**MOD** B/30/1

RÉSOLUTION 45 (RÉV.BUENOS AIRES, 2017)

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

La Conférence mondiale de développement des télécommunications (Buenos Aires, 2017),

rappelant

*a)* la Résolution 130 (Rév. Busan, 2014) 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 140 (Rév. Busan, 2014) de la Conférence de plénipotentiaires, sur le rôle de l'UIT dans la mise en oeuvre des résultats du Sommet mondial sur la société de l'information et dans l'examen d'ensemble de leur mise en oeuvre par l'Assemblée générale des Nations Unies;

*c)* 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;

*d)* la Résolution 179 (Rév. Busan, 2014) de la Conférence de plénipotentiaires sur le rôle de l'UIT dans la protection en ligne des enfants;

*e)* 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;

*f)* la Résolution 50 (Rév.Hammamet, 2016) de l'Assemblée mondiale de normalisation des télécommunications (AMNT) relative à la cybersécurité;

*g)* la Résolution 52 (Rév.Hammamet, 2016) de l'Assemblée mondiale de normalisation des télécommunications (AMNT) relative à la lutte contre le spam;

*h)* la Résolution 58 (Rév.Dubaï, 2012) de l'Assemblée mondiale de normalisation des télécommunications (AMNT), intitulée "Encourager la création d'équipes nationales d'intervention en cas d'incident informatique (CIRT), en particulier pour les pays en développement";

*i)* la Résolution 69 (Rév.Dubaï, 2014) de la Conférence mondiale de développement des télécommunications, intitulée "Faciliter la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement, et coopération entre ces équipes";

*j)* la Résolution 67 (Rév.Dubaï, 2014) de la Conférence mondiale de développement des télécommunications, sur le rôle du Secteur du développement des télécommunications de l'UIT (UIT-D) dans la protection en ligne des enfants;

*k)* les nobles principes, buts et objectifs énoncés dans la Charte des Nations Unies et dans la Déclaration universelle des droits de l'homme;

*l)* 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 (Etablir la confiance et la sécurité dans l'utilisation des TIC);

*m)* les dispositions de l'Engagement de Tunis et de l'Agenda de Tunis relatives à la cybersécurité;

*n*) la Résolution 71 (Rév. Busan, 2014) de la Conférence de plénipotentiaires, sur le Plan stratégique de l'Union pour la période 2016-2019, dans laquelle sont approuvés les cinq objectifs de l'UIT‑D, entre autres l'Objectif D.3 – Renforcer la confiance et la sécurité dans l'utilisation des télécommunications/TIC, ainsi que dans le déploiement des applications et des services correspondants, et les résultats D.3-1: Renforcement de la capacité des Etats Membres à élaborer et à mettre en oeuvre des politiques et stratégies en matière de cybersécurité dans le cadre des plans nationaux sur les TIC, ainsi qu'à élaborer et à mettre en oeuvre des législations appropriées, et D.3-2: Renforcement de la capacité des Etats Membres à réagir rapidement face aux cybermenaces, dudit Objectif;

*o)* les excellents résultats obtenus pendant les périodes d'études 2006-2010 et 2010-2014 au titre de la Question 22 de la Commission d'études 1 de l'UIT-D, comprenant un grand nombre de rapports et de contributions émanant de pays du monde entier, les travaux ayant été poursuivis au titre de la Question 3/2 de la Commission d'études 2 de l'UIT‑D pendant la période d'études 2014-2017;

*p)* le rapport du Président du Groupe d'experts de haut niveau (HLEG) pour le Programme mondial cybersécurité (GCA), établi par le Secrétaire général de l'UIT en application de la grande orientation C5, "Etablir la confiance et la sécurité dans l'utilisation des TIC";

*q)* que l'UIT et l'Office des Nations Unies contre la drogue et le crime (ONUDC) ont signé en 2011 un Mémorandum d'accord (MoU), 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 Etats 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)* que l'Assemblée générale des Nations Unies, dans sa Résolution 70/125, intitulée "Document final de la réunion de haut niveau de l'Assemblée générale sur l'examen d'ensemble de la mise en oeuvre des textes issus du Sommet mondial sur la société de l'information", affirme que le renforcement de la fiabilité et de la sécurité des technologies numériques pour le développement durable devrait également être une priorité, notamment pour faire face aux difficultés de plus en plus nombreuses qui résultent de l’utilisation de ces technologies, comme leur détournement au profit d’activités néfastes telles que le harcèlement, la criminalité et le terrorisme, et doit se faire dans le respect des droits de l'homme;

*e)* qu'il est nécessaire que les Etats Membres élaborent des programmes nationaux en matière de cybersécurité axés sur un plan national, nouent des partenariats secteur public‑secteur privé, 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" établis au titre de la Question 22 de la Commission d'études 1 de l'UIT‑D au cours des deux périodes d'études 2006-2010 et 2010‑2014, puis au titre de la Question 3/2 de la Commission d'études 2 de l'UIT‑D au cours de la période d'études 2014-2017;

