Nations Unies A/58/373

Assemblée générale

Distr. générale
17 septembre 2003
Français
Original: anglais/espagnol/français/russe

Quarante-huitième 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/58/150.

03-52341 (F) 091003 101003

I. Introduction

1. Au paragraphe 3 de sa résolution 57/53 relative aux progrès de la téléinformatique dans le contexte de la sécurité internationale, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général leurs vues et observations sur les points suivants : 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 ou des ressources en matière d'information; et c) la teneur des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux. Au paragraphe 4 de la résolution, elle a prié le Secrétaire général d'examiner la question des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information ainsi que les mesures de coopération qui pourraient être prises pour y parer et de procéder à une étude avec l'assistance d'un groupe d'experts gouvernementaux qu'il constituerait en 2004, experts qui seraient désignés sur la base d'une répartition géographique équitable et avec la coopération des États Membres à même de prêter leur concours, et de lui présenter, à sa soixantième session, un rapport sur les résultats de cette étude.

2. Par une note verbale datée du 18 février 2003, tous les États Membres ont été invités à faire connaître au Secrétaire général leurs vues et observations sur le sujet. Sept réponses ont été reçues jusqu'ici. Les réponses qui seront reçues ultérieurement seront publiées dans un additif au présent rapport.

II. Réponses reçues des États Membres

Bolivie

[Original : espagnol]
[17 juin 2003]

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

1. La Bolivie est préoccupée par l'idée que les progrès techniques ne soient utilisés à des fins incompatibles avec la stabilité et la sécurité internationale et ne portent donc atteinte à l'intégrité de l'infrastructure des États, nuisant ainsi à leur sécurité dans les domaines tant militaire que civil.

2. La Bolivie est donc d'avis qu'il faut empêcher que les ressources qu'offrent les techniques de l'information ne soient utilisées à des fins délictueuses ou terroristes.

3. C'est pourquoi il y a lieu d'examiner les critères fondamentaux relatifs à la sécurité de l'information et aux interférences illicites dans les systèmes télématiques.

Importance de l'information

4. Lorsque nous parlons d'information, nous nous référons à tout ce qui entre dans le cadre de la télématique (nouvelles technologies, nouvelles applications-nouveaux logiciels, nouveaux équipements-nouveaux matériels, nouvelles formes de

traitement de l'information conçues pour la rendre toujours plus homogène, fiable et rapide), en tenant compte principalement des risques que présentent ces systèmes et de la nécessité d'en garantir la sécurité.

5. Il ne faut pas oublier que le lieu où est centralisée l'information peut souvent être le plus utile et, en même temps, le plus vulnérable.

6. La vulnérabilité des télécommunications s'applique à l'Internet et à la téléphonie. L'Internet est directement lié aux systèmes informatiques. La téléphonie se divise en téléphonie cellulaire et téléphonie par fil. La téléphonie cellulaire est en contact direct avec un espace de propagation commun (par où transitent les ondes hertziennes), où les usagers sont immergés dans les échanges téléphoniques et exposés aux interceptions.

Les infractions liées à l'utilisation des systèmes télématiques

7. Les infractions commises accidentellement lors de l'utilisation des ordinateurs et des récepteurs sont de plus en plus nombreuses, diverses et graves. En fait, elles ne sont en grande partie découvertes que fortuitement (fraudes, falsification et vente d'informations).

8. En ce qui concerne la manipulation des systèmes informatiques, il y a lieu de considérer le virus informatique comme un programme élaboré accidentellement ou intentionnellement auquel il convient d'accorder une attention particulière et qui doit être contrecarré à l'aide d'une série d'opérations bien définies.

9. Il importe de souligner, en ce qui concerne les infractions, que lorsque apparaissent les problèmes, il faut s'attaquer à la cause et prendre immédiatement des mesures pour les résoudre; au nombre des causes qui présentent le plus grand risque, citons l'intérêt personnel, le syndrome de Robin des bois, la haine de l'organisation, les troubles mentaux et la malhonnêteté et, parmi les causes qui présentent un risque mineur, l'intérêt de l'organisation et les jeux.

Paradigmes organisationnels en ce qui concerne la sécurité

10. Les paradigmes jouent un rôle important dans la philosophie actuelle de la science puisque c'est d'eux que découlent les règles qui régissent les recherches.

11. Au nombre des principaux paradigmes, on peut citer les suivants : la responsabilité de l'audit d'un système relève de l'usager et du service de l'audit interne, les systèmes de sécurité ne prévoient pas la possibilité de fraude interne, les accidents sont peu probables après la mise en place, il existe toujours des failles étant donné qu'aucun système n'est parfait, etc.

Établissement du risque

12. Il importe de faire prendre conscience aux usagers du risque que court l'information et de les amener à comprendre que la sécurité fait partie de leurs tâches. À cette fin, il faut calculer le coût du système de sécurité, compte tenu de sa qualité, en organiser la mise en place en fonction des risques, déterminer quelles sont les applications à haut risque, évaluer les conséquences de la suspension du service et arrêter les mesures de sécurité nécessaires.

13. Une fois défini le degré de risque, il faut dresser la liste des mesures à prendre à titre préventif et de celles qui devront être prises pour remédier à la situation en cas de catastrophe, en indiquant leur ordre de priorité.

14. Il faut prévoir et quantifier le risque aux niveaux institutionnel, national et régional en indiquant les programmes de nature à contribuer à son élimination et à réparer les dommages causés.

Considérations relatives à un système de sécurité intégral

15. Élaborer un système de sécurité veut dire planifier, organiser, coordonner, diriger et contrôler les activités qui contribuent à préserver et garantir l'intégrité des ressources qu'offre l'informatique, ainsi que la défense des actifs de l'institution, de l'État et de la région.

