Nations Unies A/C.2/64/L.8

Assemblée générale

Distr. limitée
22 octobre 2009
Français
Original : anglais

Soixante-quatrième session
Deuxième Commission
Point 55 c) de l'ordre du jour
Mondialisation et interdépendance : science et technique au service du développement

Australie, Canada, États-Unis d'Amérique, Îles Marshall, Israël, et Japon : projet de résolution

Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infrastructures essentielles de l'information

L'Assemblée générale,

Rappelant ses résolutions 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles, 57/239 du 20 décembre 2002 sur la création d'une culture mondiale de la cybersécurité et 58/199 du 23 décembre 2003 sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information,

Rappelant également ses résolutions 53/70 du 4 décembre 1998, 54/49 du 1er décembre 1999, 55/28 du 20 novembre 2000, 56/19 du 29 novembre 2001, 57/53 du 22 novembre 2002, 58/32 du 8 décembre 2003, 59/61 du 3 décembre 2004, 60/45 du 8 décembre 2005, 61/54 du 6 décembre 2006, 62/17 du 5 décembre 2007 et 63/37 du 2 décembre 2008 sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale,

Rappelant en outre les documents issus du Sommet mondial sur la société de l'information, tenu à Genève du 10 au 12 décembre 2003 (première phase) et à Tunis du 16 au 18 novembre 2005 (deuxième phase)[1], dans lesquels les États ont reconnu que la liberté d'expression et la libre circulation des informations, des idées et du savoir étaient essentielles pour la société de l'information actuelle et favorisaient le développement, et que, la confiance et la sécurité dans l'utilisation des technologies de l'information et des communications étant l'un des principaux piliers de cette société, une culture mondiale solide de la cybersécurité devait être encouragée, facilitée, développée et appliquée avec détermination,

[1] Voir A/C.2/59/3 et A/60/687.

Reconnaissant que les technologies de l'information en réseau sont de plus en plus indispensables pour la plupart des tâches essentielles de la vie quotidienne, le commerce, la prestation de biens et services, la recherche, l'innovation, l'entreprise et la libre circulation de l'information entre les personnes, les organisations et les pouvoirs publics,

Notant que les pouvoirs publics, les entreprises, la société civile et les particuliers sont de plus en plus dépendants d'un réseau mondial d'infrastructures informationnelles, et que cette dépendance ne fera que s'accroître,

Notant également que si les États n'ont pas assez accès aux technologies de l'information et n'utilisent pas suffisamment ces technologies, cela peut nuire à leur prospérité économique et sociale, et notant en particulier les besoins des pays les moins avancés dans le domaine des pratiques optimales et de la formation en matière de cybersécurité,

Se déclarant préoccupée par le fait que les menaces qui pèsent sur le fonctionnement fiable des réseaux d'information essentiels et sur l'intégrité des informations acheminées par ces réseaux gagnent en complexité et en gravité, au détriment du bien-être individuel, national et international,

Affirmant que la sécurité des infrastructures essentielles de l'information est une responsabilité que les gouvernements doivent assumer de façon systématique en tant que chefs de file à l'échelon national, en coordination avec les parties concernées, qui doivent quant à elles être informées des risques, des mesures préventives et des ripostes efficaces en la matière, compte dûment tenu de leurs rôles respectifs,

Reconnaissant que les efforts nationaux devraient être appuyés par des échanges d'information et des activités de collaboration aux niveaux national, régional et international, afin de faire face efficacement à la nature de plus en plus transnationale de ces menaces,

Notant les travaux menés par les organisations régionales et internationales compétentes pour renforcer la cybersécurité, en particulier par celles qui ont encouragé les efforts nationaux et la coopération internationale,

Prenant note du rapport de l'Union internationale des télécommunications de 2009 intitulé « Securing information and communication networks: best practices for developing a culture of cybersecurity » (Protéger les réseaux d'information et de communication : pratiques optimales pour instaurer une culture de la cybersécurité), qui expose une approche nationale approfondie de la cybersécurité respectueuse de la liberté d'expression, de la libre circulation de l'information et de la légalité,

