|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Assemblée mondiale de normalisation  des télécommunications (AMNT-16) Hammamet, 25 octobre - 3 novembre 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| **SÉANCE PLÉNIÈRE** | | **Addendum 19 au Document 46-F** | |
|  | | **22 septembre 2016** | |
|  | | **Original: anglais** | |
|  | | | |
| Etats Membres de la Commission interaméricaine des télécommunications (CITEL) | | | |
| Propositions de modifications de la RÉsolution 50  de l'AMNT-12 – Cybersécurité | | | |
|  | | | |
|  | | | |

|  |  |
| --- | --- |
| **Résumé:** | Dans la présente contribution la CITEL propose d'apporter des modifications de forme à la Résolution 50 (Rév. Dubaï, 2012) de l'AMNT afin d'en aligner le texte sur celui de la Résolution 130 (Rév. Busan, 2014) de la Conférence de plénipotentiaires et de la Résolution 45 (Rév. Dubaï, 2014) de la CMDT. Ces révisions permettront de tenir compte de la situation mondiale actuelle en ce qui concerne l'instauration de la confiance et de la sécurité dans l'utilisation des TIC et d'harmoniser la contribution de l'UIT-T sur ce sujet avec les objectifs et priorités convenues des Membres. |

Introduction

Les technologies de l'information et de la communication (TIC) font partie intégrante du développement économique et social. La sécurité est un élément essentiel du fonctionnement et de l'utilisation des TIC, d’où la nécessité pour toutes les personnes concernées d'être au fait des questions de sécurité et de prendre, à leur niveau, les mesures qui s'imposent. Alors que les TIC sont de plus en plus utilisées, la cybersécurité reste une priorité pour les membres de l'UIT. Au cours des quatre dernières années, la Commission d'études 17 de l'UIT-T a poursuivi ses travaux dans ce domaine tout comme de nombreux organismes de normalisation et consortiums aux niveaux national, régional et international. En outre, la Conférence de plénipotentiaires de l'UIT de 2014 et la Conférence mondiale de développement des télécommunications de 2014 ont convenu de buts et de priorités en ce qui concerne l'instauration de la confiance et de la sécurité dans l'utilisation des TIC auxquels l'UIT-T devrait contribuer. La CITEL estime donc qu'il est opportun de mettre à jour la Résolution 50 pour qu'elle tienne compte de ces évolutions.

La cybersécurité est une question qui préoccupe les experts, y compris l'UIT, les utilisateurs et, essentiellement, les États.

Depuis la dernière Assemblée, les questions de cybersécurité non seulement ont conservé toute leur importance mais aussi requièrent une attention et une mobilisation toujours plus grandes de la part du secteur des technologies de l'information et de la communication. C'est la raison pour laquelle la présente Résolution, son libellé et sa pertinence restent essentiels pour ce qui est de la normalisation et un instrument de première importance pour l'Union et ses membres.

S'agissant de la présente proposition de modification, la République argentine est d'avis que le libellé de la Résolution doit être conservé et elle propose, pour sa part, de le mettre à jour afin de tenir compte des nouvelles avancées en matière de cybersécurité qui découlent des évolutions dans certains nouveaux domaines et qui sont liés, essentiellement, à l'apparition de nouvelles menaces. L'Argentine propose également d'inclure les éléments provenant de la dernière Conférence mondiale de développement des télécommunications (CMDT-14), qui a approuvé la contribution de l'UIT-T au Plan stratégique de l'UIT pour la période 2016-2019, souscrit à cinq Objectifs dont l'Objectif 3 – Renforcer la confiance et la sécurité dans l'utilisation des télécommunications/TIC, ainsi qu'au déploiement accru des applications et des services correspondants – et au Résultat 3.1 associé à cet Objectif: Améliorer la confiance et la sécurité dans l'utilisation des TIC et des services ainsi que le cadre d'exécution auquel figure le Programme sur la cybersécurité.

Parmi les éléments et les nouveaux domaines, on peut citer l'intérêt accru que les utilisateurs et/ou les dispositifs portent aux attaques alors que les interconnexions physiques et les échanges d'informations sont toujours plus nombreux et qu'apparaissent de nouvelles utilisations comme les transactions bancaires en ligne, les attestations en ligne, essentiellement les applications des téléphones intelligents.

De même, la progression et le développement actuel de l'Internet des objets ouvre de vastes perspectives en ce qui concerne les dispositifs et les activités et, dans le même temps, sont synonymes de menaces.

Proposition

La CITEL propose d'apporter des révisions à la Résolution 50 (Rév. Dubaï 2012) afin d'en harmoniser le libellé avec celui de la Résolution 130 (Rév. Busan, 2014) de la Conférence de plénipotentiaires et de la Résolution 45 (Rév. Dubaï, 2014) de la Conférence mondiale de développement des télécommunications et de tenir compte de la situation mondiale actuelle en ce qui concerne l'instauration de la confiance et de la sécurité dans l'utilisation des TIC.