16. À cette fin, il y a lieu de définir les éléments administratifs et les politiques de sécurité, fixer et répartir les responsabilités, fixer les procédures d'urgence, définir les objectifs de sécurité, déterminer ce qui constitue un risque pour l'information et ce qui en assure la sécurité et, finalement, élaborer un programme de sécurité.

Cuba

[Original : espagnol]
[28 mai 2003]

1. Cuba a toujours appuyé les résolutions relatives aux progrès de la téléinformatique dans le contexte de la sécurité internationale depuis que la Première Commission de l'Assemblée générale des Nations Unies a été saisie de la question en 1998.

2. L'inscription de la question à l'ordre du jour de l'Assemblée générale montre que la communauté internationale a pris conscience des dangers qui peuvent menacer la paix et la sécurité internationales lorsque les techniques de l'information ne sont pas utilisées à des fins pacifiques.

3. La préparation, puis la tenue en deux étapes – Genève en 2003 et Tunis en 2005 – du Sommet mondial sur la société de l'information a placé la question qui fait l'objet de la résolution de référence et d'autres résolutions qui lui sont étroitement liées parmi les questions prioritaires qui retiennent l'attention de la communauté internationale.

4. L'usage hostile des télécommunications dans l'intention déclarée ou non de troubler l'ordre juridique et politique des États est une manifestation négative de l'emploi de ces moyens, dont les effets peuvent engendrer des tensions et des situations préjudiciables à la paix et à la sécurité internationales, en contradiction flagrante avec les principes et buts consacrés dans la Charte des Nations Unies.

5. Dans sa résolution 57/53, l'Assemblée générale note expressément que la diffusion et l'emploi de la téléinformatique intéressent la communauté internationale tout entière et qu'une vaste coopération internationale contribuera à une efficacité optimale.

6. Au huitième alinéa du préambule, elle se déclare préoccupée par le fait que la téléinformatique risque d'être utilisée à des fins incompatibles avec le maintien de

la stabilité et de la sécurité internationales et de porter atteinte à l'intégrité de l'infrastructure des États, nuisant ainsi à leur sécurité dans les domaines tant civil que militaire.

7. Par ailleurs, au paragraphe 3 b) du dispositif, elle demande aux États de faire connaître leurs vues et observations sur 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.

8. Par « interférence illicite », Cuba entend l'emploi de ces systèmes en marge des procédures et normes arrêtées internationalement, en particulier dans le cadre de l'Union internationale des télécommunications, et en contravention des réglementations nationales qui s'y rapportent.

9. Les États qui ne l'ont pas encore fait doivent prendre toutes les mesures nécessaires pour renforcer ces réglementations nationales.

10. Il est en outre indispensable de réexaminer périodiquement les réglementations internationales en la matière étant donné la rapidité avec laquelle se développent les techniques auxquelles elles se rapportent, de façon à ce qu'elles gardent toute leur efficacité en évoluant de pair avec ce développement.

11. Les systèmes d'information et de télécommunication peuvent se transformer en armes lorsqu'ils sont conçus ou employés pour porter atteinte à l'infrastructure d'un État. Par exemple, l'agression contre des réseaux nationaux à l'aide de logiciels étrangers ou à partir de sources à l'intérieur de l'État même, mais dirigées de l'étranger ou conçues à l'étranger, les émissions de radio ou de télévision visant à encourager le renversement de l'ordre établi et des institutions constitutionnelles de l'État vers lesquels sont envoyés les signaux, les actions visant à perturber les services de radiodiffusion d'autres États, à en entraver le fonctionnement ou à les paralyser, etc.

12. Cuba souligne à nouveau que tous les États doivent respecter les règles internationales en vigueur dans ce domaine. Les accès aux systèmes d'information ou de télécommunication d'autres États doivent être conformes aux accords de coopération internationale qui ont été conclus, compte tenu du fait que l'élément fondamental en est le principe du consentement de l'État intéressé. Les formes et la portée des échanges doivent respecter la législation de l'État au système duquel il sera accédé.

13. L'agression d'un État contre les systèmes d'information ou de télécommunication d'autres États peut porter atteinte à la sécurité et à la paix internationales. Malheureusement, de tels procédés sont déjà utilisés comme moyen de mettre en pratique des politiques d'hostilité.

14. Cuba est victime de ce type d'agression encouragé, approuvé et exécuté par le Gouvernement des États-Unis depuis près d'une vingtaine d'années. Depuis 1985 et 1990, dates auxquelles le Gouvernement des États-Unis a mis illégalement en place un émetteur radio et un émetteur de télévision, respectivement, des perturbations se produisent dans les émissions de radio et de télévision cubaines. Chaque semaine, ces émetteurs, publics et privés, diffusent vers notre pays plus de 2 220 heures de programmes subversifs destinés à renverser l'ordre établi. Les fréquences utilisées pour la diffusion exclusive de ces programmes sont au nombre de 24.

15. Depuis 1990, le Gouvernement des États-Unis a investi plus de 20 millions de dollars par an dans cette agression par la radio et la télévision.

16. Comme le Ministre des relations extérieures de la République de Cuba l'a fait savoir dans sa déclaration du 22 mai 2003, le Gouvernement des États-Unis a pris de nouvelles mesures qui constituent une escalade dans l'agression par la radio et la télévision à laquelle il se livre contre Cuba depuis des dizaines d'années.

17. L'émetteur radio mis en place et exploité par le Gouvernement des États-Unis en vue d'encourager la subversion à Cuba a utilisé le 20 mai dernier quatre nouvelles fréquences, ce qui a causé des brouillages et des dysfonctionnements dans les émissions de radio cubaines.

18. Ces actes constituent une violation flagrante du droit international et des règles et réglementations établies par l'Union internationale de télécommunications, organisation internationale qui a été créée en vue de promouvoir le bon fonctionnement des télécommunications dans le monde entier et, en particulier, l'application du règlement des radiocommunications qu'elle a adopté.

