Nations Unies A/59/116/Add.1*

Assemblée générale

Distr. générale
28 décembre 2004
Français
Original: anglais/espagnol

Cinquante-neuvième session
Point 60 de l'ordre du jour
Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Les progrès de l'informatique et de la télématique et la question de la sécurité internationale

Rapport du Secrétaire général**

Additif

Table des matières

* Nouveau tirage pour raisons techniques.
** Les réponses ci-incluses ont été reçues alors que le rapport principal avait déjà été présenté.

04-47512* (F) 120105 120105

Réponses reçues des États Membres

Mexique

[Original : espagnol]
[18 août 2004]

1. L'étonnant développement actuel des systèmes téléinformatiques a sensibilisé la communauté internationale à la constitution simultanée d'un réseau interconnecté d'usagers, dont l'étendue et la diversité sont telles qu'il transcende les frontières géographiques et juridiques des États.

2. Cette étroite corrélation a créé une vulnérabilité directement proportionnelle dans le domaine de la sécurité nationale et internationale, confirmant ainsi que l'information et les systèmes de télécommunications sont des secteurs stratégiques qui ont une incidence majeure sur la paix et la sécurité internationales.

3. Le Mexique estime donc que les mesures à adopter face aux risques qui se posent dans ce domaine doivent non seulement préserver la libre circulation de l'information et promouvoir le développement de la téléinformatique à des fins pacifiques, mais aussi procurer des avancées concrètes sur la voie du désarmement et de la non-prolifération, ainsi que du rapprochement entre les nations, et favoriser une coopération internationale accrue en la matière.

4. Le domaine de la téléinformatique devrait être considéré dans une optique à la fois dynamique et prospective car le rythme du progrès de la science et de la technique a introduit un déphasage entre les normes à observer et les capacités effectives de ces systèmes, d'où une intensification immédiate des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information.

5. Compte tenu de l'actualité de la question et de la nécessité d'analyser les concepts permettant de se référer avec plus de précision à ce phénomène afin d'y faire face adéquatement, le Mexique se félicite des travaux qui ont été entrepris en février dernier en vue de créer un groupe d'experts gouvernementaux qui collaborera avec le Secrétaire général de l'Organisation des Nations Unies à l'élaboration d'une étude sur l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des mesures de coopération qui pourraient être prises pour y parer, ainsi que des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux, comme il est demandé aux paragraphes 4 et 2 de la résolution 58/32. Le Mexique espère que le rapport qui sera présenté à la soixantième session de l'Assemblée générale des Nations Unies contiendra des recommandations de fond et fera progresser la définition conceptuelle et juridique de cette question.

6. Le Mexique estime qu'il serait utile à cette fin de faire le point sur les avancées et les débats qui sont intervenus à ce sujet dans le cadre des autres commissions de l'Assemblée générale et sur les dispositions pertinentes figurant dans les textes internationaux en vigueur, ainsi que sur les progrès accomplis par d'autres organisations internationales – par exemple l'UNESCO – en matière de sécurité internationale, de terrorisme international, d'information et de société de l'information.

7. S'agissant du paragraphe 3 de la résolution 58/32, qui concerne 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 ou des ressources en matière d'information, le Mexique souligne que la notion d'« interférence » peut donner lieu à une regrettable confusion avec celle d'« ingérence » au nom de laquelle certains États tentent de justifier par des raisons discutables, d'ordre humanitaire ou autre, une intervention individuelle ou concertée dans les affaires d'autres États.

8. Il y aurait avantage à remplacer cette expression par celle d'« accès non autorisé » ou d'« accès illicite » pour désigner les actes que commettent certaines personnes physiques ou morales à l'endroit des systèmes d'information.

9. Face aux préoccupations évidentes que suscite l'éventuelle vulnérabilité des systèmes informatiques servant à gérer les programmes de défense de certains pays, ainsi que la possibilité d'une utilisation de la téléinformatique comme instrument d'un chantage terroriste, le Mexique réaffirme que le dialogue, la négociation, la coopération internationale et le droit international constituent les seules voies permettant d'éviter que les mesures adoptées face aux problèmes de sécurité de l'information n'entravent de quelque manière la liberté d'information et de communication.