MOD IAP/46A19/1

RÉSOLUTION 50 (Rév.HAMMAMET, 2016)

Cybersécurité

(Florianópolis, 2004; Johannesburg, 2008; Dubaï, 2012; Hammamet, 2016)

L'Assemblée mondiale de normalisation des télécommunications (Hammamet, 2016),

rappelant

*a)* la Résolution 130 (Rév.Busan, 2014) de la Conférence de plénipotentiaires, sur le 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. Busan, 2014) de la Conférence de plénipotentiaires, sur le rôle de l'UIT dans la protection en ligne des enfants;

*d)* la Résolution 181 (Guadalajara, 2010) de la Conférence de plénipotentiaires, sur les définitions et termes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

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

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

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

*h)* la Résolution 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 45 (Rév.Dubaï, 2012) de la Conférence mondiale de développement des télécommunications (CMDT);

*j)* la Résolution 52 (Rév. Dubaï, 2012) de la présente Assemblée, "Lutter contre le spam"; et

*k)* la Résolution 58 (Rév. Dubaï, 2012) de la présente Assemblée, "Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement[[1]](#footnote-1)1",

considérant

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

*b)* que le réseau téléphonique public commuté (RTPC) 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 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 des cyberincidents, dus à des cyberattaques, par exemple des intrusions par malveillance ou par jeu à l'aide de logiciels malveillants (vers et virus par exemple), sont diffusés par différentes méthodes, par exemple sur le web ou par l'intermédiaire d'ordinateurs infectés par des robots; que le nombre des cybermenaces et des cyberattaques et les méthodes correspondantes augmentent, tout comme la dépendance à l'égard de l'Internet et d'autres réseaux qui sont essentiels pour avoir accès aux services et à l'information;

*f)* 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 identifier les incidents de cybersécurité, s'y préparer, y faire face et prendre les mesures de rétablissement correspondantes;

*g)* 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 *f* du *considérant*,

considérant en outre

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

*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 organismes de normalisation comme leWorld Wide Web consortium (W3C), l'Organization for Advancement of Structured Information Standards (OASIS), le Groupe de travail sur l'ingénierie Internet et l'Institut des ingénieurs en électricité et en électronique, entre autres, 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,

reconnaissant

*a)* les résultats pertinents du Sommet mondial sur la société de l'information (SMSI) qui a désigné l'UIT comme coordonnateur et modérateur pour la grande orientation C5 (Etablir la confiance et la sécurité dans l'utilisation des TIC);

*b)* le *décide* de 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, et l'instruction d'intensifier les travaux hautement prioritaires menés au sein des commissions d'études de l'UIT-T;

*c)* que la CMDT-14 a approuvé la contribution au Plan stratégique de l'UIT pour la période 2016-2019 en souscrivant à cinq Objectifs dont l'Objectif 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 au Résultat 3.1 associé à cet Objectif: améliorer la confiance et la sécurité dans l'utilisation des TIC et des services et que dans le cadre d'exécution de cet objectif figurent le Programme sur la cybersécurité et la Question 3/2 du Secteur du développement des télécommunications de l'UIT (UIT-D);

*d)* que le Programme mondial cybersécurité (GCA) de l'UIT encourage la coopération internationale dans le but de proposer des stratégies en vue de l'élaboration de solutions propres à accroître la confiance et la sécurité dans l'utilisation des TIC,

reconnaissant en outre

*a)* que les vecteurs des cyberattaques, tels que le hameçonnage, le détournement d'adresses, le balayage/l'intrusion, les dénis de services distribués, le détournement de sites web, l'accès non autorisé, etc., ont de graves conséquences;

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

*c)* que l'origine des attaques est parfois difficile à identifier (par exemple, les attaques qui utilisent des adresses IP usurpées);

*d)* que la cybersécurité est l'un des éléments qui permettent d'instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC;

*e)* que, aux termes de la Résolution 181 (Guadalajara, 2010), il est reconnu qu'il est important d'étudier la question des termes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, qu'il faut prendre en compte dans ces éléments de base, outre les questions de cybersécurité, d'autres questions importantes, et qu'il faudra peut-être modifier de temps à autre la définition de la cybersécurité, afin de tenir compte de l'évolution en matière de politique;

*f)* que, aux termes de la Résolution 181 (Guadalajara, 2010), il a été décidé de tenir compte de la définition du terme "cybersécurité" approuvée dans la Recommandation UIT‑T X.1205 en vue de son utilisation dans le cadre des activités de l'UIT liées à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

*g)* que, comme il est reconnu dans la Résolution 181 (Rév. Guadalajara, 2010), la Commission d'études 17 de l'UIT-T est responsable de l'élaboration des principales Recommandations sur la sécurité des télécommunications et des TIC,

notant

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

*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)* que la coopération et la collaboration entre les organisations s'occupant de questions de sécurité peuvent promouvoir le progrès et contribuer à édifier et à entretenir une culture de la cybersécurité;

