Nations Unies A/57/166/Add.1

Assemblée générale

Distr. générale
29 août 2002
Français
Original: anglais/arabe/espagnol

Cinquante-septième session
Point 62 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**

Additif

Table des matières

* A/57/150.

** L'information contenue dans le présent rapport a été reçue après la présentation du rapport principal.

02-56150 (F) 240902 240902

Réponses reçues des Gouvernements

[Original : espagnol]
[15 juillet 2002]

Cuba

Les problèmes généraux de la sécurité de l'information

1. Au cours des dernières décennies, l'humanité a vu la science et la technologie immensément progresser. Les progrès réalisés en téléinformatique ont constitué une véritable révolution technologique dans tous les domaines de l'activité humaine. Combinés, le développement des télécommunications et celui de l'informatique multiplient à l'infini les possibilités qu'offrent chacun de ces domaines.

2. La création d'ordinateurs compacts, rapides et très puissants; l'utilisation de nouveaux matériaux qui accélèrent la transmission de l'information; et la multiplication des satellites de communication ne sont qu'un aperçu des succès obtenus.

3. Le phénomène de mondialisation auquel on assiste aujourd'hui est l'un des résultats les plus visibles de ce que l'on appelle la révolution technologique. Les distances s'estompent, les communications et les flux d'information se déplacent en temps réel. Les opérations ont changé du tout au tout dans le secteur industriel, l'outil informatique accélérant la mutation des procédés de production en contribuant à une augmentation sans précédent de l'efficacité.

4. Tout comme le secteur civil, l'industrie militaire est touchée par ces mutations. À l'heure actuelle, les armements modernes et les systèmes qu'ils emploient ne peuvent se passer de l'informatique. Au cours de la dernière décennie, dans le cadre de plusieurs conflits armés, on a assisté au déploiement, contre les cibles visées, d'armements sophistiqués dont le pouvoir de destruction et la précision mortelles étaient sans précédent. Ces armements sont, en grande partie, des applications de découvertes de l'informatique.

5. Le pouvoir de l'outil informatique a été démontré. Les logiciels possèdent une grande variété d'utilisations, les programmes prévus pour accomplir des actions et produire des effets nuisibles et hautement destructeurs se faisant cependant de plus en plus nombreux et capables de provoquer, en peu de temps, des dommages irréparables n'importe où dans le monde, du fait de l'extension des réseaux informatiques et du niveau d'accès à ceux-ci.

6. La dépendance qui se crée à l'égard de ces technologies doit faire l'objet d'une réflexion collective, de manière à ce que leur utilisation soit adéquate.

7. Le fait que cette question soit inscrite à l'ordre du jour de l'Assemblée générale démontre que la communauté internationale a pris conscience des dangers qui pèsent sur la paix et la sécurité internationales lorsque les technologies de ce type ne sont pas utilisées à des fins pacifiques.

8. Autre exemple d'utilisation nuisible des nouvelles technologies, certains cas d'utilisation hostile des télécommunications dans l'intention – avouée ou cachée – de subvertir l'ordre législatif et politique des États peuvent créer des tensions et des situations contraires à la paix et à la sécurité internationales, en contradiction totale avec les principes et les aspirations consacrés dans la Charte des Nations Unies.

9. La résolution 56/19 de l'Assemblée générale nous offre l'occasion d'analyser tous les aspects de la question de la téléinformatique dans le contexte de la sécurité internationale, et d'étudier ainsi la possibilité de renforcer le droit international en vigueur dans ce domaine et d'en élargir la portée.

Détermination des critères de base relatifs à la sécurité de l'information, en particulier en ce qui concerne l'ingérence non autorisée ou l'utilisation illicite de systèmes téléinformatiques et de moyens d'information

10. Il existe plusieurs critères essentiels :

1. L'homologation de normes et de procédures

11. Le fait que les usagers ne suivent pas un code de déontologie commun, que la participation aux réseaux de l'Internet, de même que l'utilisation des satellites et autres moyens de communication, relève d'initiatives individuelles, compromet la sécurité de l'information transmise par ces voies.

