Assemblée générale

Distr. générale
30 janvier 2004

Cinquante-huitième session
Point 91, *b*, de l'ordre du jour

Résolution adoptée par l'Assemblée générale

[*sur le rapport de la Deuxième Commission (A/58/481/Add.2)*]

58/199. Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information

L'Assemblée générale,

Rappelant ses résolutions 57/239 du 20 décembre 2002 sur la création d'une culture mondiale de la cybersécurité, 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, et 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,

Constatant l'importance croissante des technologies de l'information pour la promotion du développement socioéconomique et la fourniture des biens et services essentiels, ainsi que pour la conduite des activités économiques et l'échange d'informations par les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels,

Notant les liens de plus en plus étroits qui existent entre les infrastructures essentielles de la plupart des pays – dont celles qui sont utilisées, notamment, pour la production, la transmission et la distribution d'énergie, les transports aériens et maritimes, les services bancaires et financiers, le commerce électronique, l'approvisionnement en eau, la distribution alimentaire et la santé publique – et les infrastructures essentielles de l'information qui, toujours plus, relient et touchent leurs opérations,

Considérant que chaque pays déterminera quelles sont ses propres infrastructures essentielles de l'information,

Sachant que cette interdépendance technologique grandissante repose sur un réseau complexe d'éléments des infrastructures essentielles de l'information,

Notant que désormais, par suite des progrès de l'interconnectivité, les infrastructures essentielles de l'information se trouvent exposées à des menaces et à des faiblesses toujours plus nombreuses et diverses qui donnent lieu à de nouvelles préoccupations en matière de sécurité,

Notant également que, pour assurer la protection efficace des infrastructures essentielles de l'information, il importe notamment de définir les menaces et réduire les faiblesses auxquelles elles sont exposées, réduire au minimum les dégâts et les délais de remise en état en cas d'endommagement ou d'attaque, et identifier la cause des dégâts ou l'origine des attaques,

Considérant que la protection efficace des infrastructures exige que soient instaurées une communication, une coordination et une coopération aux niveaux national et international entre toutes les parties concernées et que les efforts déployés au niveau national doivent être étayés par l'instauration d'une coopération internationale et régionale efficace et notable entre les parties concernées,

Considérant 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 en vue de lutter contre l'exploitation de ces technologies à des fins criminelles et de créer une culture mondiale de la cybersécurité, et notant qu'il est nécessaire 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 et pour la protection des infrastructures essentielles de l'information, 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,

Prenant note de ce que font les organisations internationales et régionales compétentes pour renforcer la sécurité des infrastructures essentielles de l'information,

Considérant que les efforts visant à protéger les infrastructures essentielles de l'information doivent être déployés en tenant dûment compte des lois nationales applicables concernant la protection de la vie privée ainsi que les autres textes législatifs pertinents,

1. *Prend note* des éléments à prendre en considération pour la protection des infrastructures essentielles de l'information, figurant en annexe à la présente résolution ;

2. *Invite* toutes les organisations internationales compétentes, y compris les organismes compétents des Nations Unies, à examiner notamment, au besoin, ces éléments en vue d'assurer la protection des infrastructures essentielles de l'information dans toute activité future relative à la cybersécurité ou à la protection des infrastructures essentielles ;

3. *Invite* les États Membres à examiner, entre autres choses, ces éléments lorsqu'ils élaborent leurs stratégies visant à réduire les risques auxquels sont exposées les infrastructures essentielles de l'information, conformément aux lois et réglementations nationales ;

4. *Invite* les États Membres et toutes les organisations internationales compétentes à tenir compte, notamment, de ces éléments et de la nécessité de la protection des infrastructures essentielles de l'information dans la préparation de la deuxième phase du Sommet mondial sur la société de l'information, qui aura lieu à Tunis du 16 au 18 novembre 2005 ;

5. *Encourage* les États Membres et les organisations régionales et internationales pertinentes qui ont élaboré des stratégies relatives à la cybersécurité et visant à assurer la protection des infrastructures essentielles de l'information à partager leurs meilleures pratiques ainsi que les mesures susceptibles d'aider d'autres États Membres dans leurs efforts en vue de faciliter l'instauration de la cybersécurité ;

6. *Souligne* qu'il est nécessaire de renforcer les efforts visant à mettre fin à la fracture numérique, à réaliser l'accès universel aux technologies de l'information et des communications et à assurer la protection des infrastructures essentielles de l'information en facilitant le transfert des technologies de l'information et le renforcement des capacités, en particulier vers les pays en développement, tout spécialement les pays les moins avancés, de manière que tous les États puissent tirer pleinement parti des technologies de l'information et des communications aux fins de leur développement socioéconomique.

78e séance plénière
23 décembre 2003

Annexe

Éléments applicables à la protection des infrastructures essentielles de l'information

1. Disposer de réseaux d'alerte d'urgence à l'égard des faiblesses, des menaces et des incidents dans le domaine de la cybernétique.

2. Mener des activités de sensibilisation afin de permettre aux parties concernées de mieux comprendre la nature et la portée de leurs infrastructures essentielles de l'information ainsi que le rôle qui revient à chacune d'elles pour ce qui est de protéger ces infrastructures.

3. Examiner les infrastructures et identifier les interdépendances qui existent entre elles afin d'en renforcer la protection.

4. Promouvoir la mise en place de partenariats entre les parties concernées, du secteur public comme du secteur privé, en vue de partager et d'analyser les informations sur les infrastructures essentielles pour empêcher que celles-ci ne soient endommagées ou attaquées et mener des enquêtes et prendre des mesures correctives.

5. Créer et maintenir des réseaux de communication d'urgence et procéder à des essais afin de veiller à ce que ces réseaux restent sûrs et stables dans des situations de crise.

6. Faire en sorte que les politiques en matière de disponibilité des données tiennent compte de la nécessité de protéger les infrastructures essentielles de l'information.

7. S'attacher à retracer la filière des attaques commises contre les infrastructures essentielles de l'information et, s'il y a lieu, communiquer à d'autres pays les renseignements obtenus.

8. Procéder à des activités de formation et à des exercices afin de renforcer les capacités de réaction et de tester les plans de continuité et de circonstance en cas d'attaque contre les infrastructures de l'information, et encourager les parties concernées à mener des activités analogues.

9. Prendre des mesures de droit matériel et de droit procédural et disposer de personnel qualifié pour permettre aux États d'enquêter sur les attaques commises contre les infrastructures essentielles de l'information, engager des poursuites et assurer, s'il y a lieu, une coordination avec d'autres États.

10. Mener, s'il y a lieu, des activités de coopération internationale pour sécuriser les infrastructures essentielles de l'information, notamment en s'employant à mettre en place et à coordonner des systèmes d'alerte d'urgence, à partager et analyser des renseignements sur les faiblesses, les menaces, les incidents et les enquêtes en cas d'attaque contre ces infrastructures, et à coordonner les enquêtes sur de telles attaques conformément aux lois internes.

11. Promouvoir la recherche-développement aux niveaux national et international et encourager l'emploi de techniques de sécurisation qui soient conformes aux normes internationales.