États-Unis d'Amérique

[Original : anglais]
[13 juillet 2004]

1. Il est indispensable de veiller à la sécurité des réseaux et infrastructures d'information pour garantir la fiabilité, la disponibilité et l'intégrité des réseaux d'information nationaux et mondiaux dont sont de plus en plus tributaires les États et leurs citoyens pour leurs services essentiels et leur sécurité économique. La question qui se pose est de savoir comment les nations peuvent agir à titre individuel et collectif pour améliorer cette sécurité et prévenir les attaques portant gravement atteinte aux réseaux.

2. Certains États estiment que cet objectif peut être atteint en élaborant une convention internationale qui limiterait la mise au point ou l'utilisation des technologies de l'information les plus diverses. Ces propositions laissent entendre que les gouvernements auraient le droit d'approuver ou d'interdire les informations transmises sur le territoire national à partir de l'étranger, s'ils les jugent néfastes politiquement, socialement ou culturellement.

3. Les États-Unis sont d'avis que cette conception ne sert pas les objectifs de renforcement de la sécurité des systèmes mondiaux d'information et des communications, mais plutôt qu'elle va à l'encontre du principe de libre circulation de l'information essentielle à la croissance et au développement de tous les États. Les mesures prises pour assurer la sécurité de l'information ne doivent pas compromettre le droit de tout individu de chercher, de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit, y compris électronique, comme énoncé dans l'article 19 de la Déclaration universelle des droits de l'homme.

4. Les États-Unis estiment au contraire que la principale menace à la sécurité réside dans les attaques criminelles commises sans relâche par la criminalité organisée, les hackers et les acteurs non étatiques, y compris les terroristes. Dans ce

contexte, les avantages du cyberespace peuvent être mieux protégés si, d'une part, les États érigeaient vraiment en infraction l'exploitation des technologies de l'information à des fins criminelles et, d'autre part, prenaient des mesures systématiques pour empêcher que des infrastructures vitales d'information ne soient endommagées, quelle que soit la source de la menace, ce que les États-Unis appellent la création d'une culture mondiale de la cybersécurité. Dans cette perspective, toutes les parties prenantes (administrations, entreprises, société civile) sont conscientes de leurs responsabilités et agissent selon leurs rôles respectifs pour garantir la cybersécurité.

5. En ce qui concerne les applications militaires des technologies de l'information, une convention internationale est tout à fait inutile. Le droit des conflits armés et ses principes de nécessité, de proportionnalité et de limitation des dommages collatéraux régissent déjà l'utilisation de ces technologies.

Cybersécurité et prévention

6. Les États agissant à l'échelon national et coopérant à l'échelon international pour renforcer la sécurité de leurs infrastructures vitales d'information sont mieux à même d'atteindre l'objectif de la cybersécurité. Chaque État devrait élaborer un programme national de nature à :

a) Former et sensibiliser davantage les parties prenantes aux pratiques optimales en matière de sécurité des réseaux et des infrastructures d'information;

b) Ériger véritablement en infraction l'exploitation des technologies de l'information à des fins criminelles;

c) Favoriser la coopération entre les pouvoirs publics et l'industrie, par des mesures d'encouragement, pour garantir la sécurité de leurs systèmes;

d) Mettre en place un mécanisme national d'alerte et d'intervention ainsi que des procédures pour l'échange d'informations aux échelons national et international.

7. Chaque État devrait faire porter ses efforts sur la création d'une culture de la cybersécurité chez toutes les parties prenantes, y compris les administrations, les entreprises et les particuliers, et sur la coopération internationale entre les États vers une culture mondiale de la cybersécurité.

