|  |  |  |
| --- | --- | --- |
| C:\Users\ponder\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\BDT-25th_anniversary_2017-Logo_411959-3_transparent.png | **Conférence mondiale de développement des télécommunications (CMDT-17)**  **Buenos Aires, Argentine, 9-20 octobre 2017** | C:\Users\murphy\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\PQ94T9LJ\bd_F_25Years_Horizontal-411959 (002).jpg |
|  | |  |
| SÉANCE PLÉNIÈRE | | **Document WTDC-17/36-F** |
|  | | **8 septembre 2017** |
|  | | **Original: espagnol** |
| Brésil (République fédérative du)/Mexique | | |
| PROPOSITIONS POUR LES TRAVAUX DE LA CONFÉRENCE | | |
|  | | |
|  | | |
| **Domaine prioritaire:**  – Questions confiées aux commissions d’étude  **Résumé:**  Modification de la Question 3/2 confiée à la Commission d'études 2 de l’UIT-D "Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité".  **Résultats attendus:**  Le Brésil et le Mexique invitent toutes les délégations à la CMDT-17 à examiner le présent document dans le cadre de la discussion sur la révision de la Question 3/2, tant sur le fond que sur la forme.  **Références:**  Question 3/2 | | |

COMMISSION D'ÉTUDES 2

**MOD** B/MEX/36/1

QUESTION 3/2

Sécurisation des réseaux d'information et de communication:  
bonnes pratiques pour créer une culture de la cybersécurité

# 1 Exposé de la situation ou du problème

Les utilisations des télécommunications et des technologies de l’information et de la communication trouvent de nombreuses applications d’une grande utilité pour stimuler le développement et la croissance socio-économique au niveau mondial. Malgré tous les avantages qu'elles offrent et leur utilité, ces technologies présentent également des risques et des menaces pour la sécurité. Qu'il s'agisse des finances personnelles ou des opérations commerciales, les infrastructures nationales et les services publics et privés sont de plus en plus gérés par le biais de réseaux d’information et de communication, et sont donc plus exposés aux attaques en tous genres.

Pour instaurer la confiance dans l’utilisation et l’exploitation des télécommunications/TIC pour tous les types d’applications et de contenus, en particulier ceux qui ont des incidences positives importantes, sur les plans économique et social, découlant de l'action menée par tous les acteurs qui jouent un rôle en matière de confidentialité, de protection des données personnelles et de sécurité des réseaux, et sur les utilisateurs des réseaux eux-mêmes, une étroite collaboration est nécessaire entre les autorités nationales des différents pays, les entreprises, les établissements universitaires et les utilisateurs.

Compte tenu de ce qui précède, il est devenu essentiel aujourd'hui de sécuriser les réseaux d'information et de communication et de créer une culture de la cybersécurité, pour des raisons très diverses:

a)la généralisation accélérée du déploiement et de l'utilisation des technologies de l'information et de la communication (TIC);

b)la cybersécurité reste une préoccupation pour tous et il faut donc aider tous les pays, en particulier les pays en développement, à protéger leurs réseaux de télécommunication/TIC contre les cyberattaques et les cybermenaces;

c)la nécessité d'assurer la sécurité de ces infrastructures interconnectées à l'échelle mondiale, si l'on veut concrétiser le potentiel de la société de l'information;

d)la nécessité d'agir à l'échelle nationale, régionale et internationale, et d'adopter une approche multi-parties prenantes, pour créer une culture mondiale de la cybersécurité englobant une coordination et des infrastructures législatives nationales appropriées, des capacités de veille, d'alerte et de rétablissement, des partenariats secteur public-secteur privé, et enfin l'inclusion de la société civile et des consommateurs;

e)par sa Résolution 57/239 intitulée "Création d'une culture mondiale de la cybersécurité", l'Assemblée générale des Nations Unies invite ses Etats Membres à "créer au sein de leur société une culture de la cybersécurité dans l'application et l'utilisation des technologies de l'information";

f) l'Assemblée générale des Nations Unies, dans ses Résolutions 68/167, 69/166 et 71/199 intitulée "Le droit à la vie privée à l'ère du numérique", affirme entre autres que "les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne, y compris le droit à la vie privée";

