Nations Unies A/55/140

Assemblée générale

Distr. générale
10 juillet 2000
Français
Original: anglais/arabe/russe

Cinquante-cinquième session
Point 69 de l'ordre du jour provisoire*
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**

Table des matières

* A/55/150.
** Le présent rapport est établi sur la base des documents présentés par les États Membres.

I. Introduction

1. Aux paragraphes 2 et 3 de sa résolution 54/49 du 1er décembre 1999, portant sur les progrès de la téléinformatique dans le contexte de la sécurité internationale, l'Assemblée générale a invité tous les États Membres à communiquer au Secrétaire général leurs vues et observations sur les questions suivantes : a) les problèmes généraux en matière de sécurité de l'information; b) la définition des concepts fondamentaux en matière de sécurité de l'information, notamment les interférences illicites dans les systèmes télématiques ou l'utilisation illégale de ces systèmes; c) l'opportunité d'élaborer des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux et d'aider à combattre le terrorisme et la criminalité dans le domaine de l'information, et a prié le Secrétaire général de lui présenter un rapport à ce sujet à sa cinquante-cinquième session.

2. Le 14 mars 2000, le Secrétaire général adressait aux États Membres une note verbale par laquelle il les priait, à la demande de l'Assemblée, de lui faire part de leurs observations. On trouvera au chapitre II du présent rapport les réponses reçues à ce jour des gouvernements. Toute autre réponse reçue ultérieurement sera publiée sous forme d'additif au présent rapport.

II. Réponses reçues des gouvernements

Fédération de Russie

[Original : russe]
[12 mai 1999]

Principes de la sécurité internationale de l'information

Terminologie

Aux fins des présents principes, on utilisera la terminologie suivante :

1. *Secteur de l'information* : domaine d'activité comprenant la création, la transformation et l'utilisation de l'information, y compris la conscience individuelle et sociale, les infrastructures téléinformatiques et l'information elle-même.

2. *Ressources d'information* : infrastructure (matériel et systèmes permettant de créer, de traiter, de stocker et de transmettre l'information), y compris les fichiers et bases de données et les flux d'information.

3. *Guerre télématique* : affrontement entre États dans le domaine de l'information, en vue de détériorer les systèmes et ressources télématiques et les structures vitales, de fragiliser le régime politique et les systèmes économique et social, et de manipuler les masses pour déstabiliser la société et l'État.

4. *Armes télématiques* : moyens et méthodes utilisés pour détériorer les ressources et systèmes d'information d'un État, nuire au système de défense et aux structures administratives, politiques, sociales, économiques ou autres structures vitales d'un État, et manipuler les masses en vue de déstabiliser la société et l'État.

5. *Sécurité de l'information* : protection des intérêts fondamentaux des individus, de la société et de l'État dans le secteur de l'information, y compris les

infrastructures téléinformatiques et l'information elle-même, (intégrité, objectivité, accessibilité, confidentialité, etc.).

6. *Menace à la sécurité de l'information* : facteurs qui mettent en péril les intérêts fondamentaux des individus, de la société et de l'État dans le secteur de l'information.

7. *Sécurité internationale de l'information* : état des relations internationales tel qu'il n'y a pas de violation de la stabilité internationale ni de menace à la sécurité des États et de la communauté internationale dans le secteur de l'information.

8. *Utilisation illégale des systèmes téléinformatiques et des ressources d'information* : utilisation des systèmes et ressources téléinformatiques sans autorisation ou en violation des règles applicables, de la législation ou des normes du droit international.

9. *Intrusion dans les systèmes et ressources téléinformatiques* : intrusion dans les activités de collecte, de traitement, de stockage, de recherche, de diffusion ou d'utilisation de l'information en vue d'entraver le fonctionnement normal des systèmes d'information ou de violer l'intégrité, la confidentialité ou l'accessibilité des ressources d'information.

10. *Structures vitales* : installations, systèmes et institutions d'un État dont les ressources en matière d'information doivent être protégées parce que toute action délibérée visant ces ressources risque d'affecter directement la sécurité nationale (transports, approvisionnement en énergie, crédit et finance, communications, administration, système de défense, organismes chargés de faire appliquer la loi, ressources stratégiques d'information, établissements de recherche et progrès scientifiques et technologiques, installations présentant des risques technologiques et écologiques, et organismes chargés d'atténuer les effets des catastrophes naturelles ou d'intervenir dans des situations d'urgence).