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

*g)* les motifs qui ont présidé à l'adoption de la Résolution 37 (Rév.Dubaï, 2014) de la Conférence mondiale de développement des télécommunications relative à la réduction de la fracture numérique, compte tenu de l'importance de la mise en oeuvre multi-parties prenantes au plan international et des grandes orientations visées au paragraphe 108 de l'Agenda de Tunis, notamment celle intitulée "Etablir la confiance et la sécurité dans l'utilisation des TIC";

*h)* 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 principal pour la mise en oeuvre de la grande orientation C5 (Etablir la confiance et la sécurité dans l'utilisation des TIC);

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

*j)* 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;

*k)* que des organisations nationales et régionales ainsi que d'autres organisations internationales concernées, selon leur rôle respectif, mettent à la disposition des Etats Membres diverses informations, données, bonnes pratiques et ressources financières, selon le cas;

*l)* qu'il ressort des résultats de l'enquête sur la sensibilisation à la cybersécurité menée par le BDT et les responsables de l'étude de la Question 22-1/1 pendant la période d'études 2010‑2014 que les pays les moins avancés ont besoin d'une assistance importante dans ce domaine;

*m)* que le Programme mondial cybersécurité (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;

*n)* que l'Indice mondial de cybersécurité (GCI), élaboré dans le cadre du GCA de l'UIT, est un outil important pour permettre à chaque Etat Membre d'évaluer son propre engagement par rapport au GCA de l'UIT et d'identifier les domaines à améliorer afin de renforcer ses propres capacités en matière de cybersécurité,

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 ses Résolutions 68/167, 69/166 et 71/1999 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 dans le Plan d'action de Genève 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 oeuvre 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 Etats, 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;

*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 oeuvre des résultats du Sommet;

*i)* 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, la cybercriminalité, les virus, les vers et les dénis de service;

*j)* la nécessité d'assurer une coordination efficace entre toutes les activités de l'UIT-D,

notant

*a)* 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;

*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)* les conclusions et les recommandations figurant dans le Rapport final sur la Question 3/2 de la Commission d’études 2 de l’UIT-D, selon lesquelles il convient d'étudier, pendant la prochaine période d’études, les menaces nouvelles ou en évolution autres que le spam et les logiciels malveillants;

*d)* que la coopération et la collaboration entre les Etats Membres, les Membres de Secteur et les parties prenantes intéressées sont essentielles pour créer et entretenir une culture de la cybersécurité,

décide

1 de continuer à faire de la cybersécurité l'une des activités prioritaires de l'UIT et à examiner, dans son domaine de compétence principal, la question du renforcement de la sécurité et de la confiance dans l'utilisation des télécommunications/TIC, en sensibilisant davantage l'opinion, en déterminant de bonnes pratiques et en élaborant 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, 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 continuer d'organiser, en collaboration avec les organisations compétentes, selon qu'il conviendra, en association avec le programme relevant du Produit 3.1 de l'Objectif 3, et sur la base des contributions des membres ainsi qu'en coopération avec le Directeur du Bureau de la normalisation des télécommunications (TSB), des réunions des Etats Membres, des Membres de Secteur et d'autres parties prenantes intéressées, pour réfléchir aux moyens d'améliorer la cybersécurité;

2 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, ainsi que les dispositifs IoT, l'intelligence artificielle et d'autres nouvelles tendances, y compris la protection des enfants et des jeunes;

3 de soutenir les initiatives des Etats Membres, en particulier des pays en développement, concernant les mécanismes propres à renforcer la coopération dans le domaine de la cybersécurité;

4 d'aider les pays en développement à améliorer leur état de préparation afin d'assurer un niveau de sécurité élevé et efficace pour leurs infrastructures essentielles de télécommunication/TIC, notamment en organisant des ateliers;

5 d'aider les Etats 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 et de proposer un plan d'action destiné à renforcer leur protection, compte tenu des mécanismes et des partenariats, selon le cas;

6 de rassembler et de diffuser, dans le cadre des travaux menés au titre de la Question 3/2 de la Commission d'études 2 de l'UIT‑D, des informations sur les politiques réglementaires élaborées et/ou mises en oeuvre par les autorités nationales de régulation des télécommunications pour instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC;

7 de mettre en oeuvre la présente Résolution en coopération et en collaboration avec le Directeur du TSB;

8 de présenter à la prochaine CMDT un rapport sur les résultats de la mise en oeuvre de la présente Résolution,

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, du champ d'application et des applications de ces mécanismes de coopération, dans le but de renforcer la cybersécurité et de lutter contre les cybermenaces, afin de permettre aux Etats Membres de déterminer si des Mémorandums ou des mécanismes supplémentaires sont nécessaires;

2 à appuyer les projets mondiaux ou régionaux en matière de cybersécurité, notamment IMPACT, FIRST, OAS, APCERT, et à inviter tous les pays, en particulier les pays en développement, à y participer,

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 au Conseil et à la Conférence de plénipotentiaires en 2018,

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

1 à apporter l'appui nécessaire et à prendre part activement à la mise en oeuvre 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 entre eux afin d'améliorer les solutions relatives à la protection de la vie privée et des données personnelles ainsi que la sécurité des réseaux,

invite les Etats Membres

1 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 et à en atténuer les effets;

2 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.