Nations Unies A/55/140/Add.1

Assemblée générale

Distr. générale
3 octobre 2000
Français
Original: anglais

Cinquante-cinquième session
Point 68 de l'ordre du jour
Les progrès de la téléinformatique dans le contexte de la sécurité internationale

Les progrès de la téléinformatique dans le contexte de la sécurité internationale

Rapport du Secrétaire général

Additif

Table des matières

00-67081 (F) 061000 061000

Réponses reçues des gouvernements

Pologne

[Original : anglais]
[8 septembre 2000]

Problèmes généraux en matière de sécurité de l'information et définition des concepts fondamentaux

1. La télématique favorise grandement la libre circulation de l'information et présente d'énormes avantages pour les particuliers, les entreprises et les gouvernements du monde entier. Elle contribue au développement de la démocratie et à la liberté de parole, ainsi qu'au progrès de la société civile. La Pologne estime qu'il importe de promouvoir et d'assurer le développement de la télématique, tout en renforçant le principe de la liberté de l'information, et du choix et de l'utilisation des supports techniques.

2. La Pologne reconnaît qu'une menace d'ingérence illicite dans les systèmes télématiques ou d'utilisation à mauvais escient de ces systèmes pèse sur l'intégrité des infrastructures essentielles fondées sur l'information et sur les sources d'information des particuliers, des établissements d'enseignement, des institutions médicales et d'autres organisations du secteur privé, ainsi que des gouvernements. Pour couvrir le large éventail des problèmes relatifs à la sécurité des systèmes télématiques, la protection de l'information doit s'étendre à l'accessibilité des données recueillies dans ces systèmes, ainsi qu'à leur confidentialité, à leur disponibilité et à leur intégrité. Les lacunes de la protection des sources d'information et des systèmes télématiques, qui sont d'un intérêt vital pour les États concernés, pourraient également être une menace pour la sécurité internationale.

3. La Pologne considère cependant que les risques encourus sont de caractère transfrontalier et que n'importe qui a aisément accès aux technologies permettant d'attaquer les systèmes télématiques. Ces technologies ne peuvent d'ailleurs être classées comme civiles ou militaires par essence. La menace vient principalement de l'usage délictueux qu'en font des individus ou des organisations terroristes et, comme telle, elle ne peut être contenue par des accords relatifs à la maîtrise des armements, qui pourraient limiter ou freiner la libre circulation de l'information et les utilisations pacifiques des technologies de l'information, sur lesquelles reposent toutes les économies du monde. Toute action préventive tendant à parer à d'éventuelles attaques criminelles ou terroristes, notamment celles qui mettent en danger la paix internationale, devrait viser surtout à protéger les sources d'information et les systèmes télématiques.

4. Pour ce qui est de protéger l'intégrité des infrastructures essentielles fondées sur l'information et des sources d'information et de déjouer les risques qui menacent la sécurité de l'information, la Pologne est en faveur de l'instauration d'une coopération juridique internationale poussée et efficace, ainsi que de la stricte application des législations nationales existantes et, le cas échéant, du développement de nouveaux régimes.

Mesures nationales

5. Chaque pays a le droit et le devoir de protéger sa propre information et ses systèmes télématiques. À cette fin, la Pologne s'est dotée des textes suivants :

a) La loi sur la protection de l'information à diffusion restreinte, en date du 22 janvier 1999, qui fixe le régime de cette protection;

b) La loi sur la protection des renseignements personnels, en date du 29 octobre 1997, qui définit des règles de conduite pour le traitement des données, ainsi que les droits des personnes sur lesquelles des renseignements sont réunis;

c) Le Code pénal du 6 juin 1997, qui incrimine non seulement les crimes classiques de viol du secret de l'information – divulgation de données confidentielles et de diffusion restreinte – mais également la destruction ou la suppression de données enregistrées sur ordinateur, ou bien leur dégradation ou leur altération, ainsi que l'immixtion dans les données relatives à la défense nationale, à la sécurité des communications et au fonctionnement administratif du gouvernement, et l'obstruction à leur collecte automatique ou à leur transfert.

Opportunité de mesures et de principes internationaux nouveaux

6. Les énormes progrès de la télématique appellent à développer le droit international pour améliorer la sécurité de l'information. Les questions soulevées par la criminalité informatique, notamment sous ses aspects juridiques, étaient l'un des principaux sujets du dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, qui s'est déroulé du 10 au 17 avril 2000 (A/CONF.187/15). La Pologne reconnaît le rôle fondamental que joue la Commission pour la prévention du crime et la justice pénale des Nations Unies dans l'élaboration des principes internationaux régissant la sécurité de l'information et la mise au point de méthodes et de moyens d'action susceptibles de respecter l'équilibre nécessaire entre la protection de la vie privée et les obligations des différentes branches de gouvernement. C'est une instance qui facilite et aide également la coordination des activités des institutions interrégionales et régionales relatives à la prévention du crime et au traitement des délinquants.

7. Parallèlement, la Pologne cultive activement des relations de coopération intergouvernementale très suivies (accord conclu avec l'Allemagne; accords de négociation avec l'Estonie, la France, la Hongrie, la Slovaquie et l'Ukraine) en vue de conclure des accords concernant la protection de l'information (renseignements personnels, conclusions des examens médicaux, propriété intellectuelle, résultats de la recherche scientifique...) contre toute intervention illicite et tout autre acte frauduleux (falsification et opérations bancaires ou financières illégales notamment), et concernant également la protection des sources et réseaux d'information contre les dommages intentionnels.