11. *Terrorisme international en matière d'information* : utilisation des systèmes et ressources d'information ou de télécommunication, ou influence exercée sur ces systèmes ou ressources à des fins terroristes.

12. *Délit international en matière d'information* : utilisation des systèmes et ressources d'information ou de télécommunication, ou influence exercée sur ces systèmes ou ressources à des fins illicites.

Principe I

1. Les activités de chaque État ou autre sujet de droit international dans le secteur international de l'information doivent contribuer au développement économique et social général et être compatibles avec les objectifs du maintien de la stabilité et de la sécurité internationales, les droits souverains des autres États, les intérêts en matière de sécurité et les principes de règlement pacifique des différends et des conflits, de non-recours à la force, de non-ingérence dans les affaires intérieures d'un État et de respect des droits et libertés fondamentaux.

2. Ces activités doivent également être compatibles avec le droit de chacun de rechercher, de recevoir et de diffuser des informations et des idées, tel qu'il est énoncé dans les documents pertinents des Nations Unies, étant entendu que ce droit peut être limité par la loi afin de protéger les intérêts de chaque État en matière de sécurité.

3. En même temps, chaque État ou autre sujet de droit international doit avoir un droit égal de protéger ses ressources d'information et ses structures vitales contre l'utilisation illégale des systèmes télématiques et l'intrusion dans ces systèmes, et peut compter sur l'appui de la communauté internationale pour l'exercice de ce droit.

Principe II

Les États s'efforcent de limiter les menaces dans le domaine de la sécurité internationale de l'information et, à cette fin, s'abstiennent :

a) D'élaborer, de créer et d'utiliser des moyens permettant d'exercer une influence sur les ressources et les systèmes d'information d'un autre État ou de les endommager;

b) D'utiliser délibérément l'information en vue d'exercer une influence sur les structures vitales d'un autre État;

c) D'utiliser l'information en vue de fragiliser le régime politique et les systèmes économique et social d'un État et de manipuler la population en vue de déstabiliser la société;

d) De toute intrusion dans les systèmes et ressources téléinformatiques ainsi que de toute utilisation illégale de ces systèmes et ressources;

e) De toute initiative visant à dominer et contrôler le secteur de l'information;

f) D'interdire l'accès aux technologies de l'information les plus récentes et de créer une situation dans laquelle les autres États se retrouvent technologiquement dépendants en matière d'information;

g) D'encourager les activités d'associations, organismes ou groupes internationaux à caractère terroriste, extrémiste ou criminel, qui font planer une menace sur les ressources d'un État en matière d'information et sur ses structures vitales;

h) D'élaborer et d'adopter des plans ou doctrines qui rendraient possible une guerre de l'information, risqueraient de provoquer une course aux armements et des tensions entre les États, et de conduire effectivement à une guerre de l'information;

i) D'utiliser les technologies de l'information et les moyens de communication au détriment des droits de l'homme et des libertés dans le domaine de l'information;

j) De se livrer à la diffusion transfrontière de l'information, en violation des principes et règles du droit international et des législations nationales;

k) De se livrer à la manipulation des flux d'information, à la désinformation et à la dissimulation de l'information en vue de mettre en péril l'environnement spirituel et psychologique d'un pays et de saper les valeurs culturelles, morales, éthiques et esthétiques;

l) De développer et d'acquérir un monopole sur les infrastructures d'information et de télécommunication d'un autre État, y compris les moyens d'exploitation au niveau international.