Soulignant l'utilité d'une évaluation périodique des progrès réalisés dans le cadre des efforts nationaux visant à protéger les infrastructures essentielles de l'information,

1. *Invite* les États Membres à présenter, à titre volontaire, des exposés succincts de leurs principales initiatives en matière de cybersécurité et de protection des infrastructures essentielles de l'information, afin de mettre en lumière les résultats obtenus et les meilleures pratiques suivies au niveau national, les enseignements tirés et les domaines dans lesquels les efforts doivent se poursuivre;

2. *Propose*, à cet égard, aux États Membres d'utiliser éventuellement, s'il y a lieu, la méthode d'auto-évaluation jointe en annexe pour examiner les efforts nationaux consacrés à la cybersécurité et à la protection des infrastructures essentielles de l'information;

3. *Invite* tous les États Membres, qui ont élaboré des stratégies de cybersécurité et de protection des infrastructures essentielles de l'information, à signaler au Secrétaire général, d'ici sa soixante-cinquième session, les mesures et les pratiques les plus efficaces qui pourraient être utiles à d'autres États Membres, aux organisations régionales et internationales et aux acteurs du secteur privé et de la société civile dans le cadre de leurs efforts visant à instaurer une culture mondiale de la cybersécurité.

Annexe

Méthode d'auto-évaluation des efforts nationaux visant à protéger les infrastructures essentielles de l'information

Évaluation des besoins et des stratégies en matière de cybersécurité

1. Évaluer l'importance des technologies de l'information et des communications pour l'économie et la sécurité nationales, les infrastructures essentielles (transport, distribution d'eau et disponibilités alimentaires, santé publique, énergie, finance, services d'urgence, par exemple), et la société civile.

2. Déterminer les risques pour l'économie et la sécurité nationales, les infrastructures essentielles et la société civile qu'il faut gérer dans le domaine de la cybersécurité et de la protection des infrastructures essentielles de l'information.

3. Connaître les vulnérabilités des réseaux en service, le degré de gravité relatif des menaces qui pèsent sur chaque secteur à l'heure actuelle et le plan de gestion en vigueur; noter dans quelle mesure l'évolution du contexte économique, des priorités en matière de sécurité nationale et des besoins de la société civile influe sur ces estimations.

4. Déterminer les objectifs de la stratégie nationale en matière de cybersécurité et de protection des infrastructures essentielles de l'information, préciser ses objectifs, son degré actuel de mise en œuvre, les mesures permettant d'en évaluer l'état d'avancement, ses rapports avec les autres orientations au niveau national et la façon dont elle s'intègre dans les initiatives régionales et internationales.

Rôles et responsabilités des parties prenantes

5. Identifier les principales parties prenantes qui interviennent dans le domaine de la cybersécurité et de la protection des infrastructures essentielles de l'information et décrire le rôle de chacune d'entre elles dans l'élaboration des politiques et activités pertinentes, notamment :

- Les ministères ou organismes gouvernementaux nationaux, en précisant les principaux interlocuteurs et les responsabilités de chacun d'entre eux;
- Les autres organes des pouvoirs publics (locaux et régionaux) concernés;
- Les acteurs non gouvernementaux, notamment les entreprises, la société civile et les milieux universitaires;
- Les particuliers, en indiquant si, d'une manière générale, les utilisateurs d'Internet ont accès à une formation de base sur la façon d'éviter les menaces en ligne et s'il existe une campagne nationale de sensibilisation à la cybersécurité.

Processus politiques et participation

6. Recenser les mécanismes formels et informels qui permettent aux pouvoirs publics et aux entreprises de collaborer à l'élaboration de politiques et d'activités en matière de cybersécurité et de protection des infrastructures essentielles de l'information; déterminer les participants, leur(s) rôle(s) et leurs objectifs, les

méthodes permettant d'obtenir des contributions et de les traiter, et leur efficacité pour atteindre les objectifs voulus en matière de cybersécurité et de protection des infrastructures essentielles de l'information.