12. L'efficacité d'un réseau dépend étroitement de son niveau de *confidentialité*, d'*intégrité* ainsi que des

modalités d'*accès* à ses services. Il s'agit des conditions qui garantissent qu'une information donnée ne pourra être vue que par des utilisateurs autorisés, qu'elle ne pourra être modifiée et qu'elle sera disponible à tout moment.

13. Lorsque ces conditions ne sont pas remplies, la sécurité du réseau disparaît ou diminue. Les fabricants de produits informatiques doivent faire en sorte que les logiciels et le matériel qu'ils mettent au point interdisent toute ingérence illégale et qu'ils ne puissent servir à la création d'armes informatiques capables de détruire des éléments des systèmes d'information. Il s'agit de principes qui s'appliquent généralement à tout service, à la fabrication de tout produit et système téléinformatique.

14. Pour remplir ces conditions, les producteurs de systèmes informatiques doivent tous contrôler plus étroitement les processus de production, les technologies et les systèmes. Ils doivent également assurer un suivi afin de surveiller l'exploitation et l'utilisation des systèmes et technologies qu'ils produisent. De même, il est nécessaire de créer des mécanismes de collaboration afin que les fournisseurs et les utilisateurs puissent se signaler mutuellement toute violation dès qu'ils la détectent et évaluer la part de responsabilité des producteurs dans la résolution des problèmes de sécurité que posent les produits commercialisés.

15. Il est nécessaire de définir des normes fondamentales afin que la création de nouvelles technologies se fasse en toute sécurité. Les technologies créées doivent également être enregistrées, de manière à faciliter les procédures d'homologation. Cuba est prête à collaborer avec les pays intéressés et à mettre à leur disposition sa modeste expérience dans ce domaine.

2. Ingérence illicite dans les systèmes téléinformatiques

16. Les règlements internationaux interdisant les agressions contre les systèmes téléinformatiques doivent être renforcés. Les États ne peuvent lutter individuellement contre ce problème. Un État isolé ne saurait trouver la solution à ce problème dans un contexte marqué par l'interdépendance, résultat de l'expansion universelle des réseaux informatiques et des systèmes de télécommunication.

17. Les normes internationales déjà en vigueur doivent être respectées. Avant de pénétrer dans les systèmes d'information ou de télécommunications d'un État, il faut s'assurer que cet État a donné son autorisation et qu'il a précisé les modalités et l'ampleur de l'accès accordé.

18. La sécurité et la paix internationales peuvent être compromises par les agressions commises contre les systèmes téléinformatiques d'États donnés. De telles pratiques existent bel et bien en tant qu'instruments de politiques hostiles.

19. Cuba est l'objet d'agressions de ce type, qui sont encouragées, autorisées ou exécutées par le Gouvernement des États-Unis d'Amérique. La gravité de ce problème est illustrée par le fait que notre pays a subi, pendant plusieurs décennies, une agression menée par voie radiophonique et télévisée par les États-Unis, dans le but déclaré de perturber l'ordre intérieur de la République de Cuba et de renverser son gouvernement.

20. Ainsi, de janvier 2001 à mars 2002, environ 15 stations de radio et de télévision ont diffusé, depuis le territoire des États-Unis, des programmes véhiculant des informations fausses et tendancieuses ainsi qu'un contenu ouvertement subversif.

21. Au cours de cette période, le nombre d'heures d'émissions radiodiffusées quotidiennement depuis les stations décrites précédemment, sur ondes moyennes, sur ondes courtes et sur onde à fréquence modulée, représente de 312 à 319 heures. En moyenne, au total le temps d'émission de ces stations a été de 2 257 heures par semaine. En comptant les émissions télévisées, le total hebdomadaire du temps de diffusion s'élève à 2 288 heures.