8. Le rapport du Groupe d'experts gouvernementaux devrait mettre en évidence les principes énoncés dans les résolutions 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001, toutes deux intitulées « Lutte contre l'exploitation des technologies de l'information à des fins criminelles », et dans la résolution 57/239 du 20 décembre 2002, intitulée « Création d'une culture mondiale de la cybersécurité ». Le rapport pourrait s'inspirer de ces principes en incluant une formulation visant à promouvoir les principes de la cybersécurité déjà adoptés par les États Membres. À cette fin, on pourrait s'inspirer des efforts multilatéraux déployés récemment pour renforcer la cybersécurité régionale, notamment dans le cadre du Forum des télécommunications de l'Association de coopération économique Asie-Pacifique, l'Organisation des États américains, le Sommet mondial sur la société de l'information et le G-8.

9. Les atteintes coûteuses à l'intégrité et à la disponibilité des infrastructures d'information nationales et mondiales trouvent principalement leur origine dans leur

exploitation à des fins criminelles. De l'avis des États-Unis, il est bien plus important que les gouvernements prennent des mesures pour faire en sorte que ceux qui se livrent à de tels actes puissent véritablement faire l'objet d'enquêtes et de poursuites. C'est pourquoi les États-Unis et 34 autres États ont signé la Convention sur la cybercriminalité du Conseil de l'Europe, en date du 23 novembre 2001, qui contient des directives portant sur la législation nationale et sur la coopération transfrontière en matière de répression. Le Conseil de l'Europe devrait ouvrir la Convention à la signature d'États non membres du Conseil, conformément à la pratique établie et à l'article 37 de la Convention. En effet, tous les pays, qu'ils soient parties ou non à la Convention, peuvent s'en servir immédiatement comme modèle pour rédiger des lois permettant de lutter contre la cybercriminalité.

10. En outre, indépendamment de la source ou de la motivation d'une attaque, les outils utilisés et les dommages causés aux systèmes d'information sont semblables par nature. Par conséquent, il est plus important que les tous les États prennent des mesures rigoureuses pour réduire la vulnérabilité de leurs systèmes et inculquer à leurs citoyens une culture de la cybersécurité, ensemble de pratiques et d'habitudes en matière de sécurité conçues pour protéger leurs infrastructures d'information.

11. Pour protéger efficacement les infrastructures et les réseaux essentiels, il convient notamment de réduire leur vulnérabilité face à toutes les formes d'attaque afin de limiter au minimum les dommages et le temps de reprise en cas d'incident.

12. L'efficacité de la protection dépend également de la communication, de la coordination et de la coopération aux échelons national et international entre toutes les parties prenantes – industrie, milieux universitaires, secteur privé et administrations publiques, y compris les services de protection civile et les autorités de police. Ces efforts doivent être déployés compte dûment tenu de la sécurité de l'information et de la législation applicable concernant l'entraide judiciaire et la protection de la vie privée. En favorisant ces objectifs, les États devraient être encouragés à prendre en compte les 11 principes énoncés par les experts des pays du G-8 sur la protection des infrastructures vitales d'information, et adoptés ensuite par les ministres de l'intérieur et de la justice du G-8 en mai 2003, au moment où ils élaborent une stratégie de réduction des risques encourus par les infrastructures vitales d'information :

a) Les États devraient constituer des réseaux d'alerte et d'urgence face aux vulnérabilités, aux menaces et incidents affectant les systèmes d'information et de communication;

b) Les États devraient renforcer la sensibilisation des parties prenantes pour faciliter leur compréhension de la nature et de l'importance de leurs infrastructures vitales d'information et de communication, ainsi que du rôle que chacun doit jouer dans leur protection;

c) Les États devraient examiner leurs infrastructures et identifier leurs interdépendances afin de renforcer leur protection;

d) Les États devraient promouvoir le partenariat entre les parties prenantes, qu'elles soient publiques ou privées, afin qu'elles partagent et analysent leurs informations sur les infrastructures vitales en vue de la prévention des dégâts et des attaques à l'encontre de ces infrastructures, de leur enquête et de leur parade;