g) les bonnes pratiques en matière de cybersécurité doivent protéger et respecter le droit à la protection de la vie privée et la liberté d'expression tels qu'énoncés dans les parties pertinentes de la Déclaration universelle des droits de l'homme, de la Déclaration de principes de Genève adoptée par le Sommet mondial sur la société de l'information et d'autres instruments internationaux pertinents relatifs aux droits de l'homme;

h) la Déclaration de principes de Genève indique qu'"une culture globale de la cybersécurité doit être encouragée, développée et mise en oeuvre en coopération avec tous les partenaires et tous les organismes internationaux compétents", que le Plan d'action de Genève préconise le partage des meilleures pratiques en la matière et que l'Agenda de Tunis réaffirme la nécessité d'une culture mondiale de la cybersécurité, en particulier au titre de la grande orientation C5 (Créer la confiance et la sécurité dans l'utilisation des TIC);

i)l'UIT a été désignée par le SMSI (Tunis, 2005), dans le cadre de son programme de mise en oeuvre et de suivi, comme coordonnateur/modérateur principal pour la grande orientation C5 "Etablir la confiance et la sécurité dans l'utilisation des TIC";

j) l'Assemblée générale des Nations Unies, dans sa Résolution 70/125,qui constitue le Document final de sa réunion de haut niveau sur l’examen d’ensemble de la mise en œuvre des textes issus du SMSI, réaffirme, que le renforcement de la fiabilité et de la sécurité dans l’utilisation des technologies de l'information et de la communication pour le développement durable devrait 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;

k) conformément à la Déclaration du SMSI+10 sur la mise en oeuvre des résultats du SMSI, les gouvernements et toutes les parties prenantes concernées sont conscients de la nécessité d’une collaboration accrue pour résoudre les problèmes de fiabilité, de sécurité, de confidentialité et de protection des données personnelles, ainsi que de sécurité et de confiance dans l’utilisation des TIC;

l)la Résolution 45 (Rév.Dubaï, 2014) de la CMDT a préconisé d'améliorer la cybersécurité entre les Etats Membres intéressés;

m) par sa Résolution 130 (Rév. Busan, 2014), la PP a décidé de continuer de favoriser 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;

n) dans sa Résolution 50 (Rév.Hammamet, 2016), l'AMNT fait ressortir la nécessité de renforcer et de défendre les systèmes d'information et de télécommunication contre les cybermenaces et les cyberattaques, et de continuer 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;

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

p) divers efforts ont été entrepris, dans certains cas par des spécialistes du monde entier, pour contribuer à améliorer la sécurité des réseaux, comme l'élaboration de rapports sur les bonnes pratiques à l'UIT-D, la participation du Secrétariat de l'UIT au Programme mondial cybersécurité (GCA) et les activités de l'UIT‑D en matière de renforcement des capacités au titre du programme pertinent;

q)les gouvernements, les fournisseurs de services et les utilisateurs finals, en particulier dans les pays les moins avancés (PMA), sont confrontés à des problèmes particuliers en ce qui concerne l'élaboration de politiques et d'approches relatives à la sécurité adaptées à leurs conditions;

r)le problème du spam n'est toujours pas résolu, même s’il est nécessaire d’étudier les menaces émergentes et en évolution;

s)il est nécessaire de disposer de procédures de test simplifiées à un niveau de base pour évaluer la sécurité des réseaux de télécommunication, afin de promouvoir une culture de la sécurité.

# 2 Question ou thème à étudier

a) Favoriser l’intégrité des systèmes TIC, qui est indispensable à la poursuite de leur développement.

b) Examiner les méthodes et les bonnes pratiques permettant d'évaluer les incidences du spam sur un réseau, ainsi que les menaces émergentes et en évolution, et proposer les mesures et lignes directrices nécessaires, notamment les techniques de lutte contre le spam, les lois et les mesures réglementaires utilisables par les pays en développement, compte tenu des normes existantes et des outils disponibles.

c) Fournir des informations sur les problèmes que rencontrent actuellement les fournisseurs de services, les organismes de réglementation et d'autres parties prenantes dans le domaine de la cybersécurité.

