UIT dans le domaine du développement, en vue de renforcer la cybersécurité aux niveaux national, régional et international à l'appui des ODD, en concertation avec les autres organismes/institutions compétents du système des Nations Unies et les autres organismes internationaux compétents, en tenant compte des mandats et des domaines de compétence spécifiques de chacun, tout en gardant à l'esprit la nécessité d'éviter les chevauchements d'activités entre les organisations et au sein des Bureaux ou du Secrétariat général,

prie le Secrétaire général

de présenter un rapport sur les résultats de ces activités aux sessions ultérieures du Conseil et aux Conférences de plénipotentiaires, selon qu'il conviendra,

invite les États Membres, les Membres de Secteur, les Associés et les établissements universitaires

- 1 à apporter l'appui nécessaire et à collaborer activement à la mise en œuvre de la présente Résolution;
- 2 à continuer de travailler en collaboration avec l'UIT-D pour fournir les ressources nécessaires à la mise en œuvre d'initiatives visant à aider les pays en développement, en accordant une attention particulière aux pays les moins avancés, aux petits États insulaires en développement et aux pays en développement sans littoral, à renforcer leurs capacités en matière de cybersécurité, comme le projet "La cybersécurité au service du bien social";
- 3 à reconnaître que la cybersécurité, y compris les aspects liés aux incidences des services et des technologies de télécommunication/TIC nouveaux et émergents et la lutte contre le spam constituent des questions hautement prioritaires, à prendre des mesures appropriées et à contribuer à instaurer un climat de confiance et de sécurité dans l'utilisation des télécommunications/TIC, aux niveaux national, régional et international;
- 4 à encourager les fournisseurs de services à se prémunir contre les risques de cybersécurité identifiés, à limiter l'exposition à ces risques, à s'efforcer d'assurer la continuité des services fournis et à fournir des notifications d'infractions en matière de cybersécurité conformément à la législation nationale applicable;
- 5 à promouvoir les initiatives qui encouragent davantage de personnes, en particulier les femmes et les jeunes filles, à exercer des métiers dans le domaine de la cybersécurité, notamment en élaborant des programmes d'enseignement et de formation pertinents;
- 6 à fournir des contributions et à échanger des informations sur des solutions innovantes pour faire face aux menaces à la cybersécurité et lutter contre le spam;
- 7 à collaborer étroitement afin de contribuer à relever les défis et à tirer parti des possibilités liés aux technologies nouvelles et émergentes pour assurer la cybersécurité des services et technologies de télécommunication/TIC, et à lutter contre le spam, notamment en déployant des efforts aux niveaux national, régional et international, selon qu'il conviendra;
- 8 à collaborer au niveau national, afin d'améliorer les solutions propres à préserver la sécurité et la résilience des réseaux;
- 9 à informer l'UIT sur les cadres de coopération existants, au niveau bilatéral, entre les membres et avec d'autres entités et organismes régionaux ou internationaux;

- 10 à contribuer aux travaux menés au titre de la Question pertinente sur la cybersécurité à l'étude au sein de l'UIT-D et aux autres initiatives pertinentes du Secteur en matière de cybersécurité;
- 11 à promouvoir l'élaboration de programmes d'enseignement et de formation pour sensibiliser davantage les utilisateurs, en particulier les femmes, les enfants, les personnes handicapées, les personnes ayant des besoins particuliers et les personnes ayant un handicap lié à l'âge, aux risques en matière de cybersécurité et aux mesures qu'ils peuvent prendre pour s'en protéger;
- 12 à promouvoir l'élaboration d'outils et de supports pour renforcer les dispositifs de cybersécurité et de cyberrésilience des petites et moyennes entreprises;
- 13 à contribuer à améliorer le processus lié à l'Indice GCI, notamment dans le cadre du débat relatif aux méthodes, aux indicateurs, à la structure, à la pondération et aux questions, en utilisant le Groupe d'experts sur l'Indice GCI;
- 14 à contribuer aux discussions, à l'échange d'informations, au renforcement des capacités et aux études sur les défis et les perspectives liés à la cybersécurité et à la lutte contre le spam à mesure que les technologies d'IA se développent et sont utilisées dans les télécommunications/TIC pour les rendre plus efficaces et plus performantes;
- 15 à faire usage de l'Académie de l'UIT pour le renforcement des capacités et la formation sur les services et technologies de télécommunication/TIC nouveaux et émergents et sur les questions de cybersécurité connexes,

invite les États Membres

- 1 à mener des enquêtes et à analyser les pratiques concernant l'utilisation des technologies de télécommunication/TIC nouvelles et émergentes pour la lutte contre le spam;
- 2 à encourager les parties prenantes concernées à contribuer à sensibiliser davantage la population aux risques en matière de cybersécurité, en particulier les femmes, les enfants, les personnes handicapées, les personnes ayant des besoins particuliers, ainsi que les personnes ayant un handicap lié à l'âge;
- 3 à participer activement aux travaux de l'UIT-D en matière de cybersécurité et de lutte contre le spam et sa propagation en organisant des formations techniques et des ateliers à l'intention des régulateurs et des opérateurs de télécommunication;
- 4 à établir un cadre approprié permettant de réagir rapidement à des incidents graves de cybersécurité et à proposer un plan d'action visant à prévenir ces incidents, à en atténuer les effets et à les surmonter;

- 5 à élaborer des stratégies et à se doter des capacités nécessaires, au niveau national, pour assurer la protection des infrastructures nationales essentielles, y compris en renforçant la résilience des infrastructures de télécommunication/TIC;
- 6 à prendre des mesures en vue de développer leurs capacités nationales en matière de cybersécurité, compte tenu des piliers de l'Indice GCI, s'il y a lieu;
- 7 à promouvoir l'échange d'informations sur la cybersécurité aux niveaux national, régional et international;
- 8 à contribuer à l'élaboration du recueil de bonnes pratiques de l'UIT sur les mesures propres à aider et encourager davantage de personnes, en particulier les femmes et les jeunes filles, à opter pour une carrière dans le secteur de la cybersécurité.