19. Dans l'après-midi du 20 mai, le signal de télévision transmis à des fins subversives vers Cuba par les services officiels de propagande des États-Unis à l'aide d'un avion EC-130 des forces armées américaines a émis de 18 heures à 22 heures en utilisant les fréquences assignées légalement aux chaînes de télévision cubaines et dûment enregistrées auprès de l'organisation internationale susmentionnée.

20. Cet acte est lui aussi une violation du droit international et des règles acceptées par tous les États dans le cadre de l'Union internationale des télécommunications, en particulier de l'article 23.3 de son règlement des radiocommunications, qui interdit les émissions au-delà des limites du territoire national.

21. Ces émissions de télévision violent aussi le préambule de la Constitution de l'Union internationale des télécommunications, puisqu'il s'agit d'activités qui ne facilitent pas les relations pacifiques et la coopération entre les peuples et le développement économique et social par le bon fonctionnement des télécommunications.

22. C'est pourquoi Cuba s'élève contre la tolérance dont les autorités des États-Unis font preuve à l'égard des activités du terroriste José Basulto et de ce qu'il entreprend pour émettre des signaux de télévision vers le territoire cubain. Bien qu'il ait été fait savoir en temps opportun par la voie diplomatique que M. Basulto avait été informé que toute émission vers Cuba serait considérée comme une violation de la loi américaine et qu'il s'exposerait donc à des poursuites, ce terroriste notoire a effectué un vol librement le 20 mai dernier et, s'il n'a pas émis, c'est parce qu'il a eu des problèmes avec l'émetteur qu'il allait utiliser et non du fait des autorités américaines, qui ont agi en parfaite complicité avec lui.

23. En vertu de l'article 15.34 du Règlement des radiocommunications de l'UIT, l'agression télévisée des États-Unis constitue un brouillage nuisible, causé par une station de télévision utilisant la bande de fréquences 13 VHF (210 à 216 MHz), qui perturbe gravement les services de télévision cubains dûment enregistrés dans cette bande.

24. Les autorités cubaines chargées des radiocommunications ont dénoncé le fait auprès de la Commission fédérale des communications du Gouvernement des États-Unis en indiquant clairement les paramètres techniques et légaux qui ont été manifestement violés.

25. Cuba a également porté les faits en cause à la connaissance du Secrétaire général de l'Union internationale des télécommunications et demandé que soient prises les mesures applicables en la matière.

26. Cuba est d'avis qu'il faut renforcer le cadre juridique international en matière d'information et de télécommunication. Elle considère également indispensable que soit respecté l'ordre international déjà établi en la matière, en vertu du principe du respect absolu du droit international et de la Charte des Nations Unies, qui doit primer sur les relations entre les États. Il existe déjà en effet des principes, des réglementations et des procédures internationaux qui doivent être respectés.

27. Il convient de s'employer à élaborer des directives non contraignantes ainsi que d'adopter des règles qui pourraient être réunies sous forme de protocoles ou de conventions internationales, multilatérales et juridiquement contraignantes.

28. Dans les deux cas, il conviendrait de tenir compte des critères fondamentaux tels que les interférences illicites dans les systèmes télématiques ou l'utilisation illégale de ces systèmes et des ressources en matière d'information, les aspects de la souveraineté liés à ces questions, l'utilisation pacifique des moyens d'information et de télécommunication sous tous leurs aspects, l'encouragement de la coopération internationale en vue de favoriser le développement des systèmes télématiques dans les pays en développement considérant l'effet déterminant des techniques de l'information et des communications sur le développement économique et social, la prévention, la répression et la suppression des pratiques hostiles dans l'utilisation de ces systèmes et l'application de mesures nationales grâce auxquelles les États pourraient mieux contrôler les systèmes télématiques et réprimer les actes délictueux en la matière.

29. Outre ce qui précède, Cuba juge nécessaire d'appeler l'attention sur les points ci-après, qui sont étroitement liés au renforcement des télécommunications en tant qu'instrument de consolidation de la paix et de la sécurité internationales :

- Tous les États doivent s'abstenir de prendre unilatéralement des mesures de coercition contraires au droit international, qui imposent à l'État visé des restrictions en matière d'accès aux technologies et aux réseaux internationaux d'échange d'informations et de communication;
- Les systèmes d'homologation et les sanctions qui pourraient être imposées à un État en ce qui concerne l'accès aux technologies des télécommunications et autres technologies qui leur sont étroitement liées, au cas où la paix et la sécurité internationales risqueraient d'être compromises, doivent être de nature multilatérale et être fondés sur des modèles arrêtés par la communauté internationale;
- Il faut renforcer la coopération internationale en la matière en mobilisant les ressources nécessaires pour aider les pays en développement à consolider et à développer leurs systèmes de télécommunication;
- Il faut adopter des mesures législatives et autres, au niveau tant national qu'international, en vue d'interdire la concentration dans des mains d'intérêts

privés de la propriété et du contrôle des moyens de télécommunication – ainsi que d'autres moyens d'information et de communication – considérant qu'une telle concentration nuit à la diversité indispensable des sources d'information et pourrait être un instrument de propagande contre la paix et d'incitation à la guerre;

– Il faut créer un système multilatéral, intergouvernemental, démocratique et transparent d'administration et de contrôle de l'Internet et autres réseaux internationaux d'information et de communication. Le caractère intergouvernemental du système d'examen est une condition indispensable;

– Les systèmes de contrôle et de surveillance des télécommunications et autres formes de communications internationales doivent être multilatéraux et transparents; les responsabilités doivent être clairement définies, de même que les procédures d'examen public, afin qu'il soit mis fin aux violations de la confidentialité et aux atteintes à la souveraineté et à la sécurité de nombreux États que commettent les systèmes mondiaux d'espionnage mis au point par certaines puissances industrielles, en particulier les États-Unis;

– Il faut prendre des mesures pour garantir fermement le respect de la diversité culturelle et éliminer toute forme de discrimination ou d'incitation à la haine du contenu des informations diffusées par les systèmes télématiques au niveau international.

