RÉSOLUTION 45 (Rév. Kigali, 2022)

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

La Conférence mondiale de développement des télécommunications (Kigali, 2022),

rappelant

a) la Résolution 130 (Rév. Dubaï, 2018) 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. Dubaï, 2018) 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 45 (Rév. Dubaï, 2014) de la Conférence mondiale de développement des télécommunications (CMDT);

f) la Résolution 50 (Rév. Genève, 2022) de l'Assemblée mondiale de normalisation des télécommunications (AMNT) relative à la cybersécurité;

g) la Résolution 52 (Rév. Hammamet, 2016) de l'AMNT relative à la lutte contre le spam;

h) la Résolution 58 (Rév. Genève, 2022) de l'AMNT, intitulée "Encourager la création d'équipes nationales d'intervention en cas d'incident informatique (CIRT), en particulier pour les pays en développement"[1];

i) la Résolution 69 (Rév. Kigali, 2022) 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;

---

[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 67 (Rév. Kigali, 2022) 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;

k) les avis pertinents du sixième Forum mondial des politiques de télécommunication (FMPT-21) 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 buts énoncés dans le plan stratégique de l'Union en vigueur;

p) la Question de l'UIT-D à l'étude, intitulée "Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité", dans le cadre de laquelle un grand nombre de membres ont collaboré au cours du dernier cycle d'études pour établir des rapports, et notamment du matériel didactique à l'usage des pays en développement, par exemple un recueil de données d'expérience nationales et de bonnes pratiques relatives aux partenariats secteur public-secteur privé (PPP), à la création d'une équipe CIRT, avec le matériel didactique correspondant, et à un cadre de gestion des équipes CIRT;

q) 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, "Établir la confiance et la sécurité dans l'utilisation des TIC", et conformément à la Résolution 140 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires sur le rôle de l'UIT en tant que coordonnatrice unique pour la grande orientation C5 du SMSI ainsi qu'à la Résolution 58 (Rév. Genève, 2022) de l'AMNT, "Encourager la création d'équipes CIRT nationales, en particulier pour les pays en développement";

r) 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;

s) que l'UIT et l'Office des Nations Unies contre la drogue et le crime ont signé un Mémorandum d'accord, afin de renforcer la sécurité dans l'utilisation des TIC,

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 enjeux toujours plus nombreux et aux menaces 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 de coopérer aux niveaux régional et international, compte tenu des cadres existants;

c) 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;

d) qu'il est nécessaire que les États Membres élaborent des programmes nationaux en matière de cybersécurité axés sur un plan national, nouent des partenariats PPP, créent des bases juridiques solides, mettent au point des moyens de gestion des incidents, de veille, d'alerte, d'intervention et de rétablissement et instaurent une culture de la sensibilisation, en se fondant sur les rapports intitulés "Bonnes pratiques pour une approche nationale de la cybersécurité: éléments de base pour l'organisation d'activités nationales en matière de cybersécurité";

e) 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 et du sabotage intentionnel dans le monde alarment tous les pays développés et les pays en développement du monde, sans exception;

f) les motifs qui ont présidé à l'adoption de la Résolution 37 (Rév. Kigali, 2022) 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";

g) 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 Bureau de développement des télécommunications, pour que l'UIT puisse s'acquitter de son mandat en tant que coordonnateur pour la mise en œuvre de la grande orientation C5 (Établir la confiance et la sécurité dans l'utilisation des TIC);

h) que plusieurs organisations issues de tous les secteurs de la société travaillent en collaboration pour renforcer la cybersécurité des télécommunications/TIC;

