|  |  |  |
| --- | --- | --- |
| 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 13 auDocument 44-F** |
|  | **3 octobre 2016** |
|  | **Original: anglais** |
|  |
| Administrations des pays membres de la Télécommunauté Asie-Pacifique |
| proposition de modification de la résolution 50 de l'amnt‑12 – Cybersécurité |
|  |
|  |
| **Résumé:** | Dans le présent document, les Administrations des pays membres de la Télécommunauté Asie-Pacifique proposent d'apporter des modifications à la Résolution 50. |

Introduction

Depuis l'AMNT-12, l'UIT‑T a réalisé des progrès en ce qui concerne les activités relatives à la cybersécurité. L'environnement des menaces sur la cybersécurité a connu certains changements. Il est nécessaire de renforcer ces activités et d'étudier les questions de sécurité qui se font jour, pour la prochaine période d'études (2017-2020).

Il est nécessaire de mettre à jour la Résolution 50, pour tenir compte des changements et des progrès qui ont eu lieu depuis 2012.

Proposition

Les Administrations des pays membres de l'APT souhaitent proposer d'apporter des modifications à la Résolution 50 sur la cybersécurité, comme indiqué en annexe.

MOD APT/44A13/1

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 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;

*c)* les Résolutions pertinentes de l'Assemblée générale des Nations Unies, notamment la Résolution 57/239, la Résolution 58/199 et la Résolution 64/211, relatives à la création d'une culture mondiale de la cybersécurité et à la protection des infrastructures essentielles de l'information;

*d)* 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;

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

*f)* 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 revêtent l'infrastructure des TIC et les applications associées pour pratiquement toutes les formes d'activités sociales et économiques, y compris de nouveaux domaines de développement, tels que la quatrième révolution industrielle et l'Internet des objets;

*b)* que le nombre des cybermenaces et des cyberattaques augmente, tout comme notre dépendance à l'égard de l'Internet et d'autres réseaux qui sont essentiels pour avoir accès à des services et à l'information;

*c)* que la question de la cybersécurité est intersectorielle, et que l'environnement de la cybersécurité est complexe et diversifié, et compte de nombreuses parties prenantes différentes aux niveaux national, régional et mondial chargées d'identifier, d'examiner et de résoudre les problèmes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

*d)* que le Secteur de la normalisation des télécommunications de l'UIT (UIT-T) a adopté près de 300 normes sur l'instauration de la confiance et de la sécurité dans l'utilisation des TIC;

*e)* le rapport final sur la Question 22-1/1 (Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité) du Secteur du développement des télécommunications de l'UIT (UIT-D);

*f)* les travaux de normalisation sur les questions de sécurité relatives aux applications de l'Internet des objets (IoT) et des villes et des communautés intelligentes (SCC) qui ont des incidences sur la sécurité des internautes;

*g)* 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, aux fins de prévention, de préparation, de réaction et de rétablissement en cas d'incidents liés à la sécurité, et que l'UIT-T a un rôle à jouer à cet égard, dans le cadre de son mandat et de ses compétences;

*h)* le caractère dynamique de l'économie mondiale, où l'offre d'équipements électroniques et informatiques, qui fait partie de l'écosystème des fournisseurs, est très diversifiée et joue un rôle déterminant dans la gestion des menaces sur la cybersécurité;

*i*) les travaux qui ont été entrepris et qui sont en cours à l'UIT, notamment au sein de la Commission d'études 17 de l'UIT-T, de la Commission d'études 2 de l'UIT-D, et les travaux menés au titre du Plan d'action de Dubaï, adopté par la CMDT (Dubaï, 2014);

*j)* que l'UIT-T a un rôle à jouer dans le cadre de son mandat et de ses compétences s'agissant de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC et en ce qui concerne le point *g)* 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) 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,

consciente du fait

*a)* que l'UIT‑T et d'autres organisations internationales examinent actuellement, dans le cadre de diverses activités, des questions liées à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, notamment la stabilité, ainsi que des mesures visant à combattre le spam, les logiciels malveillants, les dispositifs contrefaits, etc., et à protéger les informations d'identification personnelle;

