Assemblée générale

Distr. générale
31 janvier 2003

Cinquante-septième session
Point 84, *c*, de l'ordre du jour

Résolution adoptée par l'Assemblée générale

[*sur le rapport de la Deuxième Commission (A/57/529/Add.3)*]

57/239. Création d'une culture mondiale de la cybersécurité

L'Assemblée générale,

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

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

Rappelant ses résolutions 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001, qui établissent le cadre légal de la lutte contre l'exploitation des technologies de l'information à des fins criminelles,

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 et 57/53 du 22 novembre 2002 sur les progrès de la téléinformatique dans le contexte de la sécurité internationale,

Consciente que l'efficacité de la cybersécurité n'est pas une simple affaire de pratiques administratives ou 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,

Sachant également que les écarts entre les pays concernant l'accès aux technologies de l'information et leur utilisation peuvent nuire à l'efficacité de la coopération internationale en matière de lutte contre l'exploitation des technologies de l'information à des fins criminelles et de création d'une culture mondiale de la cybersécurité, et notant la nécessité de faciliter le transfert des technologies de l'information, en particulier vers les pays en développement,

Consciente de l'importance de la coopération internationale dans l'instauration de la cybersécurité, sous la forme d'un soutien aux efforts déployés sur le plan national pour renforcer les capacités humaines, accroître les possibilités de formation et d'emploi, améliorer les services publics et la qualité de la vie, en tirant parti de technologies et de réseaux très modernes, fiables et sûrs de l'information et des communications et en favorisant l'accès universel,

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,

Prenant note des travaux des organisations internationales et régionales compétentes sur le renforcement de la cybersécurité et de la sécurité des technologies de l'information,

1. *Prend note* des éléments à prendre en considération pour la création d'une culture mondiale de la cybersécurité, présentés en annexe à la présente résolution ;

2. *Invite* toutes les organisations internationales compétentes à prendre en considération, entre autres choses, ces éléments pour la création d'une telle culture dans toute future activité relative à la cybersécurité ;

3. *Invite* les États Membres à tenir compte de ces éléments, notamment dans leurs efforts pour créer au sein de leur société une culture de la cybersécurité dans l'application et l'utilisation des technologies de l'information ;

4. *Invite* les États Membres et toutes les organisations internationales compétentes à tenir compte, notamment, de ces éléments et de la nécessité d'une culture mondiale de la cybersécurité dans la préparation du Sommet mondial sur la société de l'information qui aura lieu à Genève du 10 au 12 décembre 2003 et à Tunis en 2005 ;

5. *Souligne* la nécessité de faciliter le transfert des technologies et la mise en place de capacités en matière d'information dans les pays en développement, afin de les aider à prendre des mesures dans le domaine de la cybersécurité ;

78e séance plénière
20 décembre 2002

Annexe

Éléments à prendre en considération pour créer une culture mondiale de la cybersécurité

Les progrès rapides des technologies de l'information ont changé la manière dont pouvoirs publics, entreprises, autres organisations et utilisateurs individuels qui développent, possèdent, fournissent, gèrent, 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 éléments complémentaires suivants :

a) *Sensibilisation.* Les parties prenantes doivent être conscientes de la nécessité d'assurer la sécurité des systèmes et réseaux d'information et de ce qu'elles peuvent faire pour renforcer cette 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 et 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 au besoin échanger l'information dont elles disposent sur les menaces et les points vulnérables, 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'informations 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, notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, 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 que la technologie, les facteurs physiques et humains, les politiques et les services de tierces parties ayant 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 œuvre de la sécurité.* Les parties prenantes doivent intégrer la sécurité, comme élément essentiel, à la planification et à 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 reposant sur l'évaluation des risques, qui soit dynamique et capable de 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 corriger les points vulnérables à mesure qu'ils se présentent ou se transforment.