Assemblée générale

Distr. générale
17 mars 2010

Soixante-quatrième session
Point 55, *c*, de l'ordre du jour

Résolution adoptée par l'Assemblée générale le 21 décembre 2009

[*sur la base du rapport de la Deuxième Commission (A/64/422/Add.3)*]

64/211. 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 du Sommet mondial sur la société de l'information qui s'est tenu à Genève du 10 au 12 décembre 2003 (première phase) et à Tunis du 16 au 18 novembre 2005 (deuxième phase)[1],

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,

Sachant également que les moyens informatiques 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 pouvoirs publics, les entreprises et la société civile,

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

Considérant qu'il appartient aux pouvoirs publics, aux entreprises et aux organisations, ainsi qu'aux propriétaires et utilisateurs individuels des technologies de l'information d'en assurer et d'en renforcer la sécurité, compte dûment tenu de leurs rôles respectifs,

Consciente de l'importance du mandat du Forum sur la gouvernance d'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 tous les gouvernements devraient avoir un rôle et des responsabilités égaux en ce qui concerne la gouvernance internationale de l'Internet et la préservation de la stabilité, de la sécurité et de la continuité de ce réseau,

Réaffirmant que la coopération doit continuer d'être renforcée pour que les gouvernements puissent jouer leur rôle et exercer leurs responsabilités sur un pied d'égalité en ce qui concerne les politiques publiques internationales concernant l'Internet mais non les questions techniques et opérationnelles courantes qui n'ont pas d'incidence sur ces politiques,

Sachant que chaque pays déterminera lesquelles de ses infostructures sont 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 si les États n'ont pas l'accès voulu à ces technologies ou ne les utilisent pas suffisamment, cela risque de nuire à leur prospérité économique, et réaffirmant également que la coopération est un bon moyen de lutter contre l'exploitation des technologies de l'information à des fins criminelles et de 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 infostructures essentielles en facilitant les transferts de technologies de l'information aux pays en développement, surtout les moins avancés, ainsi que le renforcement des capacités de ces pays, dans les domaines des pratiques optimales et de la formation en matière de cybersécurité,

Se déclarant préoccupée par le fait que les menaces qui pèsent sur le bon fonctionnement des infostructures essentielles et sur l'intégrité des informations acheminées par ces réseaux sont de plus en plus complexes et de plus en plus graves, ce qui nuit aux intérêts individuels, nationaux et internationaux,

Affirmant que la sécurité des infostructures essentielles est une responsabilité que les gouvernements doivent assumer de façon systématique et un domaine dans lequel ils doivent prendre l'initiative à l'échelon national, en coordination avec les parties concernées qui doivent, quant à elles, être conscientes des risques, des mesures préventives et des interventions efficaces en la matière, compte tenu de leurs rôles respectifs,

Considérant que les efforts nationaux doivent être appuyés par des échanges d'information et des activités de collaboration au niveau international, compte tenu de la nécessité de faire face à des menaces qui, de plus en plus, ont un caractère transnational,

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

Prenant note également du rapport sur la sécurisation des réseaux d'information et de communication et les pratiques optimales propres à créer une culture de cybersécurité que l'Union internationale des télécommunications a élaboré en 2009, lequel met l'accent sur une approche nationale globale de la cybersécurité qui respecte la liberté d'expression, la libre circulation de l'information et la légalité,

Jugeant utile l'évaluation périodique des progrès accomplis dans le cadre des efforts nationaux visant à protéger les infostructures essentielles,

1. *Invite* les États Membres à utiliser, si et quand ils le jugent opportun, la méthode d'auto-évaluation volontaire des efforts nationaux visant à protéger les infostructures essentielles, décrite en annexe, pour évaluer les efforts qu'ils font à cet égard et pour renforcer leur cybersécurité, afin de mettre en lumière les domaines dans lesquels les efforts doivent se poursuivre pour que s'instaure une culture mondiale de cybersécurité ;

2. *Engage* les États Membres et les organisations régionales et internationales concernées qui ont élaboré des stratégies de cybersécurité et de protection des infostructures essentielles à faire connaître leurs pratiques optimales 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.

66e séance plénière
21 décembre 2009

Annexe

Méthode d'auto-évaluation volontaire des efforts nationaux visant à protéger les infostructures essentielles[2]

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 en vivres, santé publique, énergie, finances et protection civile, par exemple) et la société civile.

2. Déterminer les risques qui existent, du point de vue de la cybersécurité et de la protection des infostructures essentielles, pour l'économie et la sécurité nationales, les infrastructures essentielles et la société civile.