22. Depuis 1990, le Gouvernement des États-Unis a investi plus de 20 millions de dollars par an et, au cours du présent exercice budgétaire, environ 24 millions dollars, afin de mener cette agression par radiodiffusion et par télédiffusion.

23. La plupart des messages diffusés incitent à la désobéissance civile, au vandalisme et au terrorisme. Il y a peu, une émission radiophonique diffusée par le Gouvernement des États-Unis est allée jusqu'à inspirer un incident destiné à créer des troubles internes à Cuba et qui, en outre, toucha la représentation diplomatique d'un pays tiers, créant ainsi des tensions qui auraient pu compromettre les relations entre Cuba et ce pays.

3. Utilisation illicite de systèmes téléinformatiques

24. Il s'agit d'une utilisation de ce type de systèmes qui ne respecte pas les procédures et les normes internationales et qui viole la réglementation internationale en la matière. Les États ne l'ayant pas encore fait, doivent prendre toutes les mesures nécessaires au renforcement de la réglementation internationale.

25. Étant donné le rapide développement des technologies de la téléinformatique, la réglementation internationale les concernant devra être révisée régulièrement afin que son efficacité évolue au même rythme que ces technologies.

26. À l'heure actuelle, aucun milieu social, aucune activité humaine, ou presque, n'échappe à l'influence des systèmes téléinformatiques. De ce fait, toute utilisation non raisonnable de ces systèmes peut avoir des effets incalculables.

4. Les systèmes d'information et de télécommunications dépendent de technologies à double usage

27. L'histoire démontre que les nouveaux systèmes téléinformatiques ont pour particularité d'avoir eu, au fur et à mesure qu'ils étaient développés, des applications tour à tour civiles et militaires. Ainsi, nombre de technologies qui sont aujourd'hui couramment utilisées dans la vie civile furent créées pour une application militaire, et vice versa.

28. Il est donc nécessaire que l'action de la communauté internationale dans ce domaine suive deux axes : la prévention, la lutte et l'éradication de l'emploi des systèmes téléinformatiques à des fins hostiles et le renforcement de la coopération internationale en vue de l'utilisation pacifique de ces mêmes systèmes.

29. En ce qui concerne les systèmes téléinformatiques, il convient notamment d'étudier les points suivants :

a) Définir et appliquer universellement des procédures empêchant l'accès non autorisé à ces systèmes;

b) Garantir la transparence dans l'utilisation de ces outils;

c) Élaborer des mesures spéciales en vue de protéger les systèmes informatiques utilisés en relation avec les armes de destruction massive et avec d'autres armements sophistiqués;

d) Adopter des mesures destinées à empêcher l'accès non autorisé aux systèmes informatiques des centrales nucléaires, des centrales électriques et des autres installations stratégiques à l'intérieur des pays;

e) En vue de prévenir les actes illicites, faire en sorte que les États échangent des informations concernant les activités illicites dans lesquelles sont impliquées des personnes physiques ou morales se trouvant sous leur contrôle ou leur juridiction;

f) Renforcer la coopération internationale dans le domaine des échanges technologiques ainsi que la formation et la consolidation des capacités nationales dans ce domaine;

g) Interdire l'installation, dans l'espace, d'instruments utilisant ces technologies à des fins militaires;

h) Confirmer le principe essentiel des relations internationales relatif à la non-ingérence dans les affaires intérieures d'un État, notamment grâce à l'adoption de mesures interdisant l'utilisation de systèmes téléinformatiques à des fins semblables.

5. Les armes de l'information

30. Les systèmes d'information et de télécommunications peuvent se transformer en armes lorsqu'ils sont conçus ou utilisés en vue de provoquer des dégâts dans l'infrastructure d'un État. Une telle utilisation peut notamment s'illustrer dans l'attaque de réseaux nationaux au moyen de logiciels étrangers ou depuis un site se trouvant dans l'État attaqué mais avec des moyens appuyés ou créés à l'étranger; dans des émissions radiodiffusées ou télédiffusées utilisant des moyens non autorisés ni approuvés par l'État qui est agressé; ou pour influencer sur le comportement des personnes dont l'intention est de déstabiliser les sociétés, de renverser les gouvernements ou de modifier l'ordre politique et social des pays.