El Salvador

[Original : espagnol]
[30 juin 2003]

Réponse du Gouvernement salvadorien au paragraphe 3 du dispositif de la résolution 57/53, « Les progrès de la téléinformatique dans le contexte de la sécurité internationale »

1. L'article 24 de la Constitution salvadorienne interdit l'ingérence et l'intervention dans les communications téléphoniques et constitue le cadre constitutionnel qui régit El Salvador en ce qui concerne la sécurité de l'information et des télécommunications.

2. À cet égard, les articles 184, 185, 186 et 302 du Code pénal sanctionnent l'appropriation par quiconque de communications écrites, de supports informatiques ou de quelque autre document ou effet personnel qui ne lui est pas destiné et l'appropriation de données confidentielles de caractère personnel ou familial; il est interdit notamment de capter des communications, d'intercepter ou d'interrompre des communications télégraphiques ou téléphoniques, de s'ingérer ou d'intervenir dans ces communications, en utilisant des dispositifs techniques d'écoute ou d'enregistrement.

3. De tels actes ne constituent pas des délits dans les cas de réception de menaces, ou de sauvetage d'une personne privée de liberté ou enlevée, ou lorsqu'il s'agit de délits de criminalité organisée et que la victime, l'auteur de l'acte ou son représentant, le cas échéant, ont demandé au Bureau du Procureur général de la République de procéder à l'écoute ou à l'enregistrement de conversations ou

d'actions au cours desquelles des menaces ou exigences de ce type ont été formulées, ou l'ont autorisé par écrit à ce faire.

4. L'application du cadre de réglementation des télécommunications et l'imposition de sanctions administratives relèvent de la compétence de la Superintendance générale de l'électricité et des télécommunications, conformément à l'article 4 de la loi portant création de cet organe et à l'alinéa b) de l'article 29 de la loi sur les télécommunications, qui stipulent la protection de la confidentialité des communications.

5. En 2001 et 2002, l'Assemblée législative a été saisie d'une proposition de réforme de la Constitution, qui permettrait l'ingérence ou l'intervention dans les communications téléphoniques, comme mécanisme d'appui à la lutte contre la criminalité organisée et le trafic de stupéfiants, mais à ce jour cette proposition n'a pas encore été approuvée.

Fédération de Russie

[Original : russe]
[28 avril 2003]

Questions liées aux travaux du Groupe d'experts gouvernementaux sur le problème de la sécurité de l'information

1. En application des résolutions 56/19 et 57/53, intitulées « Les progrès de la téléinformatique dans le contexte de la sécurité internationale », que l'Assemblée générale a adoptées par consensus les 29 novembre 2001 et 22 novembre 2002, respectivement, un groupe d'experts gouvernementaux sera constitué en 2004. Ces résolutions, donnant pour mission au Groupe d'experts gouvernementaux d'examiner la question des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information ainsi que les mesures de coopération qui pourraient être prises pour y parer, de procéder à une étude sur des principes internationaux qui seraient susceptibles de renforcer la sécurité des systèmes télématiques mondiaux et de présenter un rapport sur les résultats de cette étude à l'Assemblée générale à sa soixantième session.

2. La Fédération de Russie note que la question de la sécurité internationale de l'information reste au premier plan de l'actualité et estime qu'à l'heure actuelle, la sécurité de l'information constitue un aspect important de la sécurité nationale des États et qu'elle fait également partie intégrante d'un système global de sécurité internationale et de stabilité stratégique. Les questions relatives à l'utilisation des technologies de l'information et des moyens de télécommunication sont directement liées à celle du maintien de la sécurité politique et militaire des pays du monde entier et exigent, par voie de conséquence, une approche globale universelle et non discriminatoire fondée sur la participation d'un nombre maximum de pays à leur examen et sur le principe d'une représentation géographique équitable.

3. Le travail accompli sous l'égide de l'Organisation des Nations Unies peut justement garantir une telle approche car avec les atouts dont elle dispose en tant qu'organisation internationale centrale représentant au mieux les intérêts de tous les pays et jouant un rôle de coordination dans le domaine du désarmement, il est

possible de forger un système efficace et équilibré de sécurité universelle en s'appuyant sur elle.

4. Nous estimons que, pour ce qui est de l'étude de l'ensemble des questions liées à la problématique de la sécurité internationale de l'information, et de l'élaboration de recommandations connexes, les résolutions de l'Assemblée générale 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, qui sont traditionnellement adoptées par consensus et reflètent de ce fait les points de vue de tous les membres de la communauté internationale sur le problème considéré, ont joué un rôle utile, de même que les contributions correspondantes des États, qui figurent dans les rapports du Secrétaire général publiés sous les cotes A/54/213, A/55/140 et Corr.1 et Add.1, A/56/164 et Add.1 et A/57/166 et Add.1.

5. S'agissant de l'inventaire des approches qui existent à l'heure actuelle à l'égard des questions relatives à la sécurité de l'information sur le plan international, le séminaire international que l'Institut des Nations Unies pour la recherche sur le désarmement a organisé sur ce thème en août 1999 à Genève conformément aux recommandations figurant dans la résolution 53/70 et auquel ont assisté des représentants de plus de 50 pays, a joué un rôle important.