3. Connaître les vulnérabilités des réseaux utilisés, la gravité relative des menaces qui pèsent sur chaque secteur et le plan de gestion en vigueur ; noter dans quelle mesure l'évolution du contexte économique, des priorités de sécurité nationale et des besoins de la société civile influe sur ces éléments.

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

4. Déterminer les objectifs de la stratégie nationale de cybersécurité et de protection des infostructures essentielles, en préciser les objectifs et le niveau de mise en œuvre, décrire les mesures permettant d'en évaluer l'état d'avancement et les rapports qui existent avec les autres objectifs nationaux et la façon dont la stratégie s'intègre dans les initiatives régionales et internationales.

Rôles et responsabilités des parties prenantes

5. Recenser les principales parties prenantes qui interviennent dans le domaine de la cybersécurité et de la protection des infostructures essentielles et décrire le rôle de chacune dans l'élaboration des politiques et activités pertinentes, notamment :

- Les ministères ou organismes gouvernementaux (préciser les principaux interlocuteurs et les responsabilités de chacun) ;
- Les autres entités gouvernementales (locales et régionales) concernées ;
- Les intervenants non gouvernementaux, notamment les entreprises, la société civile et les établissements universitaires ;
- Les particuliers (indiquer 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).

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 ; recenser les participants et déterminer leur(s) rôle(s) et leurs objectifs, les méthodes permettant d'obtenir des contributions et de les traiter, et déterminer l'utilité de ces contributions du point de vue de la réalisation des objectifs de cybersécurité et de protection des infostructures essentielles.

7. Recenser les autres instances ou structures dont le pays pourrait avoir besoin pour intégrer les perspectives gouvernementales et non gouvernementales et les connaissances nécessaires à la réalisation des objectifs nationaux de cybersécurité et de protection des infostructures essentielles.

Coopération entre les secteurs public et privé

8. Recenser 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. Recenser toutes les initiatives en cours ou prévues visant à promouvoir les intérêts communs et à régler les problèmes qui concernent à la fois ceux qui jouent un rôle touchant les infostructures essentielles et les acteurs du secteur privé qui sont tributaires de la même infostructure essentielle interconnectée.

Gestion des incidents et reprise après sinistre

10. Déterminer quel organisme gouvernemental est chargé de coordonner la gestion des incidents (veille, alerte, intervention et reprise après sinistre) et recenser les organismes gouvernementaux qui coopèrent avec lui, les intervenants non gouvernementaux, notamment les entreprises et autres partenaires, et les dispositifs de coopération et d'échange d'informations fiables.

11. Recenser séparément les capacités nationales d'intervention en cas d'incident informatique, déterminer s'il existe une équipe d'intervention informatique ayant des attributions au niveau national et, dans ce cas, quelles sont les attributions de cette équipe et quels outils et procédures ont été mis en place pour assurer la protection des réseaux informatiques de l'État et la diffusion d'informations relatives à la gestion des incidents.

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

Cadres juridiques

13. Examiner les textes juridiques (notamment ceux qui se rapportent à la cybercriminalité, la confidentialité, la protection des données, le droit commercial, les signatures numériques et le codage) et actualiser ceux qui seraient devenus obsolètes du fait de l'adoption rapide de nouvelles technologies de l'information et des communications et de la dépendance du pays vis-à-vis de ces technologies, en se fondant sur les conventions, mécanismes et précédents régionaux et internationaux. Déterminer si le pays a légiféré en matière d'enquêtes 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 relatives à la lutte contre l'exploitation des technologies de l'information à des fins criminelles, ainsi que des initiatives régionales telles que la Convention du Conseil de l'Europe sur la cybercriminalité.

14. Déterminer quelle est la situation en ce qui concerne les procédures et mécanismes nationaux de lutte contre la cybercriminalité, y compris les textes juridiques, et les structures nationales, et dans quelle mesure les procureurs, les juges et les législateurs sont sensibilisés aux problèmes de cybercriminalité.

15. Déterminer dans quelle mesure les codes et textes juridiques existants sont adéquats compte tenu des difficultés qui sont et seront à l'avenir associées à la cybercriminalité et, d'une manière plus générale, au cyberespace.

16. Évaluer la participation du pays aux initiatives internationales de lutte contre la cybercriminalité, par exemple au Réseau de contacts contre la cybercriminalité qui fonctionne 24 heures sur 24 et sept jours sur sept.

17. Déterminer ce dont ont besoin les services nationaux de répression pour coopérer avec leurs homologues d'autres pays à des enquêtes sur des affaires de cybercriminalité transnationale dans lesquelles l'infostructure est située sur le territoire national ou les auteurs des infractions résident sur ce territoire, mais les victimes résident ailleurs.

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, 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 s'adressant notamment aux particuliers, enfants compris, et des activités de formation en matière de cybersécurité et de protection des infostructures essentielles.