**MOD** ACP/22A7/11

QUESTION 3/2

Bonnes pratiques et lignes directrices pour faire face aux menaces nouvelles et émergentes en matière de cybersécurité

# 1 Exposé de la situation ou du problème

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 prise de conscience de plus en plus nette, aux niveaux national, régional et international, de la nécessité d'élaborer et de promouvoir de bonnes pratiques, des normes, des directives techniques et des procédures propres à rendre les réseaux TIC moins vulnérables et moins exposés aux menaces;

e)la nécessité d'agir à l'échelle nationale et de coopérer à l'échelle régionale et internationale 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;

f)la nécessité d'opter pour une approche multi-parties prenantes, pour utiliser effectivement les divers moyens disponibles propres à instaurer la confiance dans l'utilisation des réseaux TIC;

g)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";

h) l'Assemblée générale des Nations Unies, dans sa Résolution 68/167 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";

i) 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;

j) 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);

k)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") et l'UIT-T, l'UIT-R, l'UIT-D et le Secrétariat général, compte tenu de cette responsabilité et en application des Résolutions pertinentes adoptées par la Conférence mondiale de développement des télécommunications (CMDT) (Doha, 2006 et Hyderabad, 2010), par la Conférence de plénipotentiaires (Antalya, 2006 et Guadalajara, 2010) ainsi que par l'Assemblée mondiale de normalisation des télécommunications (AMNT) (Johannesburg, 2008 et Dubaï, 2012), ont mené de nombreuses études visant à améliorer la cybersécurité;

l)le SMSI, dans ses conclusions (phases de Genève (2003) et de Tunis (2005)), a invité à établir la confiance et la sécurité dans l'utilisation des TIC;

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

n)conformément à son mandat, l'UIT-D devrait contribuer à rassembler les Etats Membres, les Membres de Secteur et d'autres spécialistes, afin d'échanger des données d'expérience et de mettre en commun les compétences en vue de sécuriser les réseaux TIC;

o)les résultats obtenus au titre de la Question 3/2 au cours de la dernière période d'études, au nombre desquels figurent de nombreux rapports et des contributions provenant du monde entier;

p) divers efforts ont été entrepris, dans certains cas par des spécialistes du monde entier, pour contribuer à améliorer la sécurité des réseaux, notamment les travaux des Etats Membres et des Membres de Secteur dans le cadre des activités de normalisation de l'UIT-T, 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)les Etats Membres et les opérateurs d'infrastructures tireraient profit de rapports additionnels décrivant de façon détaillée, d'une part, les diverses ressources, stratégies et outils disponibles pour instaurer la confiance dans l'utilisation des réseaux TIC et, d'autre part, le rôle de la coopération internationale à cet égard;

s)le problème du spam et des logiciels malveillants n'est toujours pas résolu;

t)l'évolution des méthodes de test, selon des critères de test communs pour les réseaux de télécommunication;

u)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) Examiner les méthodes et les bonnes pratiques permettant d'évaluer les incidences du spam et des logiciels malveillants sur un réseau, et proposer les mesures nécessaires, notamment les techniques de lutte contre le spam utilisables par les pays en développement, compte tenu des normes existantes et des outils disponibles.

b) 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.

c) Continuer de recueillir auprès des Etats Membres des données d'expérience concernant la cybersécurité et de recenser et d'étudier les thèmes communs qui s'en dégagent.

d) Continuer d'analyser les résultats de l'enquête sur la connaissance de la cybersécurité réalisée au cours de la dernière période d'études et publier une enquête actualisée, afin d'évaluer les progrès accomplis dans l'intervalle.

e) 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.

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

g) 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.

h) Continuer de recueillir des données d'expérience et de recenser les besoins, au niveau national, dans le domaine de la protection en ligne des enfants, en assurant une coordination avec les autres activités pertinentes.

i) 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 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.

j) Rassembler des données d'expérience nationales et recenser les besoins au niveau national, en ce qui concerne les critères communs et les tests de sécurité qui contribueraient à établir un cadre et des lignes directrices propres à accélérer la réalisation des tests de sécurité des équipements de télécommunication, 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.

# 3 Résultats attendus

1 Rapports à l'intention des membres sur les questions visées aux § 2 *a)* à *j)* 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 et les logiciels malveillants. 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 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

(A compléter) 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) Autres sources, éventuellement.

# 7 Destinataires de l'étude

| Destinataires de l'étude | Pays développés | Pays en développement[[1]](#footnote-8)1 |
| --- | --- | --- |
| Décideurs en matière de télécommunication | Oui | Oui |
| Régulateurs des télécommunications | Oui | Oui |
| Fournisseurs de services/opérateurs | Oui | Oui |
| Equipementiers | 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

Coordination avec l'UIT-T, en particulier avec la Commission d'études 17 ou la commission d'études qui lui succèdera, avec les responsables de l'étude de la Question 7/1 de l'UIT‑D sur les personnes handicapées, ainsi qu'avec les autres organisations concernées, notamment 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, les Registres Internet régionaux (RIR), les Groupes d'opérateurs de réseaux (NOG), le Groupe M3AAWG, l'association ISOC et le Forum GFCE. Compte tenu des compétences techniques spécialisées de ces groupes sur la question, tous les documents (questionnaires, rapports intérimaires, projets de rapport final, etc.) devraient leur être communiqués 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-8)