6. Le séminaire a confirmé que la question de la sécurité de l'information était d'actualité et qu'il était opportun de l'aborder sur un plan international. Il a également permis de cerner différentes approches pour l'examen de la nature des problèmes. À l'heure actuelle, il n'existe pas de normes ou d'instruments adéquats et universellement acceptés, dans lesquels la problématique de la sécurité de l'information serait envisagée sous l'angle des mesures à prendre pour réduire les risques qui se posent ou pourraient se poser dans ce domaine à l'échelle mondiale.

7. À cet égard, il apparaît nécessaire d'étudier les conceptions et les approches qui existent sur le sujet considéré, ainsi que de procéder à une analyse des instruments juridiques internationaux qui ont déjà été adoptés sur divers aspects de la sécurité internationale de l'information, en établissant une concertation à laquelle tous les pays pourront participer.

8. Nous pensons qu'avec la création d'un groupe d'experts gouvernementaux sur la question de la sécurité de l'information, le dialogue multilatéral qui s'est instauré sur cette problématique entre maintenant dans une nouvelle phase. Ce groupe d'experts offre à la communauté internationale un cadre idéal pour étudier l'ensemble des questions qui ont été mentionnées plus haut.

9. La Fédération de Russie souhaiterait participer de façon constructive aux travaux du Groupe d'experts gouvernementaux et voudrait, à ce propos, partager quelques réflexions au sujet des questions qui, selon elle, pourraient figurer à son ordre du jour.

10. Lorsqu'on se penche sur les problèmes liés à la sécurité internationale de l'information, il faut commencer par définir des valeurs communes à toute l'humanité, telles que la nécessité de garantir un échange universel, libre, équitable et sûr d'informations au niveau international, fondé sur les règles et principes généralement admis du droit international.

11. Dans le cadre des travaux du Groupe d'experts, il faudrait tenir compte des contributions présentées par les États en application des résolutions pertinentes de

l'Assemblée générale relatives à la sécurité internationale de l'information et d'autres documents qui pourraient être soumis à l'examen du Groupe.

12. À notre avis, le Groupe pourrait axer ses débats sur les considérations suivantes qui nous paraissent essentielles :

13. Premièrement, recherche d'un consensus sur des outils conceptuels appropriés dans le domaine de la sécurité internationale de l'information. Au cours de cette phase de ses travaux, le Groupe d'experts gouvernementaux pourrait s'attacher à définir des notions fondamentales – réseaux et systèmes d'information, ressources en information, infostructures, armes informatiques –, à déterminer les caractéristiques des menaces contre la sécurité de l'information et leur typologie à établir une classification correspondante.

14. Deuxièmement, examen des facteurs qui influent sur l'état de la sécurité internationale de l'information. La sécurité de l'information est un sujet vaste et complexe qui exige, de la part de la communauté internationale, une approche globale tenant compte de l'existence de menaces de nature terroriste ou criminelle tant dans le domaine militaire que dans le domaine civil.

15. Dans la société mondiale de l'information qui se dessine, les technologies de l'information et des communications sont liées entre elles et ont une dimension transfrontière. Il en résulte que, au sein de cette société, la question de la sécurité internationale de l'information est indissolublement et naturellement liée à celles qui ont trait à la détermination de l'origine des menaces et à leur localisation (interne ou externe), à la souveraineté nationale des États et au respect des droits de l'homme et des libertés fondamentales, en particulier le droit à la protection de la vie privée. Ces questions et d'autres questions connexes pourraient faire l'objet de discussions dans le cadre des travaux du Groupe d'experts gouvernementaux.

16. L'étape suivante pourrait porter sur la définition de mesures mutuellement acceptables visant à prévenir l'exploitation des technologies et des moyens d'information à des fins terroristes ou à d'autres fins criminelles et à limiter l'emploi d'armes informatiques, en particulier à l'encontre de structures étatiques vitales. À notre avis, les tâches auxquelles on pourrait s'atteler seraient les suivantes : étudier les possibilités d'élaborer une procédure de notification mutuelle et de prévention de l'utilisation d'influence non utilisées de l'information en vue d'influencer d'autres États, de créer un système de surveillance internationale destiné à décaler les menaces dans le domaine de l'information, un mécanisme chargé de veiller au respect du régime international de sécurité de l'information, et un mécanisme de règlement des différends dans le domaine de la sécurité de l'information, et de mettre en place un système international de certification de la sécurité des technologies de l'information et des moyens de télécommunication (y compris les logiciels et le matériel informatique).

17. Il conviendrait de réfléchir sur les formes que pourrait prendre la 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, et plus particulièrement en vue de détecter les sources d'agressions; de se pencher sur le problème de la coordination des législations des différents pays sur les questions relatives à la sécurité de l'information afin d'harmoniser la classification des délits dans le domaine de la sécurité de l'information et de permettre le déclenchement de poursuites à l'encontre des auteurs d'actes délictueux.

18. On pourrait aussi proposer d'évaluer la possibilité de fournir une assistance internationale aux pays qui ont été victimes d'agressions dans le domaine de

l'information en vue d'atténuer les conséquences des perturbations qu'elles entraînent, surtout lorsqu'elles visent des infrastructures vitales de l'État.

19. À plus long terme, il conviendrait peut-être de s'appliquer à élaborer un instrument multilatéral mutuellement acceptable visant à renforcer le régime de sécurité juridique internationale, en vertu duquel les États et d'autres sujets de droit international devront assumer une responsabilité internationale pour les activités qu'ils mènent ou qui sont menées à partir de territoires relevant de leur juridiction, dans le domaine de l'information.

20. De l'avis de la Fédération de Russie, l'idée fondamentale qui sous-tend la création d'un régime universel de sécurité de l'information au niveau international pourrait résider dans l'obligation, pour les participants, de ne pas se livrer, dans le domaine de l'information, à des activités qui auraient pour but de porter atteinte aux réseaux, systèmes, sources et processus d'information d'un autre État, ou à son infrastructure, de saper des systèmes politiques, économiques et sociaux ou d'exercer une vaste manipulation psychologique sur des populations en vue de déstabiliser une société et un État.