6. Le terrorisme appliqué aux systèmes téléinformatiques

31. Le terrorisme sous toutes ses formes et dans toutes ses manifestations doit être combattu et repoussé, quelles que soient sa source et sa cible. Les

technologies de la téléinformatique peuvent être utilisées en vue de commettre des actes de terrorisme. Pour les terroristes, leur utilisation est avantageuse puisqu'elles sont largement diffusées, d'un accès relativement facile et d'un bon rapport coût-résultat.

32. Les systèmes téléinformatiques peuvent servir à obtenir des résultats aussi différents et dangereux que le blocage des systèmes automatisés d'un aéroport; l'interférence dans les systèmes de navigation d'avions commerciaux; la perturbation des systèmes de contrôle d'une centrale électrique, de l'approvisionnement en eau et de la circulation automobile; ainsi que le démantèlement de réseaux de communication.

33. Il est indispensable d'examiner les problèmes associés au terrorisme dans le cadre d'une évaluation des rapports entre les progrès de la téléinformatique et la sécurité internationale. Ce problème pourrait être abordé, indirectement, dans le cadre des négociations menées aux Nations Unies au sujet de la lutte internationale contre le terrorisme en vue de l'établissement de normes et de réglementations internationales, ainsi que dans le cadre d'autres initiatives multilatérales pertinentes.

34. Cuba s'engage à examiner tous les principes essentiels proposés et examinés dans le cadre de l'Organisation des Nations Unies qui, en tant que principal garant de la paix et de la sécurité internationales, est l'instance la plus appropriée pour en débattre.

35. Les institutions internationales dont les domaines de compétence incluant les systèmes téléinformatiques doivent également participer au débat.

Nécessité d'élaborer des principes internationaux augmentant la sécurité des systèmes téléinformatiques mondiaux et renforçant la lutte contre le terrorisme et la délinquance dans le domaine de l'information

36. La nécessité de renforcer le droit international dans le domaine de la téléinformatique est évidente. Les bases ont été posées, il existe des principes, réglementations et procédures internationaux s'appliquant dans ce domaine et qui doivent être pris en compte. Il faut également tenir compte de l'expérience de chaque pays.

37. Il faut s'employer à définir des directives non contraignantes et adopter des normes pouvant être codifiées dans des protocoles ou conventions internationaux, multilatéraux et juridiquement contraignants.

38. Dans les deux cas, il sera nécessaire d'examiner les critères essentiels ici esquissés, ainsi que ceux qui seront proposés ultérieurement, en particulier le critère d'ingérence non autorisée ou d'utilisation illicite de systèmes téléinformatiques et d'outils d'information; les aspects de la souveraineté relatifs aux thèmes étudiés; l'utilisation pacifique des outils téléinformatiques sous toutes leurs formes; la prévention, la lutte et l'éradication des pratiques hostiles lors de l'utilisation de ces systèmes; l'application de mesures nationales qui assurent un contrôle renforcé des États sur les systèmes téléinformatiques et qui prévoient des poursuites en cas d'actes délictueux dans ce domaine.

[Original : espagnol]
[24 juin 2002]

Panama

1. La République de Panama est consciente des dangers qui sont apparus sur ce que l'on nomme « champs de bataille virtuel » avec les avancées technologiques réalisées dans le domaine de la téléinformatique, au point d'en faire un nouveau défi pour la sécurité internationale, la technologie ayant une incidence sur les conflits armés eux-mêmes mais aussi sur leur règlement (renseignement, cibles, amélioration de la qualité des armes plutôt qu'augmentation de leur quantité).

