Conférence de plénipotentiaires (PP-06)
Antalya, 6-24 novembre 2006

SÉANCE PLÉNIÈRE

Document 24-F
4 septembre 2006
Original: anglais

Note du Secrétaire général

RAPPORT DE LA REUNION SUR LES MECANISMES DE COOPERATION EN MATIERE DE CYBERSECURITE ET DE LUTTE CONTRE LE SPAM (RESOLUTION 45 (DOHA, 2006) DE LA CMDT) (Genève, 31 août - 1er septembre 2006)

1 Introduction

Par sa Résolution 45 (Doha, 2006), la CMDT a chargé le Directeur du Bureau de développement des télécommunications (BDT) d'organiser et de coordonner avec le Programme 3 du Plan d'action de Doha, une réunion sur les mécanismes de coopération en matière de cybersécurité et de lutte contre le spam et de rendre compte de cette réunion à la Conférence de plénipotentiaires de 2006.

La réunion a été ouverte par M. Hamadoun TOURÉ, Directeur du BDT, qui, dans ses observations liminaires, a mis l'accent sur l'importance et la vaste portée de la cybersécurité. Il a également souligné qu'il était important que cette réunion aboutisse à des solutions concrètes propres à répondre aux besoins de tous les membres, compte tenu des problèmes particuliers que rencontrent les pays en développement et des solutions existantes.

M. Makhtar FALL (Sénégal) a présidé la réunion avec l'assistance de M. Alexander NTOKO du BDT. Il a présenté l'ordre du jour, qui a été adopté. Dans ses observations liminaires, il a également mis en évidence les problèmes rencontrés par les pays en développement dans ce domaine et a invité les participants à faire preuve d'esprit de collaboration et de consensus afin de parvenir à des résultats concrets.

Une cinquantaine de personnes ont participé à cette réunion de deux jours, notamment des délégués de 24 Etats Membres, des Membres de Secteur, des représentants de l'Office des Nations Unies contre la drogue et le crime, du Conseil de l'Europe, de la Commission européenne et de la Banque mondiale ainsi que des fonctionnaires de l'UIT (BDT, TSB et Secrétariat général). Les débats se sont tenus dans les six (6) langues de l'Union. On trouvera de plus amples informations et des documents d'information à l'adresse: http://www.itu.int/ITU-D/cybersecurity.

2 Présentation des contributions

A la suite de l'adoption de l'ordre du jour et des observations liminaires du Président, le BDT a présenté le mandat du Secteur du développement des télécommunications en ce qui concerne la cybersécurité et la lutte contre le spam. D'autres documents d'information ou de référence ont servi de base de discussion et de réflexion. Les pays et les entités ci-après ont fait des exposés sur les initiatives prises aux niveaux national, régional, multilatéral et international en matière de cybersécurité et de lutte contre le spam: Australie, Cisco Systems, Conseil de l'Europe, Commission européenne, Lituanie, Niger, Fédération de Russie, Soudan, République arabe syrienne (au nom des Etats arabes), Royaume-Uni, Etats-Unis d'Amérique, Ouzbékistan et Banque mondiale. Ces exposés ont permis de mettre en évidence des initiatives ayant trait au renforcement des capacités, à la législation, aux technologies, aux moyens d'intervention en cas d'incident, aux politiques générales et stratégies, aux partenariats et aux mécanismes d'application.

Outre les initiatives existantes, des délégués de pays en développement en ont présenté de nouvelles, notamment des propositions relatives à l'élaboration d'un Mémorandum d'accord. Les contributions ont confirmé l'existence de plusieurs initiatives prises pour l'essentiel par des pays développés et auxquelles les pays en développement participaient dans une moindre mesure.