*b)* que la Commission d'études 17 de l'UIT-T, les Commissions d'études 1 et 2 de l'UIT-D et d'autres commissions d'études compétentes de l'UIT poursuivent leurs travaux sur les moyens techniques permettant d'assurer la sécurité des réseaux d'information et de communication, conformément aux Résolutions 50 et 52 (Rév. Dubaï, 2012) et aux Résolutions 45 et 69 (Rév. Dubaï, 2014);

*c)* que l'UIT‑T fournit aussi une assistance aux pays en développement pour l'instauration de la confiance et de la sécurité dans l'utilisation des TIC et qu'elle appuie la création d'équipes CIRT, y compris d'équipes CIRT chargées de la coopération entre les gouvernements, et qu'il importe d'assurer une coordination entre toutes les organisations concernées, conformément à la Résolution 58 (Rév. Dubaï, 2012),

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), ce qui a été réaffirmé lors de la réunion de haut niveau de l'Assemblée générale des Nations Unies sur l'examen d'ensemble de la mise en oeuvre des textes issus du Sommet mondial sur la société de l'information, en décembre 2015;

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

*c)* 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 incidents liés à la cybersécurité sont de nature et de type divers et variés (notamment, mais pas seulement: les attaques d'ingénierie sociale et les menaces persistantes avancées), qu'ils changent continuellement au cours du temps, et que les sources des attaques de cybersécurité sont parfois difficiles à identifier;

*b)* que les menaces sur la cybersécurité apparaissent en cas de failles dans les codes, les logiciels ou les matériels, ce qui peut être dangereux pour les infrastructures nationales et peut même nuire à la vie humaine, de sorte qu'il est nécessaire de gérer les failles au bon moment et de distribuer des correctifs pour les logiciels/matériels, au besoin;

*c)* que les données deviennent des ressoures essentielles des réseaux d'information et de télécommunication, ainsi que la principale cible des attaques de cybersécurité,

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 la gestion de l'identité, 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 l'UIT-D a un rôle à jouer dans la fourniture aux pays en développement d'une assistance adaptée aux conditions et aux exigences particulières de chaque pays en ce qui concerne les activités de renforcement des capacités en matière de cybersécurité;

*d)* 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,

décide

1 de continuer d'accorder à ces travaux un rang de priorité élevé à l'UIT-T, conformément à ses compétences et à ses connaissances spécialisées, notamment en favorisant une compréhension commune, entre les gouvernements et les autres parties prenantes, de l'instauration de la confiance et de la sécurité dans l'utilisation des TIC aux niveaux national, régional et international;

2 que toutes les commissions d'études de l'UIT-T doivent continuer d'évaluer les Recommandations existantes, les nouvelles Recommandations et les Recommandations en cours d'élaboration, quant à la robustesse de leur conception et aux risques d'une exploitation par des acteurs malveillants, en particulier l'exploitation des nouveaux services et des nouvelles applications (notamment, mais pas seulement: l'analyse des mégadonnées, l'informatique en nuage, les villes intelligentes, les services financiers numériques, l'informatique au bord du réseau mobile, l'informatique quantique, les réseaux mobiles de la 5ème génération, la cybersanté, l'Internet des objets, les réseaux pilotés par logiciel, la virtualisation des fonctions de réseau, l'Internet industriel, les réseaux électriques intelligents et les systèmes de transport intelligents, fondés sur les réseaux de télécommunication/TIC tels que les réseaux IMT-2020), qui seront pris en charge par l'infrastructure mondiale des télécommunications/TIC, et faire rapport au Groupe consultatif de la normalisation des télécommunications (GCNT), selon qu'il conviendra;

3 que l'UIT-T devrait entreprendre des études sur des normes relatives à la sécurité des mégadonnées, en se concentrant sur la protection des données tout au long de leur cycle de vie et sur les normes et les pratiques concernant l'évaluation de la sécurité des données;