7. Recenser les autres instances ou structures dont on pourrait avoir besoin pour intégrer les orientations gouvernementales et non gouvernementales et les connaissances nécessaires à la réalisation des objectifs nationaux en matière de cybersécurité et de protection des infrastructures essentielles de l'information.

Coopération entre les secteurs public et privé

8. Réunir toutes les mesures prises et tous les plans établis en vue de développer la coopération entre les pouvoirs publics et le secteur privé, y compris les dispositions éventuelles en matière d'échange d'informations et de gestion des incidents.

9. Réunir toutes les initiatives en cours ou prévues visant à promouvoir les intérêts et à régler les problèmes communs, à la fois à ceux qui jouent un rôle dans les infrastructures essentielles et aux acteurs du secteur privé tributaires de la même infrastructure essentielle interconnectée.

Gestion des incidents et reprise après sinistre

10. Identifier l'organisme gouvernemental chargé de coordonner la gestion des incidents, y compris les fonctions de veille, d'alerte, d'intervention et de reprise après sinistre; les organismes gouvernementaux coopérants; les intervenants non gouvernementaux, notamment les entreprises et autres partenaires; et les dispositions éventuellement prises en matière de coopération et d'échange d'informations fiables.

11. Recenser séparément les capacités nationales d'intervention en cas d'incident informatique, notamment l'équipe d'intervention informatique éventuellement responsable au niveau national, ainsi que les attributions de cette équipe et les outils et les procédures en place pour assurer la protection des réseaux informatiques gouvernementaux et la diffusion d'informations aux fins de la gestion des incidents.

12. Recenser les réseaux et les processus de coopération internationale qui pourraient renforcer les interventions en cas d'incident et la planification d'urgence, en indiquant, lorsqu'il y a lieu, les partenaires et les mécanismes de coopération bilatérale et multilatérale.

Cadres juridiques

13. Examiner et actualiser les bases juridiques (notamment celles concernant la cybercriminalité, la confidentialité, la protection des données, le droit commercial, les signatures numériques et le codage) que l'adoption rapide des nouvelles technologies de l'information et des communications dont on est devenu tributaire a pu rendre obsolètes, en se fondant sur les conventions, mécanismes et précédents régionaux et internationaux en vigueur. Déterminer si votre pays est partie ou à l'intention de devenir partie à la Convention de Budapest sur la cybercriminalité, ou s'il a l'intention d'adopter les dispositions législatives correspondantes.

14. Déterminer la situation actuelle en ce qui concerne les responsabilités et les procédures nationales en matière de cybercriminalité, notamment les responsabilités

juridiques, les services nationaux compétents en matière de cybercriminalité et le niveau de coopération entre le ministère public, les juges et les législateurs en ce qui concerne les questions de cybercriminalité.

15. Déterminer dans quelle mesure les codes et cadres juridiques existants sont adéquats pour relever les défis actuels et futurs de la cybercriminalité, et d'une manière plus générale du cyberespace.

16. Déterminer si votre pays participe aux efforts internationaux de lutte contre la cybercriminalité, par exemple au réseau de points de contact, joignables 24 heures sur 24, sept jours sur sept (Réseau 24/7), et dans quelle mesure une telle participation contribuerait à la réalisation des objectifs nationaux en matière de cybersécurité.

17. Déterminer ce dont ont besoin les services nationaux de répression de votre pays pour coopérer avec leurs homologues internationaux à des enquêtes sur des affaires de cybercriminalité transnationale dans lesquelles l'infrastructure ou les auteurs des infractions se trouvent sur le territoire national mais les victimes résident ailleurs.

Instaurer une culture mondiale de la cybersécurité

18. Récapituler les mesures prises et les plans établis en vue d'instaurer la culture nationale de la cybersécurité mentionnée dans les résolutions 57/239 et 58/199 de l'Assemblée générale des Nations Unies, notamment pour mettre en œuvre un plan de cybersécurité pour les systèmes exploités par les pouvoirs publics, des programmes nationaux de sensibilisation, des programmes visant à toucher notamment les enfants et les particuliers, et des activités pour répondre aux besoins nationaux de formation en matière de cybersécurité et de protection des infrastructures essentielles de l'information.