*d)* les efforts de collaboration importants déployés par et entre les gouvernements, le secteur privé, la société civile, les milieux techniques et universitaires pour instaurer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication,

décide

1 que toutes les commissions d'études de l'UIT-T doivent continuer à évaluer les Recommandations existantes et les nouvelles Recommandations en cours d'élaboration, notamment les Recommandations concernant les protocoles de signalisation et de télécommunication, quant à la robustesse de leur conception et aux risques d'une exploitation par des acteurs malveillants cherchant à intervenir de manière destructive dans leur déploiement dans l'infrastructure mondiale de l'information et de télécommunication, élaborer de nouvelles Recommandations relatives aux questions de sécurité qui se font jour et tenir compte des nouveaux services et des nouvelles applications qui seront assurés par l'infrastructure mondiale des télécommunications/TIC (par exemple, l'informatique en nuage, les réseaux électriques intelligents et les systèmes de transport intelligents, qui sont fondés sur les réseaux de télécommunication/TIC);

2 que l'UIT-T, dans sa sphère d'action et d'influence, doit continuer à sensibiliser au besoin de renforcer et de défendre les systèmes d'information et de télécommunication contre les cybermenaces et les cyberattaques, et à promouvoir la coopération entre les organisations internationales et régionales appropriées afin de renforcer l'échange d'informations techniques dans le domaine de la sécurité des réseaux d'information et de télécommunication;

3 que l'UIT-T doit travailler en étroite collaboration avec l'UIT-D, en particulier dans le contexte de la Question3/2;

4 que, pour évaluer les failles de sécurité dans les réseaux et les protocoles et faciliter l'échange d'informations sur la cybersécurité, il convient de prendre en compte et d'appliquer, selon qu'il conviendra, les Recommandations UIT-T, y compris celles de la série X et leurs Suppléments, notamment les Recommandations UIT-T X.805, UIT-T X.1205 et UIT-T X.1500, les normes de l'ISO/CEI et d'autres produits pertinents d'autres organisations;

5 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;

6 que les parties intéressées doivent être invitées à travailler ensemble à l'élaboration de normes et de lignes directrices pour contrer les cybermenaces et les cyberattaques et faciliter l'identification de la source d'une attaque;

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

8 que toutes les commissions d'études de l'UIT-T doivent continuer de faire rapport régulièrement sur la sécurité des télécommunications/TIC au Groupe consultatif de la normalisation des télécommunications (GCNT) en ce qui concerne les progrès réalisés dans l'évaluation des Recommandations existantes et dans l'élaboration de nouvelles Recommandations;

9 que les commissions d'études de l'UIT-T doivent continuer à assurer la liaison avec les organisations de normalisation et d'autres organismes travaillant dans ce domaine, tels que le JTC 1 de l'ISO/CEI, l'Organisation de coopération et de développement économiques (OCDE), le Groupe de travail sur les télécommunications et l'information de la Coopération économique Asie-Pacifique (APEC-TEL) et l'*Internet Engineering Task Force* (IETF),

10 que la Commission d'études 17 doit poursuivre ses travaux sur les questions traitées dans la Résolution 130 (Rév.Busan, 2014), ainsi que sur les Recommandations UIT-T de la série X, y compris leurs Suppléments, selon qu'il conviendra,

charge le Directeur du Bureau de la normalisation des télécommunications

1 de continuer à tenir à jour , compte tenu de la base d'informations associée à la "Feuille de route pour la normalisation de la sécurité des 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;

2 de faire rapport chaque année au Conseil de l'UIT, conformément aux dispositions de la Résolution 130 (Rév. Busan, 2014), sur les progrès accomplis dans les domaines visés ci‑dessus;

3 de continuer de reconnaître le rôle que jouent d'autres organisations possédant une expérience et des compétences dans le domaine des normes de sécurité et d'assurer une coordination avec ces organisations, selon qu'il conviendra,

charge en outre le Directeur du Bureau de la normalisation des télécommunications

1 de continuer d'assurer le suivi des activités du SMSI relatives à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, en coopération avec les parties prenantes compétentes, en vue de partager des informations au plan mondial sur les initiatives en matière de cybersécurité nationales, régionales et internationales, et non discriminatoires;

2 de coopérer avec le BDT au sujet de toute question concernant la cybersécurité, conformément à la Résolution 45 (Rév.Dubaï, 2012);

3 compte tenu de la Résolution 45 (Rév. Dubaï, 2012), d' appuyer les projets mondiaux ou régionaux en matière de cybersécurité, notamment IMPACT, FIRST, OAS, APCERT LAC-CSIRT, et d'inviter tous les pays, en particulier les pays en développement, à y participer;

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

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

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

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