Géorgie

[Original : anglais]
[24 juin 2003]

1. Le Gouvernement géorgien travaille actuellement à élaborer une stratégie nationale de l'information visant à développer le domaine des télécommunications et à promouvoir les nouvelles technologies, en soulignant dans le même temps l'importance de la politique suivie par les pouvoirs publics pour sécuriser l'utilisation de la téléinformatique.

2. En outre, le Gouvernement géorgien adopte des politiques visant à intégrer la Géorgie dans la société mondiale de l'information, étant là aussi consciente de tous les risques et problèmes qui existent dans le domaine de la sécurité de l'information.

3. Le Gouvernement géorgien estime de la plus haute importance de participer à des programmes et projets de coopération internationaux visant à établir une société internationale de l'information plus sûre, étant bien entendu qu'étant donné les réalités actuelles des technologies et systèmes de téléinformatique, ainsi que des particularités de la région dans laquelle la Géorgie est située, il est impossible de s'attaquer aux problèmes de la sécurité téléinformatique de façon unilatérale.

Sénégal

[Original : français]
[9 juin 2003]

1. Les mesures relatives à la sécurité téléinformatique interviennent dans le domaine de l'échange d'informations, notamment celles liées à la circulation des armes. Ces informations doivent être revêtues du sceau de la confidentialité.

2. Par conséquent, elles doivent être sécurisées par un certain nombre de dispositions, à savoir :

a) La sécurité des matériels, des logiciels et traitements informatiques par la mise en place de dispositifs techniques adaptés;

b) La sécurité des procédures d'échanges d'informations grâce à une réglementation précise et unique.

Ukraine

[Original : russe]
[27 mai 2003]

1. Problèmes généraux en matière de sécurité de l'information

1. Les processus internationaux de mondialisation, l'adoption des technologies de pointe et l'avènement de la société de l'information renforcent l'importance de cet aspect de la sécurité nationale que constitue la sécurité de l'information.

2. Le développement de l'infrastructure informationnelle de l'État, l'élaboration et la mise en application de nouvelles technologies font naître des menaces particulières contre la sécurité de l'information, dont les plus importantes sont celles à caractère intentionnel, qui peuvent avoir pour origine l'existence objective et subjective, pour les personnes physiques et morales participant aux échanges d'informations, d'intérêts moraux, intellectuels et matériels, ainsi que les moyens, les formes et les méthodes employés pour satisfaire ces intérêts, le tout pouvant être source de situation conflictuelle.

3. Les principales menaces contre la sécurité de l'information prennent les formes suivantes :

– Manipulation de l'information (désinformation, dissimulation ou altération de données);

– Violation de l'ordre établi concernant l'échange de données, accès non autorisé ou restriction non justifiée de l'accès aux ressources informationnelles, collecte et utilisation illicites de données;

– Atteinte à l'espace informatique de l'État ou utilisation de cet espace à des fins hostiles à l'État;

– Terrorisme informatique, comme, par exemple, la propagation de « virus » informatiques, l'installation de logiciels et autres programmes renifleurs, la pose de dispositifs électroniques d'interception des données dans les équipements et les locaux, l'utilisation illégale des systèmes de téléinformatique et de leurs ressources et la diffusion massive de fausses informations, notamment.

4. Ces agissements aboutissent directement à l'altération de l'information, c'est-à-dire la déformation et/ou la destruction de l'infrastructure informationnelle de l'État et de ses ressources, à la mise hors service d'importants systèmes informatiques gouvernementaux, industriels, financiers, scientifiques et culturels et, par voie de conséquence, à la perte de la souveraineté nationale en matière d'information.

5. Il ressort de cette analyse que les problèmes les plus courants en matière de sécurité de l'information concernent le maintien du niveau quantitatif et qualitatif

des ressources informationnelles, l'élaboration de stratégies pour l'utilisation de ces ressources et de technologies correspondantes, la mise en place d'une infrastructure appropriée, la sécurité de l'information dans les systèmes informatiques et les télécommunications, ainsi que la lutte contre les effets préjudiciables des atteintes à la sécurité de l'information pour les individus, la société et l'État dans son ensemble.

6. Un niveau insuffisant de protection des ressources informationnelles de l'État peut entraîner des dommages économiques considérables, par suite de la dépréciation et de la perte de la valeur marchande des technologies industrielles et informatiques, et compromettre gravement l'ensemble de la sécurité nationale, par suite d'éventuels dysfonctionnements des systèmes de communication, de contrôle et de gestion ou de la divulgation d'informations relevant du secret d'État, etc.

7. La sécurité de l'information suppose l'application de mesures de protection à tous les stades. Elle vise à assurer l'intégrité des systèmes, à protéger et garantir l'exactitude et l'intégrité de l'information, ainsi qu'à limiter les effets des problèmes qui pourraient survenir en cas d'altération ou de destruction des données.

8. La réalité objective du monde contemporain est celle de l'utilisation, dans différents domaines d'activité de la société et de l'État, de systèmes informatiques locaux et mondiaux, conçus pour accélérer l'échange de données et l'accès à toutes sortes de ressources informationnelles.

9. Le large recours à ces systèmes, notamment dans les domaines d'activité liés à l'administration de l'État, fait naître des possibilités réelles d'accès non autorisé aux ressources informationnelles de l'État et à leurs systèmes de gestion, de diffusion d'informations au contenu illicite et d'atteinte à l'intégrité et à l'accessibilité de l'information, etc.