3 Débats et analyse

Les délégués ont commenté les exposés et ont proposé quelques solutions pour aller de l'avant. La nécessité d'une coopération et d'une collaboration dans ce domaine a été soulignée dans la plupart des exposés et des débats. Les délégués sont convenus qu'il fallait exploiter les connaissances spécialisées existantes pour répondre aux besoins des pays en développement. La plupart des exposés et des débats ont fait ressortir des domaines dans lesquels des mesures aux niveaux national, régional et international étaient considérées nécessaires. Les activités ayant trait au renforcement des capacités, à la législation nationale, aux politiques et stratégies nationales, à des partenariats entre secteur public et secteur privé, aux mécanismes d'application, au partage de l'information, à la création d'entités chargées de la coordination au niveau national, aux moyens d'intervention en cas d'incident et aux solutions techniques ont été jugées importantes pour la coopération des Etats Membres en matière de cybersécurité et de lutte contre le spam. Les participants se sont accordés sur la nécessité de mettre en place certains mécanismes pour fournir une assistance aux pays demandeurs. Au cours des débats et de l'analyse des problèmes[1] et des initiatives existantes, il est clairement ressorti que si les cybermenaces et le spam devaient être combattus au niveau mondial, il fallait également tenir compte des besoins particuliers en la matière, notamment ceux des pays en développement. Pour que tous les pays intéressés (tant développés qu'en développement) participent à une initiative multilatérale d'envergure mondiale, il faudrait qu'ils remplissent tous un minimum de conditions au niveau national, notamment sur le plan de la législation, des capacités humaines et institutionnelles ainsi que des politiques et stratégies nationales concernées.

Les exposés et les débats ont permis d'identifier un certain nombre de domaines dans lesquels l'UIT-D devrait entreprendre des activités dans l'avenir en vue de résoudre les problèmes rencontrés par les pays en développement et les pays les moins avancés.

---

[1] Point c) du *reconnaissant* de la Résolution 45 (Doha, 2006) de la CMDT (voir l'Annexe).

Bien que de nombreuses activités devaient être réalisées au niveau national, il a été convenu qu'une coopération et une coordination entre les différentes parties prenantes et les différentes initiatives étaient nécessaires et que l'UIT-D avait là un rôle à jouer pour faciliter la mise en oeuvre des mesures relevant de son mandat et souhaitées par les Etats Membres. Il a été suggéré de définir certaines tâches concrètes dans ce contexte et de faire appel à l'expérience et aux compétences spécialisées de l'UIT pour les mener à bien.

Conformément à l'esprit et à l'objectif de la Résolution 45 (Doha, 2006), et compte tenu du consensus général selon lequel certains domaines d'activité appelaient une coordination allant au-delà des cadres existants, il s'est surtout agi, à ce stade, de convenir du type de mécanisme à mettre en place pour permettre à l'UIT-D de fournir l'assistance requise aux pays en développement. Trois options ont été examinées:

a) un Mémorandum d'accord conclu par les Etats Membres intéressés et dont le Secrétaire général de l'UIT serait le dépositaire;

b) un ou plusieurs cadres de coopération technique entre l'UIT et les Etats Membres et partenaires intéressés;

c) un projet sur la mise en oeuvre de la Résolution 45 (Doha, 2006) pour les pays intéressés, avec la participation d'entités ayant des compétences spécialisées reconnues dans ce domaine.

Ces trois options sont toutes destinées à établir des mécanismes propres à améliorer la coopération entre les parties prenantes intéressées en faisant appel aux compétences spécialisées et aux données d'expérience acquises par certaines entités ou dans le cadre d'initiatives existantes. Elles seraient non contraignantes pour les Etats Membres, ouvertes à la participation des pays intéressés et axées sur les besoins des pays qui ne font pas partie de cadres de coopération existants.

Le fait que le mandat de l'UIT-D en matière de cybersécurité et de lutte contre le spam repose en particulier sur trois éléments principaux - Programme 3 du Plan d'action de Doha, Question 22 confiée à la Commission d'études 1 de l'UIT-D et Résolution 45 (Doha, 2006) de la CMDT - a été l'une des considérations importantes. C'est pourquoi les résultats obtenus et les recommandations formulées à cette réunion ont porté sur des propositions qui ne reprenaient pas les décisions approuvées par les membres à la CMDT-06, mais visaient au contraire à favoriser des mécanismes qui, sans s'inscrire dans le cadre des décisions existantes, étaient néanmoins nécessaires et souhaités par les pays en développement.

4 Recommandations concernant des mesures futures

Il est résulté de la réunion thématique du SMSI sur la lutte contre le spam que les travaux consacrés à la cybersécurité et à la lutte contre le spam doivent passer par:

1) une législation efficace;

2) l'élaboration de mesures techniques;

3) l'établissement de partenariats avec le secteur privé, notamment avec des fournisseurs de services internet, des opérateurs de téléphonie mobile et des associations de vente directe;

4) la sensibilisation des consommateurs et des acteurs du secteur aux mesures antispam et aux pratiques en matière de sécurité sur l'internet.