4 que l'UIT-T, dans le cadre de son mandat et de ses compétences, doit continuer à sensibiliser au besoin de défendre les systèmes d'information et de télécommunication contre la menace de 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;

5 que l'UIT-T doit travailler en étroite collaboration avec l'UIT-D, en particulier dans le contexte de la Question 3/2 (Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité);

6 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;

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 la Commission d'études 17, en étroite collaboration avec toutes les autres commissions d'études de l'UIT-T, doit élaborer un plan d'action en vue d'examiner les Recommandations existantes, les Recommandations en cours d'élaboration et les nouvelles Recommandations de l'UIT-T quant aux failles de sécurité et continuer de faire rapport régulièrement sur la sécurité des télécommunications/TIC au GCNT;

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 les commissions d'études de l'UIT-T doivent se pencher sur la gestion des menaces sur la cybersécurité, couvrant les fonctions et les responsabilités qui incombent aux fournisseurs d'équipements, de logiciels et de services, ainsi qu'aux utilisateurs finals, pour faire en sorte que la gestion des cybermenaces soit efficace, et prévoyant clairement que plusieurs parties ont des responsabilités dans la réduction des menaces sur la cybersécurité;

11 que la Commission d'études 17 doit poursuivre ses travaux sur les moyens techniques de sécurité des réseaux TIC, en particulier sur des sujets pertinents traités dans la Résolution 130 (Rév. Busan, 2014),

charge le Directeur du Bureau de la normalisation des télécommunications

1 de dresser, 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 contribuer aux rapports annuels soumis au Conseil de l'UIT sur l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, comme indiqué dans la Résolution 130 (Rév. Busan, 2014);

3 de publier le rapport annuel sur les progrès accomplis en ce qui concerne les activités menées au titre de la "Feuille de route pour la normalisation de la sécurité des TIC" soumis au Conseil de l'UIT comme indiqué dans la Résolution 130 (Rév. Busan, 2014), et d'évaluer l'efficacité des travaux et plans actuels, en vue des futurs travaux, orientations ou feuilles de route;

4 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;

5 de continuer d'assurer la mise en oeuvre et le suivi des activités pertinentes du SMSI relatives à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC, en collaboration avec d'autres secteurs de l'UIT et 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;

6 de coopérer avec le BDT au sujet de toute question concernant la cybersécurité, en particulier la mise en oeuvre de la Résolution 45 (Rév. Dubaï, 2014);

7 de continuer de collaborer dans le cadre du Programme mondial cybersécurité (GCA) , selon qu'il conviendra, de développer des relations et de nouer des partenariats avec diverses organisations et initiatives régionales ou internationales liées à la cybersécurité;

8 d'encourager la collaboration avec l'UIT-D pour l'élaboration de principes et d'un cadre de gestion de la cybersécurité qui serviront de référence aux Etats Membres;

9 de déterminer et de répertorier les mesures concrètes propres à renforcer la sécurité dans l'utilisation des TIC au niveau international, sur la base de pratiques, de lignes directrices et de recommandations largement reconnues, que les Etats Membres pourront choisir d'appliquer pour améliorer leur capacité à lutter contre les cybermenaces et les cyberattaques, et de renforcer la coopération internationale pour instaurer la confiance et la sécurité dans l'utilisation des TIC, en tenant compte du Programme mondial cybersécurité (GCA) de l'UIT, et dans les limites des ressources financières disponibles,

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

1 à travailler en étroite collaboration en vue de renforcer la coopération aux niveaux régional et international, en tenant compte de la Résolution 130 (Rév. Busan, 2014), dans le but de renforcer la confiance et la sécurité dans l'utilisation des TIC, afin de réduire les risques et les menaces;

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

3 à travailler ensemble à l'élaboration de normes et de lignes directrices relatives à la cybersécurité pour contrer les cyberattaques;

4 à utiliser les Recommandations UIT-T pertinentes, en particulier les Recommandations UIT-T de la série X et leurs Suppléments.

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

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)