Nations Unies A/C.2/57/L.10

Assemblée générale

Distr. limitée
18 octobre 2002
Français
Original: anglais

Cinquante-septième session
Deuxième Commission
Point 84 c) de l'ordre du jour
Questions de politique macroéconomique : science et technique au service du développement

États-Unis d'Amérique et Japon : projet de résolution

Création d'une culture mondiale de la cybersécurité

L'Assemblée générale,

Notant que les gouvernements, les entreprises et les autres organisations et les utilisateurs individuels sont de plus en plus tributaires des technologies de l'information pour les approvisionnements en biens et services essentiels, pour la conduite de leurs opérations et pour l'échange d'information,

Constatant que le besoin de cybersécurité grandit à mesure qu'augmente la participation des différents pays à l'économie numérique,

Rappelant ses résolutions 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001,

Consciente que l'efficacité de la cybersécurité n'est pas une simple affaire de pratiques gouvernementales et répressives, mais qu'elle exige une action préventive et le soutien de la société tout entière,

Consciente également que la technologie ne saurait à elle seule assurer la cybersécurité et qu'il faut donner la priorité à sa planification et sa gestion dans toute la société,

Sachant que, selon leurs rôles respectifs, les gouvernements, les entreprises, les autres organisations et les propriétaires et utilisateurs individuels des technologies de l'information doivent être avertis des risques liés à la cybersécurité et des parades correspondantes, assumer leurs responsabilités et prendre des dispositions pour renforcer la sécurité de ces technologies,

Notant que désormais, par suite des progrès de l'interconnectivité, les systèmes et réseaux d'information se trouvent exposés à des menaces et présentent des points vulnérables toujours plus nombreux et plus divers, qui soulèvent des questions de sécurité inédites pour tous les utilisateurs d'ordinateur,

02-64805 (F) 181002 181002

Prenant note des travaux des organisations internationales et régionales sur le renforcement de la cybersécurité et de la sécurité des technologies de l'information, notamment la Déclaration sur la sécurité des infrastructures de l'information et des communications, adoptée par la cinquième Réunion ministérielle de l'APEC sur les télécommunications et l'industrie de l'information, tenue les 29 et 30 mai 2002 à Shanghai (Chine), les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information, de la culture de la sécurité, adoptées, le 25 juillet 2002, par le Conseil de l'Organisation de coopération et de développement économiques (OCDE), et le document intitulé « Sécurité des réseaux et de l'information : proposition pour une approche politique européenne », adressé le 6 juin 2000 par la Commission des communautés européennes au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions,

1. *Adopte* les principes annexés à la présente résolution, applicables aux fins de la création d'une culture mondiale de la cybersécurité;

2. *Invite* les États Membres à tenir compte de ces principes dans leurs efforts pour instaurer à travers toutes leurs sociétés une culture de la cybersécurité dans l'application et l'utilisation des technologies de l'information;

3. *Invite* les États Membres à tenir compte de ces principes et de la nécessité d'une culture mondiale de la cybersécurité dans la préparation du Sommet mondial de la société de l'information qui aura lieu en décembre 2003 à Genève.

Annexe

Principes applicables aux fins de la création d'une culture mondiale de la cybersécurité

Les progrès rapides des technologies de l'information ont changé la manière dont gouvernements, entreprises, autres organisations et utilisateurs individuels qui développent, possèdent, fournissent, entretiennent et utilisent les systèmes et réseaux d'information (« les parties prenantes ») doivent envisager la cybersécurité. Une culture mondiale de la cybersécurité exigera de toutes les parties prenantes qu'elles s'attachent aux neuf principes complémentaires suivants :

a) *Sensibilisation.* Les parties prenantes doivent être averties de la nécessité d'assurer la sécurité des systèmes et réseaux d'information et de ce qu'elles peuvent faire pour renforcer la sécurité;

b) *Responsabilité.* Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information, selon leurs rôles respectifs. Elles doivent régulièrement examiner leurs propres politiques, pratiques, mesures et procédures pour s'assurer que celles-ci sont adaptées à leur environnement;

c) *Réaction.* Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir et détecter les incidents de sécurité et pour y faire face. Elles doivent échanger l'information dont elles disposent sur les menaces et les points vulnérables, selon que de besoin, et mettre en place des procédures permettant une coopération rapide et efficace pour prévenir et détecter ces incidents ainsi que pour y faire face. Cela peut impliquer des échanges d'information et une coopération transfrontières;

d) *Éthique.* Étant donné l'omniprésence des systèmes et réseaux d'information dans les sociétés modernes, les parties prenantes doivent respecter les

intérêts légitimes d'autrui et être conscientes du tort qu'elles peuvent causer à autrui par leur action ou leur inaction;

e) *Démocratie*. La sécurité doit être assurée dans le respect des valeurs reconnues par les sociétés démocratiques, et notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et de la communication, la protection adéquate de l'information de caractère personnel, l'ouverture et la transparence;

f) *Évaluation des risques*. Toutes les parties prenantes doivent, pour déceler les dangers qui menacent et les points vulnérables, procéder périodiquement à des évaluations des risques qui soient suffisamment larges pour couvrir l'ensemble des principaux facteurs internes et externes, tels la technologie, les facteurs physiques et humains, les politiques et les services de tierces parties, impliquant des conséquences pour la sécurité, qui permettent de déterminer le niveau acceptable de risque et qui facilitent la sélection des mesures de contrôle appropriées pour gérer le risque de préjudices susceptibles d'être causés aux systèmes et réseaux d'information, selon la nature et l'importance de l'information à protéger;

g) *Conception et mise en oeuvre de la sécurité*. Les parties prenantes doivent intégrer la sécurité, comme élément essentiel, à la planification et la conception, au fonctionnement et à l'utilisation des systèmes et réseaux d'information;

h) *Gestion de la sécurité*. Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité qui repose sur l'évaluation des risques et qui soit dynamique et globale, pour couvrir leurs activités à tous les niveaux et leurs opérations sous tous les rapports;

i) *Réévaluation*. Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et apporter les modifications appropriées à leurs politiques, pratiques, mesures et procédures de sécurité pour faire face aux menaces et remédier aux points vulnérables qui sont nouveaux ou en cours d'évolution.