10. La stabilité du fonctionnement des sphères politique, économique, militaire et financière, notamment, de l'État dépend non seulement de l'efficacité mais aussi de la fiabilité du fonctionnement des télécommunications et des systèmes informatiques. Dans le contexte de la création d'un espace informatique, les questions de fiabilité et de protection des systèmes informatiques et des télécommunications utilisés à des fins administratives se posent avec une acuité et une actualité particulières. Avoir accès aux systèmes d'information permet non seulement d'obtenir des données importantes, mais aussi – en entravant ou en bloquant le fonctionnement desdits systèmes – de paralyser totalement ou partiellement l'activité d'installations vitales, voire de pans entiers de l'économie, de pervertir les ressources informationnelles et de diffuser des informations interdites par la loi.

11. La sécurité des données qui circulent dans les systèmes de téléinformatique est l'un des principaux facteurs, ainsi qu'une condition essentielle, de la sécurité de l'information, de la souveraineté nationale et du développement social durable.

12. Au stade actuel de développement des systèmes informatiques et des télécommunications, les menaces les plus graves concernant les données susvisées prennent les formes suivantes :

– Entrave au bon fonctionnement des grands systèmes d'information et de télécommunications;

– Actes fortuits ou intentionnels portant atteinte à la confidentialité, à l'intégrité et à l'accessibilité de l'information;

– Déclenchement d'une situation conflictuelle en matière d'information (propagation de « virus » informatiques, installations de logiciels et autres programmes renifleurs, pose de dispositifs électroniques d'interception des données dans les équipements et les locaux, interception et déchiffrement des données, diffusion massive de fausses informations, utilisation de moyens électroniques pour pervertir les systèmes de mot de passe et d'identifiant ou mettre hors service les systèmes de communication et de gestion, etc.).

13. Les systèmes informatiques et les télécommunications, à commencer par ceux des pouvoirs publics, ne pourront être efficacement protégés contre les atteintes que si l'on met en place un système complexe de protection des données, prévoyant l'utilisation de moyens cryptographiques et techniques de protection, ainsi que l'application de toute une série de mesures d'ordre organisationnel et technique.

14. Le problème du raccordement des réseaux informatiques aux réseaux internationaux doit bénéficier d'une attention particulière.

15. Pour devenir membre à part entière de la communauté internationale, l'Ukraine doit renforcer son interaction avec les systèmes mondiaux de transmission de données, dont le réseau Internet. Ces systèmes proposent un large choix de services de téléinformatique, dont beaucoup prétendent garantir la sécurité des données.

16. Cependant, un grand nombre de moyens mis en oeuvre par ces systèmes (dont les caractéristiques sont très difficiles, voire impossible, à apprécier si l'on ne dispose pas des codes sources des programmes) risquent de compromettre la sécurité de l'information, les transactions financières et les télépaiements. On connaît de nombreux cas d'utilisation malencontreuse par les banques de technologies importées permettant à un bon informaticien de faire intrusion dans un système à l'occasion d'une connexion d'une dizaine de minutes.

17. Il convient également de prêter attention au danger posé par le raccordement des abonnés et des réseaux locaux aux réseaux mondiaux. Pratiquement n'importe quel réseau informatique local relié à l'Internet sans mesure de protection devient aisément accessible aux « hackers ».

18. Le passage à des formes et modes nouveaux de réalisation des échanges informatiques, notamment la généralisation des nouvelles formes d'initiative économique utilisant l'Internet (commerce électronique), tout comme la mise en place progressive de systèmes d'administration électronique, s'accompagne d'un large recours aux technologies informatiques et d'une augmentation des volumes de données sous forme électronique. Les utilisateurs deviennent ainsi de plus en plus tributaires du degré de protection de ces données, qui, à leur tour, sont convoitées par des individus mal intentionnés et les groupes auxquels ils appartiennent. L'insuffisance des systèmes et dispositifs existants de protection favorise l'accès non autorisé aux ressources informationnelles ainsi que l'utilisation, le blocage ou la destruction desdites données, qui sont créées, traitées, transmises et conservées sous forme électronique.

19. Le problème de l'ingérence dans les ressources informationnelles de l'État touche désormais le monde entier. Alors que, jusqu'au début des années 90, les États

se souciaient principalement de se protéger contre les services de renseignements étrangers, le principal problème qui se pose depuis peu, avec le recours accru aux technologies de l'information dans tous les domaines de la vie sociale, est celui des agissements de ce qu'il est convenu d'appeler les délinquants informatiques. En témoigne le fait que la délinquance informatique est reconnue au niveau international comme une nouvelle forme d'atteinte à la propriété intellectuelle. Qui plus est, les auteurs de ces infractions sont non seulement des groupes criminels organisés, mais aussi des organisations terroristes et des individus agissant pour leur propre compte.

20. Ces délinquants s'intéressent particulièrement aux systèmes informatiques des pouvoirs publics, des autorités chargées de l'application des lois, des administrations douanières et fiscales, des établissements bancaires, de l'armée, etc. En particulier, les services de répression ukrainiens ont été amenés à constater à maintes occasions des opérations illicites concernant l'utilisation des cartes des systèmes de paiement internationaux, ainsi que des télépaiements fictifs effectués pour obtenir illégalement de l'argent, et des cas d'ingérence dans des réseaux informatiques par le biais de l'Internet, notamment.

2. Définition des concepts fondamentaux en matière de sécurité informatique, notamment les interférences illicites dans les systèmes télématiques ou l'utilisation illégale de ces systèmes

21. Le développement extrêmement rapide des technologies de l'information et de la communication donne une grande acuité aux problèmes d'intrusion ou d'utilisation illicite des systèmes correspondants, et à celui de la protection des ressources informationnelles.

22. L'expression *sécurité informatique* doit s'entendre d'un état de protection de l'espace informatique d'un pays favorisant les intérêts nationaux et respectant les droits de la personne, de la société et de l'État.