5) la coopération internationale au niveau des pouvoirs publics, du secteur privé, des consommateurs, des entreprises et des groupes de lutte contre le spam, afin de traiter le problème d'une façon globale et coordonnée;

Outre les points susmentionnés, il est apparu au cours des débats et des exposés que les domaines énumérés ci-après (dans un ordre qui n'indique aucun degré de priorité) étaient eux aussi importants pour l'assistance aux Etats Membres et la coopération, activités auxquelles l'UIT-D était susceptible de participer avec des entités ayant des compétences spécialisées reconnues en matière de cybersécurité et de lutte contre le spam:

a) sensibilisation accrue à des questions de base;

b) législation nationale appropriée;

c) renforcement des capacités humaines et institutionnelles;

d) mécanismes d'application (renforcement des capacités);

e) politiques et stratégies nationales relatives à la cybersécurité;

f) partage de l'information entre les pays et les parties prenantes pertinentes;

g) création d'entités chargées de la coordination au niveau national;

h) suivi et évaluation des progrès accomplis dans le cadre des initiatives existantes;

i) intervention en cas d'incident, surveillance et dispositifs d'alerte;

j) évaluation des points faibles et des menaces en matière de cybersécurité;

k) outils et applications efficaces pour les réseaux et la cybersécurité;

l) partenariats;

m) coopération internationale.

Les participants à la réunion sont parvenus au consensus selon lequel l'UIT-D devrait jouer un rôle essentiel dans la coordination des initiatives existantes et mettre en place un cadre fédérateur qui rassemble ces initiatives en vue de répondre aux besoins des pays en développement.

Ils ont invité l'UIT-D à tenir compte, le cas échéant, des travaux pertinents d'autres parties prenantes ayant des connaissances reconnues dans des domaines spécialisés, par exemple l'UIT-T, le Plan d'action de Londres, la Banque mondiale, le Mémorandum d'accord Séoul-Melbourne (MoU), l'Office des Nations Unies contre la drogue et le crime, la Convention sur la cybercriminalité du Conseil de l'Europe, le Groupe de travail sur les télécommunications et l'information de la Coopération économique de la zone Asie-Pacifique (APEC TEL), l'Organisation de coopération et de développement économiques (OCDE) dans le cadre de sa contribution à la lutte contre le spam, et autres partenaires compétents.

Pour ce qui est des points énumérés ci-dessus, les participants ont recommandé que le BDT, au titre de la coordination du Programme 3, élabore un projet qui serve de mécanisme de mise en oeuvre de la Résolution 45 (Doha, 2006) de la CMDT. Sur la base des besoins et des priorités des pays en développement qui demandent l'assistance de l'UIT dans ce domaine, ce projet devrait tenir compte, le cas échéant, des entités ayant des compétences spécialisées reconnues en la matière ainsi que des initiatives existantes, notamment: l'UIT-T, le Plan d'action de Londres, la Banque mondiale, le Mémorandum d'accord Séoul-Melbourne (MoU), l'Office des Nations Unies contre la drogue et le crime, la Convention sur la cybercriminalité du Conseil de l'Europe, le Groupe de travail sur les télécommunications et l'information de la Coopération économique de la zone Asie-Pacifique (APEC TEL), l'Organisation de coopération et de développement économiques (OCDE) dans le cadre de sa contribution à la lutte contre le spam, et autres partenaires compétents.

En ce qui concerne le projet:

– Intitulé "Projet visant à renforcer la coopération en matière de cybersécurité et de lutte contre le spam", il débutera en 2007, durera 4 ans et fera partie du Plan opérationnel du BDT pour 2007.

– Des rapports d'avancement annuels seront présentés au Conseil de l'UIT.

– La mise en oeuvre du projet devrait tenir compte des décisions de la CMDT-06 concernant le mandat du Secteur du développement en matière de cybersécurité et de lutte contre le spam.

– Il devrait mettre l'accent en priorité sur l'assistance à fournir aux pays en développement dans les domaines d'activité susmentionnés que les participants à la réunion ont considéré comme essentiels pour la coopération en matière de cybersécurité et de lutte contre le spam.

– Pour ce qui est de la législation pertinente, il faudrait prendre en compte, si nécessaire, les travaux du Conseil de l'Europe pour aider les pays à élaborer une législation nationale qui soit compatible avec la Convention sur la cybercriminalité.

– La mise en œuvre des activités dans le cadre de ce projet devrait être fondée sur les demandes des pays, en particulier des pays en développement.

– Une fois la phase de conception terminée, il conviendrait de présenter le projet aux bailleurs de fonds potentiels, y compris les Etats Membres, des entités du secteur privé et des organisations internationales comme la Banque mondiale ou la Commission européenne.