Principe III

L'Organisation des Nations Unies et les organismes compétents des Nations Unies s'emploient à promouvoir la coopération internationale pour limiter les menaces dans le domaine de la sécurité internationale de l'information et à établir à cette fin un cadre juridique international en vue de :

a) Déterminer les principales caractéristiques des guerres télématiques et procéder à une classification;

b) Déterminer les principales caractéristiques des armes télématiques ainsi que des moyens pouvant être considérés comme tels, et procéder à une classification;

c) Limiter le trafic des armes télématiques;

d) Interdire la mise au point, la diffusion et l'utilisation des armes télématiques;

e) Conjurer la menace de guerre télématique;

f) Reconnaître que l'utilisation d'armes télématiques contre les structures vitales d'un État est comparable à l'utilisation d'armes de destruction massive;

g) Créer les conditions nécessaires à l'échange équitable et sûr d'informations au niveau international fondé sur les règles et principes généralement admis du droit international;

h) Prévenir l'utilisation des technologies de l'information et des moyens de communication à des fins terroristes ou criminelles;

i) Prévenir l'utilisation des technologies de l'information et des moyens de communication pour influencer la conscience sociale en vue de déstabiliser une société ou un État;

j) Élaborer une procédure de notification mutuelle et de prévention de l'utilisation non autorisée de l'information en vue d'influencer d'autres États;

k) Créer un système de surveillance internationale destiné à déceler les menaces dans le domaine de l'information;

l) Créer un mécanisme chargé de veiller au respect du régime international de sécurité de l'information;

m) Créer un mécanisme de règlement des différends dans le domaine de la sécurité de l'information;

n) Créer un système international de certification de la sécurité des technologies de l'information et des moyens de communication (y compris les logiciels et le matériel informatique);

o) Mettre en place un système de coopération internationale entre les organismes chargés de faire appliquer la loi en vue de prévenir et de réprimer les délits dans le domaine de l'information;

p) Harmoniser, à titre volontaire, les législations nationales en matière de sécurité de l'information.

Principe IV

Les États et autres sujets du droit international assument la responsabilité internationale des activités menées dans le secteur de l'information par eux-mêmes, sous leur juridiction ou dans le cadre d'organisations internationales dont ils sont membres, ainsi que de la compatibilité de ces activités avec les principes énoncés dans le présent document.

Principe V

Tout différend entre États ou autres sujets de droit international qui résulterait de l'application des présents principes se règle au moyen du mécanisme créé à cette fin.

Jordanie

[Original : arabe]
[16 mai 1999]

1. L'utilisation de la technologie et des systèmes d'information a eu des effets positifs pour la communauté internationale en ce qui concerne le maintien de la stabilité et de la sécurité. Toutefois, une utilisation malavisée de ces nouvelles techniques risque de :

a) Favoriser l'organisation de réseaux terroristes dont les éléments sont dispersés sur de vastes aires géographiques, compte tenu des capacités qu'offrent les communications rapides;

b) Rendre plus difficile la surveillance des communications modernes compte tenu de la complexité croissante des technologies et de l'existence, dans la plupart des pays, de lois limitant la capacité d'empiéter sur la liberté individuelle de communiquer.

2. Désireux de voir prendre les mesures appropriées et en vue de prévenir tout acte terroriste, nous recommandons ce qui suit :

a) Formuler une loi d'exception autorisant les services de sécurité à pénétrer ou à contrôler partiellement les centres de commande des sociétés utilisant des systèmes de pointe;

b) En coordination avec les sociétés et institutions s'occupant de communication, assurer, au sein des services de sécurité, la formation de spécialistes capables de commander ces systèmes en cas de crise;

c) Fournir un appui au secteur des technologies de l'information et de la communication et promouvoir les notions de sécurité qui lui sont liées; assurer une infrastructure et une formation qui permettent de contribuer au maintien de la paix et de la sécurité internationales.

Qatar

[Original : arabe]
[17 mai 1999]

1. *Espionnage* : empêcher une partie non autorisée d'avoir accès au contenu des systèmes internationaux d'information et de communication.

2. *Sabotage* : prévenir la destruction partielle ou totale des systèmes télématiques internationaux.

3. *Enregistrement* : enregistrer les informations transmises par les systèmes télématiques internationaux, y compris la propriété intellectuelle.

4. *Contrefaçon* : prévenir la contrefaçon des informations transmises par les systèmes télématiques internationaux.

5. *Protection* : développer la protection électronique des informations transmises par les systèmes télématiques internationaux.

6. *Législation* : formuler les lois appropriées pour toutes les opérations électroniques de manière à assurer que les droits des intéressés soient garantis et que les contrevenants soient punis.