Nations Unies A/C.2/64/L.8/Rev.1

Assemblée générale

Distr. limitée
20 novembre 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, Bulgarie, Canada, Estonie, États-Unis d'Amérique, France, Hongrie, Îles Marshall, Irlande, Israël, Japon, Nigéria, Panama, Pologne, Portugal, République de Corée, République de Moldova, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et Slovénie : projet de résolution

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

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 des Sommets mondiaux sur la société de l'information tenus en 2003 et 2005[1],

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

Sachant que la confiance et la sécurité dans l'utilisation des technologies de l'information et des communications sont l'un des principaux piliers de la société de l'information, et qu'une culture mondiale solide de la cybersécurité doit être encouragée, promue, développée et résolument appliquée,

Consciente du fait que les technologies de l'information en réseau sont de plus en plus indispensables pour de nombreuses tâches essentielles de la vie quotidienne, le commerce, la prestation de biens et services, la recherche, l'innovation et l'initiative économique ainsi que la libre circulation de l'information entre les personnes et les organisations, les gouvernements, les entreprises et la société civile,

Consciente également qu'il appartient aux gouvernements, aux entreprises et autres organisations, ainsi qu'aux propriétaires et utilisateurs individuels des technologies de l'information d'en assurer la sécurité, compte dûment tenu de leurs rôles respectifs, et de prendre des mesures de sécurisation renforcée,

Consciente en outre de l'importance du mandat du Forum sur la gouvernance de l'Internet, qui offre un espace de dialogue multipartite sur diverses questions, notamment les grandes questions de fond liées aux éléments clefs de la gouvernance de l'Internet, afin d'assurer la viabilité, la solidité, la sécurité, la stabilité et le développement de l'Internet, et réaffirmant que les gouvernements devraient exercer leur rôle et leurs responsabilités à égalité dans la gouvernance internationale de l'Internet et dans la préservation de la stabilité, de la sécurité et de la continuité de ce réseau,

Réaffirmant qu'il faut continuer de renforcer la coopération afin de permettre aux gouvernements d'exercer sur un pied d'égalité leur rôle et leurs responsabilités, sur les questions de politiques publiques internationales concernant l'Internet, mais non pas sur les questions techniques et opérationnelles courantes qui n'ont pas d'incidence sur ces politiques,

Consciente que chaque pays déterminera ses propres infostructures essentielles,

Réaffirmant qu'il importe d'exploiter le potentiel des technologies de l'information et des communications pour promouvoir la réalisation des objectifs de développement arrêtés au niveau international, notamment les objectifs du Millénaire pour le développement, sachant que les États qui n'ont pas assez accès à ces technologies et ne les utilisent pas suffisamment risquent de nuire à leur prospérité économique et réaffirmant également qu'il faut une coopération internationale pour lutter contre l'exploitation des technologies de l'information à des fins criminelles et créer une culture mondiale de la cybersécurité,

Soulignant la nécessité de redoubler d'efforts pour combler la fracture numérique afin de réaliser l'accès universel aux technologies de l'information et des communications et de protéger les infotructures essentielles en facilitant les transferts de technologies de l'information et le renforcement des capacités, surtout dans les 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 infostructures essentielles et sur l'intégrité des informations acheminées par ces réseaux acquièrent une complexité et une gravité accrues, au détriment du bien-être individuel, national et international,

Affirmant que la sécurité des infostructures essentielles 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 interventions efficaces en la matière, compte dûment tenu de leurs rôles respectifs,

Consciente que les efforts nationaux devraient être appuyés par des échanges d'information et des activités de collaboration au niveau international, afin de faire face efficacement à la nature de plus en plus transnationale de ces menaces,

Prenant note des travaux menés par les organisations régionales et internationales compétentes pour renforcer la cybersécurité, et rappelant le rôle qu'elles jouent pour ce qui est d'encourager les efforts nationaux et la coopération internationale,