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

j) 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 le cas;

k) 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;

l) que la cybersécurité est devenue un enjeu très important au niveau international pour le développement durable, et que l'UIT-D peut, dans le cadre de son mandat, continuer de contribuer à l'action menée pour instaurer un climat de confiance et de sécurité dans l'utilisation des télécommunications/TIC,

reconnaissant

a) 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;

b) que l'Assemblée générale des Nations Unies, dans sa Résolution 68/167 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 protégées en ligne, y compris le droit à la vie privée;

c) 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), 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 des réseaux de télécommunication/TIC et la nécessité de protéger les réseaux de télécommunication/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);

d) qu'il faut faire face 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, ce qui serait au détriment de la sécurité des États, et coopérer pour prévenir toute utilisation abusive des ressources et technologies de l'information à des fins criminelles et terroristes, tout en respectant les droits de l'homme;

e) que les télécommunications/TIC jouent un rôle dans la protection et l'épanouissement de l'enfant et qu'il est nécessaire de renforcer les mesures propres à protéger les enfants et les jeunes gens contre tout abus et à assurer la défense de 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;

f) la volonté et la détermination de toutes les parties concernées d'édifier une société de l'information à dimension humaine, solidaire, 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);

g) 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;

h) 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 Sommet;

i) 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;

j) la nécessité de traiter efficacement le problème préoccupant du spam, comme indiqué dans le paragraphe 41 de l'Agenda de Tunis, ainsi que, entre autres, le spam, la cybercriminalité, les virus, les vers et les dénis de service;

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

notant

a) le travail accompli en permanence par la Commission d'études 17 (Sécurité) de l'UIT-T et d'autres organisations de normalisation sur différents aspects de la sécurité des télécommunications/TIC;

b) 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 appropriés;

c) que la coopération et la collaboration entre les États Membres, les Membres de Secteur et les parties prenantes intéressées contribuent à créer et à entretenir une culture de la cybersécurité,

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 déterminant de 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 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,

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;

3 de continuer, en collaboration avec les organisations et les parties prenantes intéressées, de mener des études sur le renforcement de la cybersécurité 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;

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 modifier le mode de présentation des 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 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 collaboration avec le Directeur du TSB;

9 d'aider les États Membres, en particulier les pays en développement, en fournissant des orientations et des bonnes pratiques permettant de surmonter les problèmes liés à la cybersécurité et au spam qui découlent des technologies nouvelles et émergentes;

10 d'aider les pays en développement à améliorer leur état de préparation afin d'assurer un niveau de cybersécurité élevé et efficace, y compris en matière de cyberrésilience, pour leurs infrastructures essentielles de télécommunication/TIC, notamment en organisant des ateliers et des formations pour promouvoir la cyberhygiène;

11 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;

12 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;

13 de faciliter l'examen par les commissions d'études concernées de l'UIT-D des travaux de recherché liés à la cybersécurité, en collaborant avec différentes parties prenantes;

14 d'encourager toutes les parties concernées à participer 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;

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

16 d'aider les pays en développement à progresser dans le développement de leurs capacités, en organisant des ateliers, des séminaires ou des manifestations au titre des piliers du GCA relatifs aux mesures organisationnelles et techniques, en collaboration avec le Directeur du TSB;

17 de présenter à la prochaine CMDT un rapport sur les résultats de la mise en œuvre de la présente Résolution;

18 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, 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,

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 Mémorandums 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 Mémorandums 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

1 de porter la présente Résolution à l'attention de la prochaine Conférence de plénipotentiaires pour examen et suite à donner, selon qu'il conviendra;

2 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 reconnaître que la cybersécurité 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, tant aux niveaux national et régional qu'au niveau international;

3 à encourager les fournisseurs de services à se prémunir contre les risques identifiés, à s'efforcer d'assurer la continuité des services fournis et à notifier les infractions aux mesures de sécurité;

4 à collaborer au niveau national, afin d'améliorer les solutions propres à préserver la sécurité et la résilience des réseaux;

5 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,

invite les États Membres

1 à collaborer étroitement en vue de renforcer la coopération aux niveaux régional et international, pour remédier aux problèmes actuels et futurs liés à la cybersécurité et au spam;

2 à établir un cadre approprié permettant de réagir rapidement à des incidents graves et à proposer un plan d'action visant à prévenir ces incidents, à en atténuer les effets et à les surmonter;

3 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;

4 à promouvoir l'échange d'informations sur la cybersécurité aux niveaux national, régional et international.