e) Les États devraient créer et entretenir des réseaux de communication de crise, et les tester afin de garantir leur bon fonctionnement, leur sécurisation et leur stabilité en cas de crise;

f) Les États devraient s'assurer que les règles d'accès à l'information ne nuisent pas au besoin de protection des infrastructures vitales;

g) Les États devraient faciliter le traçage des attaques contre les infrastructures vitales d'information et de communication et, lorsque les circonstances s'y prêtent, la divulgation des données de traçage aux pays étrangers;

h) Les États devraient assurer des actions de formation et mener des exercices pour améliorer leur capacité de riposte et tester leurs plans de continuité et de secours face aux attaques contre les infrastructures d'information et de communication, et devraient encourager les opérateurs à faire de même;

i) Les États devraient s'assurer que leurs dispositions législatives pénales et procédurales, à l'instar de celles de la Convention du 23 novembre 2001 du Conseil de l'Europe relative à la cybercriminalité, et que leur personnel formé leur permettent d'enquêter sur les actes de malveillance contre des infrastructures vitales d'information et de communication et de les poursuivre, et de coordonner, en tant que de besoin, de telles investigations avec des pays étrangers;

j) Les États devraient s'engager dans une coopération internationale, lorsque les circonstances s'y prêtent, pour sécuriser les infrastructures vitales d'information et de communication, y compris, dans le respect des lois nationales, le développement et la coordination des systèmes d'alerte et d'urgence, l'échange et l'analyse d'informations relatives aux vulnérabilités, aux menaces et aux incidents, et la coordination des enquêtes sur les attaques contre de telles infrastructures;

k) Les États devraient promouvoir la recherche et le développement nationaux et internationaux et encourager l'application de techniques de sécurité certifiées au regard de normes internationales.

13. L'efficacité de la sécurité des réseaux et des infrastructures d'information peut être améliorée grâce à l'éducation et à la formation, aux mesures prises et à la législation, et à la coopération internationale, et peut s'appuyer sur la technologie.

14. Il convient d'appuyer l'ONU et les autres organisations multilatérales dans leurs efforts visant à encourager les États Membres à :

a) Évaluer la sécurité de leurs infrastructures et réseaux vitaux d'information, y compris en analysant leurs vulnérabilités et leurs interdépendances;

b) Former et sensibiliser davantage les parties prenantes aux bonnes pratiques en matière de sécurité des réseaux et des infrastructures d'information;

c) Ériger véritablement en infraction l'exploitation des technologies de l'information à des fins criminelles et favoriser les enquêtes transfrontières sur la cybercriminalité;

d) Favoriser un partenariat entre les pouvoirs publics et l'industrie prévoyant des mesures d'encouragement pour garantir la sécurité de leurs systèmes;

e) Mettre en place un mécanisme national d'alerte et d'intervention ainsi que des procédures pour l'échange d'informations aux échelons national et international.

Venezuela (République bolivarienne du)

[Original : espagnol]
[28 juin 2004]

1. Le Gouvernement de la République bolivarienne du Venezuela estime que toute atteinte à la sécurité de l'information est contraire au droit des États d'exercer leur pleine et légitime souveraineté et qu'en ce sens l'emploi des moyens et des techniques téléinformatiques à des fins de déstabilisation politique et économique est contraire aux valeurs fondamentales de la démocratie.

2. Le concept de sécurité de l'information présente donc deux aspects : d'une part, le respect et la protection de l'information; d'autre part, l'usage judicieux et la véracité de l'information. Tant l'utilisation illicite que la non-utilisation délibérée des systèmes télématiques ou des ressources en matière d'information à des fins déstabilisatrices constituent un facteur de dérèglement dans le contexte de la sécurité internationale.

3. La République bolivarienne du Venezuela souscrit à l'élaboration de principes internationaux visant à renforcer la sécurité des systèmes téléinformatiques mondiaux dans le dessein de permettre ou de faciliter la lutte contre le terrorisme et la criminalité en matière d'information, sans préjudice de la souveraineté des États.