d) Continuer de recueillir auprès des Etats Membres des données d'expérience concernant la cybersécurité, la confidentialité et la protection en ligne des enfants, et de recenser et d'étudier les thèmes communs qui s'en dégagent et, à partir de ces informations, établir des lignes directrices permettant aux Etats Membres d’élaborer des mécanismes efficaces en matière de sécurité et de confidentialité dans l’environnement numérique.

e) Analyser les défis en matière de cybersécurité que présentent l’Internet des objets, l’intelligence artificielle ou d’autres technologies émergentes, ainsi que les mesures à prendre pour affronter ces défis.

f) Examiner les perspectives et les bonnes pratiques en matière de protection de la vie privée et des données personnelles.

g) Promouvoir la sensibilisation des utilisateurs et le renforcement de leurs capacités en ce qui concerne la protection des données, la confidentialité et la cybersécurité.

h) Etablir un recueil des activités pertinentes dans le domaine de la cybersécurité menées par les Etats Membres, les organisations, le secteur privé et la société civile aux niveaux national, régional et international, activités auxquelles peuvent participer les pays en développement et tous les secteurs, y compris les renseignements obtenus au titre du paragraphe c) ci‑dessus.

i) Examiner les besoins spécifiques des personnes handicapées, en collaboration avec les responsables de l'étude des autres Questions pertinentes.

j) Réfléchir aux moyens permettant de prêter assistance aux pays en développement, en particulier les PMA, en ce qui concerne les problèmes liés à la cybersécurité.

k) Encourager la coopération entre les acteurs concernés, en vue d’organiser des séances ad hoc, des séminaires et des ateliers pour échanger des connaissances, des informations et de bonnes pratiques concernant les mesures et activités concrètes, efficaces et utiles à mettre en place pour renforcer la cybersécurité, renforcer la confiance et protéger les données et l’intégrité du réseau, compte tenu des risques existants et potentiels pour les TIC, en utilisant les résultats de l'étude, dont la tenue devra être la plus proche possible de celle des réunions de la Commission d'études 1 ou des réunions du groupe du rapporteur de la Commission d'études 1 pour la Question.

l) Travailler en collaboration avec les commissions d'études concernées de l'UIT-T et d'autres organisations de normalisation, le cas échéant, et compte tenu des informations et des données dont disposent ces entités.

m) Elaborer des lignes directrices qui facilitent la mise en place, aux niveaux national, régional et international, de mesures visant à lutter contre l’envoi massif de messages électroniques non sollicités.

n) compiler les données d’expérience de pays sur la réglementation ou les politiques mises en œuvre par les autorités de régulation des télécommunications, en vue de renforcer la confiance et la sécurité dans l’utilisation des télécommunications/TIC.

# 3 Résultats attendus

1 Rapports à l'intention des membres sur les questions visées aux § 2 *a)* à *n)* ci‑dessus. Ces rapports feront ressortir que des réseaux d'information et de communication sécurisés font partie intégrante de l'édification de la société de l'information et du développement socio-économique de tous les pays. Les problèmes de cybersécurité sont notamment les suivants: accès éventuellement non autorisé aux informations transmises sur des réseaux TIC, destruction et modification de ces informations et lutte contre le spam. Toutefois, il est possible d'atténuer les conséquences de ces problèmes en sensibilisant davantage l'opinion aux questions de cybersécurité, en concluant des partenariats public-privé efficaces, en faisant connaître les bonnes pratiques utilisées par les décideurs et les entreprises et en collaborant avec les autres parties prenantes.

En outre, une culture de la cybersécurité peut promouvoir la confiance des utilisateurs dans ces réseaux, favoriser une utilisation sécurisée, garantir la protection des données et de la vie privée tout en améliorant l'accès à ces réseaux et les opérations commerciales en ligne et permettre ainsi aux pays de mieux tirer parti des avantages socio‑économiques de la société de l'information.

2 Matériels didactiques destinés à être utilisés dans le cadre d'ateliers, de séminaires, etc.

3 Rassembler des connaissances, des informations et de bonnes pratiques concernant les mesures et activités concrètes, efficaces et utiles à mettre en place pour renforcer la cybersécurité dans les pays en développement, dans le cadre de séances ad hoc, de séminaires et d'ateliers.