ANNEXE

RESOLUTION 45 (Doha, 2006)

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

La Conférence mondiale de développement des télécommunications (Doha, 2006),

rappelant

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

b) l'appui résolu qu'elle a apporté au Programme 3 (Cyberstratégies et applications TIC), qui confirme que ce programme sera responsable au premier chef de la grande orientation C5 de l'Agenda de Tunis (C5 - Etablir la confiance et la sécurité dans l'utilisation des TIC);

c) les dispositions des paragraphes 35, 36 et 37 de la Déclaration de principes de Genève;

d) les dispositions du paragraphe 15 de l'Engagement de Tunis,

considérant

a) le rôle que jouent les TIC en tant qu'outil efficace pour promouvoir la paix, 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 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 (paragraphe 15 de l'Engagement de Tunis);

b) qu'il est nécessaire d'instaurer un climat de confiance et de sécurité pour l'utilisation des TIC (paragraphe 39 de Agenda de Tunis) et de poursuivre en justice les auteurs de cybercrimes, aux niveaux national et régional, compte tenu des cadres existants, par exemple des Résolutions 55/63 et 56/121 de l'Assemblée générale des Nations Unies sur "*la lutte contre l'exploitation des technologies de l'information à des fins criminelles*", et des initiatives régionales, dont la *Convention sur la cybercriminalité* du Conseil de l'Europe;

c) que les pertes considérables que les systèmes TIC ont subies en raison du problème toujours plus préoccupant de la cybercriminalité dans le monde devraient alarmer la communauté internationale dans son ensemble, et l'UIT en particulier;

d) qu'il est nécessaire de lutter contre le problème lié à la cybersécurité, notamment le spam, sur plusieurs fronts, y compris dans le cadre d'une coopération internationale, ce problème n'ayant pas bénéficié de la priorité voulue au titre du paragraphe 41 de à l'Agenda de Tunis;

e) les motifs qui ont présidé à l'adoption de la Résolution 37 (Istanbul, 2002) de la Conférence mondiale de développement des télécommunications relative à la réduction de la fracture numérique, compte tenu 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",

rappelant

a) la volonté et la détermination de toutes les parties intéressées d'édifier une société de l'information à dimension humaine, solidaire 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 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 du Millénaire pour le développement;

b) 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;

c) que le Sommet de Tunis a constitué une occasion unique de faire prendre conscience des avantages que les 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,

reconnaissant

a) 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 (paragraphe 42 de l'Agenda de Tunis);

b) la nécessité de protéger les dimensions éthiques de la société de l'information conformément à la Déclaration de principes et au Plan d'action de Genève (paragraphe 43 de l'Agenda de Tunis) et de lutter contre le terrorisme (paragraphe 44 de l'Agenda de Tunis) ainsi que l'importance de la continuité et de la stabilité de l'internet (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 (paragraphe 46 de l'Agenda de Tunis),

c) qu'il faut faire face efficacement aux problèmes et aux menaces résultant de l'utilisation des TIC 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 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;

d) que les TIC jouent un rôle dans la protection et l'épanouissement de l'enfant et qu'il convient de prendre des mesures propres à protéger les enfants contre tout abus et à assurer la défense de leurs droits dans le contexte des TIC, en insistant sur le fait que l'intérêt supérieur de l'enfant doit être une considération primordiale,

notant

a) que la Résolution 50 (Florianópolis, 2004) de l'Assemblée mondiale de normalisation des télécommunications relative à la cybersécurité traite uniquement de l'étude des aspects techniques permettant de réduire les incidences de ce phénomène;

b) que le spam est un problème important et qui ne cesse de s'aggraver pour les utilisateurs, les réseaux et l'internet dans son ensemble et que les questions du spam et de la cybersécurité devraient être traitées aux niveaux national et international appropriés,

exhorte les Etats Membres

à fournir l'appui nécessaire à la mise en oeuvre de la présente Résolution,

décide de charger le Directeur du Bureau de développement des télécommunications

1 d'organiser et de coordonner avec le Programme 3, sur la base des contributions des membres, des réunions à l'intention des Etats Membres et des Membres de Secteur, pour débattre des moyens d'améliorer la cybersécurité, notamment dans le cadre d'un Mémorandum d'accord conclu entre les Etats Membres intéressés ayant pour objet d'améliorer la cybersécurité et de combattre le spam;

2 de rendre compte des résultats de ces réunions à la Conférence de plénipotentiaires (Antalya, 2006).