2. Une agression utilisant les nouvelles technologies de la téléinformatique peut entraîner des dégâts plus grands que ceux qu'un bombardement conventionnel, notamment, pourrait provoquer. Aujourd'hui, l'information financière, la circulation du pétrole et du gaz dans les oléoducs et les gazoducs, les réserves d'eau et le contrôle des barrages, le trafic aérien, la circulation sur le Canal de Panama et les services d'urgence, entre autres, sont tous contrôlés et régulés par des ordinateurs. C'est pourquoi la définition de critères fondamentaux relatifs à la sécurité de l'information, en particulier à l'ingérence non autorisée dans les systèmes téléinformatiques et dans les outils d'information ou l'utilisation illicite des systèmes de

protection, exige des systèmes de protection à la mesure de cette nouvelle forme de violence. Toutefois, de tels systèmes de protection, notamment les coupe-feu, exigent des ressources financières et humaines considérables, que nos pays possèdent rarement.

3. Ainsi, le renforcement de la sécurité des systèmes téléinformatiques mondiaux passe par la création d'un système sûr permettant un échange d'informations entre les États afin de surveiller et de prévenir les actions effectuées par des individus ou des groupes d'individus utilisant les nouvelles technologies dans la préparation d'activités criminelles, ou afin d'empêcher ces individus ou ces groupes d'individus de communiquer entre eux. Cette nécessité entraîne cependant, pour les pays techniquement avancés, une obligation de fournir et de transférer leurs connaissances aux pays qui le sont moins et de les aider à renforcer leurs capacités dans ce domaine. En outre, les pays qui possèdent une avance dans le domaine technologique doivent s'engager à ne pas l'utiliser dans le cadre d'opérations d'espionnage commercial ou industriel, au détriment d'autres pays ne disposant pas des mêmes avancées.

4. En dépit des dommages qu'ils peuvent provoquer, l'Internet et les nouvelles technologies téléinformatiques sont des outils qui, utilisés convenablement, peuvent contribuer à la sécurité internationale car ils peuvent fournir des outils nécessaires à la réalisation de l'objectif de sécurité humaine.

[Original : arabe]
[28 août 2002]

République arabe syrienne

Sont reproduites ci-après les vues des parties concernées en République arabe syrienne sur la question des progrès de la téléinformatique dans le contexte de la sécurité internationale.

- Levée de l'embargo sur la technologie de la téléinformatique et l'importation de celle-ci dans les États en développement Membres de l'Organisation des Nations Unies.
- L'Organisation des Nations Unies devrait jouer un rôle actif sur les plans législatif et matériel en vue d'éliminer le fossé numérique entre les États avancés d'un point de vue technologique et scientifique et les États en développement.
- Établir des lois empêchant les États, les organisations et les particuliers d'accéder de façon illégitime aux systèmes de téléinformatique des autres États, ces législations devant prévoir des sanctions contre les parties qui y contreviennent.
- La mise en application des résolutions émanant de l'Union internationale des télécommunications qui protègent les fréquences radiophoniques de chaque État Membre de l'Organisation des Nations Unies contre le brouillage ou les interférences illégitimes par tout autre État ou toute autre partie.
- La mise en place de bases et de règles internationales relatives à la diffusion d'informations ayant trait à l'histoire, à la civilisation et à la culture des peuples dans les bases de données et les réseaux d'information (Internet), en s'abstenant de désinformer en diffusant des renseignements erronés, et la prise de mesures appropriées donnant les moyens d'agir contre les parties qui commettent des infractions.
- Création d'une autorité internationale bénéficiant d'un soutien international et ayant pour fonction d'apporter les justifications et les preuves aux États qui lui demandent de coopérer sur le plan de la sécurité concernant le régime de la téléinformatique. Cette autorité internationale aurait notamment pour fonctions d'assurer un soutien matériel et technologique à ces États en vue de leur permettre de faire ce que l'on attend d'eux et de former un cadre technique spécialisé appartenant à ces États au moyen de la coopération concernant la technologie de la sécurité des systèmes téléinformatiques.