Prenant note aussi du rapport établi en 2009 par l'Union internationale des télécommunications sur les pratiques optimales pour créer une culture de la cybersécurité et protéger ainsi les réseaux d'information et de communication, qui expose une approche nationale globale de la cybersécurité respectueuse de la liberté d'expression, de la libre circulation de l'information et de la légalité,

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

1. *Invite* les États Membres à utiliser éventuellement et s'il y a lieu la méthode d'auto-évaluation volontaire décrite en annexe pour examiner les efforts nationaux en matière de protection des infostructures essentielles et de cybersécurité afin de mettre en lumière les domaines dans lesquels les efforts doivent se poursuivre afin d'instaurer une culture mondiale de la cybersécurité;

2. *Invite* les États Membres et les organisations régionales et internationales concernées qui ont élaboré des stratégies de cybersécurité et de protection des infostructures essentielles à indiquer leurs meilleures pratiques et les mesures susceptibles d'aider d'autres États Membres dans leurs efforts de cybersécurisation, en communiquant ces renseignements au Secrétaire général pour compilation et diffusion auprès des États Membres.

Annexe

Méthode d'auto-évaluation volontaire des efforts nationaux visant à protéger les infostructures essentielles[a]

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, approvisionnement en 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 infostructures essentielles.

3. Connaître les vulnérabilités des réseaux en service, le degré de gravité relatif des menaces qui pèsent actuellement sur chaque secteur 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 infostructures essentielles, préciser ses objectifs, son niveau 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'elles dans l'élaboration des politiques et activités pertinentes, notamment :

- Les ministères ou organismes gouvernementaux, en précisant les principaux interlocuteurs et les responsabilités de chacun d'entre eux;
- Les autres entités gouvernementales (locales et régionales) concernées;
- Les intervenants 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.

[a] Cet outil peut être utilisé partiellement ou dans son intégralité par les États Membres quand et s'il le jugent opportun, afin de les aider dans les efforts qu'ils déploient pour protéger leurs infostructures essentielles et renforcer leur cybersécurité.

Élaboration de 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 infostructures essentielles; identifier les participants et déterminer leur(s) rôle(s) et leurs objectifs, les méthodes permettant d'obtenir des contributions et de les traiter, ainsi que 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 infostructures essentielles.

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 dispositifs éventuels d'échange d'informations et de gestion des incidents.

9. Réunir toutes les initiatives en cours ou prévues visant à promouvoir les intérêts mutuels 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 dispositifs éventuels 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 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 mécanismes 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 dispositifs de coopération bilatérale et multilatérale.

Cadres juridiques

13. Examiner et actualiser les textes juridiques (notamment ceux 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 a

légiféré en matière d'enquête et de poursuites pour cybercriminalité, en ayant à l'esprit les dispositifs existants tels que les résolutions 55/63 et 56/121 de l'Assemblée générale des Nations Unies concernant la lutte contre l'exploitation des technologies de l'information à des fins criminelles, ainsi que des initiatives régionales comme la Convention du Conseil de l'Europe sur la cybercriminalité.

14. Déterminer la situation actuelle en ce qui concerne les procédures et mécanismes nationaux de lutte contre la cybercriminalité, y compris les textes juridiques, les structures nationales en matière de cybercriminalité et le degré de sensibilisation des procureurs, des juges et des législateurs aux problèmes de cybercriminalité.

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

16. Examiner la participation de votre pays aux efforts entrepris à l'échelon international pour lutter contre la cybercriminalité, par exemple au réseau de points de contact joignables 24 heures sur 24 et sept jours sur sept (Réseau 24/7).

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'infostructure ou les auteurs des infractions se trouvent sur le territoire national mais les victimes résident ailleurs.

Créer une culture mondiale de la cybersécurité

18. Récapituler les mesures prises et les plans établis en vue de créer 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 d'information notamment à l'intention des enfants et des particuliers, et des activités visant à répondre aux besoins nationaux de formation en matière de cybersécurité et de protection des infostructures essentielles.