4) Recommandations propres à faciliter l'adoption par les Membres, de mesures permettant de renforcer la confiance et la sécurité dans l’utilisation des TIC.

# 4 Echéance

Il est proposé que cette étude dure quatre ans et que des rapports d'activité préliminaires soient élaborés après un délai de 12, 24 et 36 mois.

# 5 Auteurs de la proposition/sponsors

Commission d'études 1 de l'UIT-D, Etats arabes, Proposition interaméricaine, Japon, République islamique d'Iran.

# 6 Origine des contributions

a) Contributions des Etats Membres et des Membres de Secteur.

b) Travaux des commissions d'études concernées de l'UIT-T et de l'UIT-R.

c) Documents pertinents d'organisations internationales ou régionales.

d) Organisations non gouvernementales compétentes s'occupant de la promotion de la cybersécurité et d'une culture de la sécurité.

e) Enquêtes, ressources en ligne;

f) Spécialistes dans le domaine de la cybersécurité.

g) Indice mondial de cybersécurité - GCI (Global Cybersecurity Index).

h) Autres sources, éventuellement.

# 7 Destinataires de l'étude

| Destinataires de l'étude | Pays développés | Pays en développement[[1]](#footnote-1)1 |
| --- | --- | --- |
| Décideurs en matière de télécommunication | Oui | Oui |
| Régulateurs des télécommunications | Oui | Oui |
| Fournisseurs de services/opérateurs | Oui | Oui |
| Equipementiers | Oui | Oui |
| Etablissements universitaires | Oui | Oui |

a) Destinataires de l'étude

Décideurs à l'échelle nationale et Membres de Secteur, autres parties prenantes intervenant dans les activités en matière de cybersécurité ou responsables de ces activités, en particulier celles des pays en développement.

b) Méthodes proposées pour la mise en oeuvre des résultats

Le programme d'étude vise avant tout à recueillir des informations ainsi que des bonnes pratiques. Il est censé avoir un caractère purement informatif et pourra être utilisé pour sensibiliser les Etats Membres et les Membres de Secteur aux questions de cybersécurité et pour attirer l'attention sur les informations, les outils et les bonnes pratiques disponibles; les résultats pourront être utilisés dans le cadre de sessions ad hoc, de séminaires et d'ateliers organisés par le BDT.

# 8 Méthodes proposées pour traiter la Question ou le thème

La Question sera traitée au sein d'une commission d'études pendant la période d'études de quatre ans (avec soumission de résultats préliminaires) et sera gérée par un rapporteur et des vice‑rapporteurs. Les Etats Membres et les Membres de Secteur pourront ainsi faire part de leur expérience et des enseignements qu'ils ont tirés en ce qui concerne la cybersécurité.

# 9 Coordination en ce qui concerne la sécurité

Coordination avec l'UIT-T, en particulier avec la Commission d'études 17qui est chargée d’instaurer la confiance et la sécurité dans l’utilisation des technologies de l’information et de la communication, ainsi qu'avec les autres organisations concernées, comme le Forum FIRST, le partenariat IMPACT, l'Equipe d'intervention en cas d'incident informatique pour l'Asie‑Pacifique (APCERT), le Comité CICTE de l'OEA, l'OCDE, l’Organisation de coopération économique Asie-Pacifique (APEC), les Registres Internet régionaux (RIR), les Groupes d'opérateurs de réseaux (NOG), le Groupe M3AAWG et l’UCENET. Compte tenu des compétences techniques spécialisées de ces groupes sur la question, tous les documents (questionnaires, rapports intérimaires, projets de rapport final, etc.) devraient être communiqués à la CE 17 pour observations et soumission de contributions, avant d'être présentés à l'ensemble des membres de la commission d'études de l'UIT-D pour observations et approbation.

# 10 Lien avec les programmes du BDT

Les responsables du programme du BDT relevant du Produit 3.1 de l'Objectif 3 faciliteront l'échange d'informations et utiliseront, s'il y a lieu, les résultats de l'étude pour atteindre les objectifs du programme et satisfaire les besoins des Etats Membres.

# 11 Autres informations utiles

–

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

1. 1 Par pays en développement, on entend 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)