23. Étant donné la gravité des dangers que présentent pour la société ces actes illicites, et l'importance du bon fonctionnement des systèmes informatiques et des télécommunications, le Code pénal ukrainien définit les délits ci-après en matière d'utilisation des ordinateurs, des systèmes et des réseaux, et prévoit les sanctions correspondantes, notamment :

- Intrusion dans le fonctionnement d'ordinateurs, de systèmes et de réseaux informatiques – actes ayant entraîné l'altération ou la destruction de données informatiques ou de fichiers, propagation de virus informatiques par différents moyens (programmes, techniques) visant à accéder frauduleusement à des ordinateurs, des systèmes ou des réseaux;
- Vol, appropriation illicite ou extorsion de données informatiques ou acquisition par des moyens frauduleux ou par utilisation abusive de la situation professionnelle;
- Enfreinte des règles d'exploitation d'ordinateurs, de systèmes ou de réseaux informatiques par une personne responsable de leur exploitation – actes ayant entraîné le vol, l'altération ou la destruction de données informatiques ou de moyens de protection, ou la copie illicite de telles données, ou une perturbation grave du fonctionnement d'ordinateurs, de systèmes ou de réseaux.

24. De manière plus générale, on peut définir le *délit informatique* comme acte illicite portant atteinte à l'ordre de fonctionnement établi de systèmes informatiques et d'accès à ces systèmes, violant l'intégrité ou la confidentialité des données ou les modalités d'accès à des données, ou les droits et les libertés des personnes au cours de leurs activités informatiques.

3. Teneur des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux

25. Le XXIe siècle doit entrer dans l'histoire comme la période de mise en place et de développement de la société informatique mondiale, appelée à remplacer ou compléter les processus d'échanges matériels par des processus informatiques, et à favoriser par ailleurs la croissance de la productivité du travail et l'élévation du niveau de vie. Il y a déjà de nombreux pays qui se dotent de la base structurelle et technique nécessaire pour la mise en place d'infrastructures nationales et mondiales. L'ONU examine s'il y a lieu d'inclure l'accès aux moyens de base d'information et de communication parmi les droits fondamentaux inscrits dans la Déclaration universelle.

26. L'expérience des pays développés en matière de solutions d'informatisation efficaces, diffusée dans la seconde moitié des années 90 par des organisations internationales (Union internationale des télécommunications, Commission électrotechnique internationale, Institut européen des normes de télécommunications) et par nombre d'organisations nationales de normalisation, montre qu'il est indispensable de créer des infrastructures informatiques multiniveaux (nationales et régionales), qui seraient à terme réunies en une infrastructure mondiale de l'information (GII).

27. La participation de l'Europe à une GII ne nécessite pas seulement la mise en place dans la région d'une infrastructure européenne de l'information, mais aussi la promotion de la création d'infrastructures nationales de l'information dans différents pays, qui serait mutuellement avantageuse pour eux et pour l'Europe dans son ensemble. Plutôt que d'« infrastructure européenne de l'information », l'Union européenne a préféré parler de « Société de l'information européenne », qui se construit à partir des réseaux, des services de base et des services auxiliaires. Les réseaux déjà en place en Europe peuvent être renforcés par la réalisation d'une autoroute européenne de l'information à large bande, groupant en un ensemble unique tous les réseaux européens – télécommunications, réseaux câblés et réseaux satellitaires. Les pays d'Europe soutiennent l'utilisation de services de base transeuropéens, y compris le courrier électronique et la transmission de fichiers et de vidéos.

28. Les pays d'Europe prêtent beaucoup d'attention aussi aux aspects sociaux de l'étape actuelle de la révolution technologique. Le Conseil de l'Europe a consacré des résolutions et d'autres textes à l'élaboration de politiques nationales pour l'édification d'une société de l'information, perçue non pas comme concession à la mode, mais comme condition *sine qua non* du développement, dont le refus entraîne une baisse des rendements et la perte de positions économiques et technologiques de pointe.

29. Dans le monde, les tendances de la régulation juridique des activités relevant des technologies modernes de transmission des données rendent manifeste la nécessité d'arriver à des conceptions uniformes en matière de législation et de

réglementation pour tous ceux qui participent aux échanges internationaux d'informations. Il est désormais indispensable, selon l'*American Bar Association*, de créer une commission multinationale chargée de légiférer dans le cyberespace. Parmi les décisions qu'elle aurait à examiner, l'une des plus importantes concernerait la création d'un cybertribunal. Actuellement, le problème principal, si on veut protéger la sécurité informatique par la législation, est de mettre les textes à niveau pour qu'ils ne soient pas en retard sur les progrès de la technologie.

30. Il est impossible pour le moment d'imaginer l'espace informatique sans réseaux d'ordinateurs, qui sont précisément à l'origine de la naissance et du développement de nombre d'activités commerciales : cartes de débit, opérations interbanques, services des bourses de valeurs, des bureaux de courtiers, etc.

31. On prévoit que d'ici à 2005, la moitié de la population de l'Union européenne aura accès à Internet. Les pays de l'Union s'efforcent donc de consolider la confiance dans les opérations commerciales et financières réalisées en ligne, et d'accélérer le passage au commerce électronique.

32. Le Parlement européen a coordonné le 7 mai 1999 le projet de loi ENFOPOL 98, qui donnerait le droit aux services compétents de surveiller les réseaux en toute légalité. C'est le projet de la résolution du Conseil européen concernant l'interception légale des télécommunications dans le cadre des nouvelles technologies, qui ouvre aux services chargés de la surveillance en temps réel l'accès à tous les réseaux de télécommunications, y compris Internet et les réseaux de téléphonie par satellites. Le Gouvernement britannique a pour sa part lancé un projet de centre qui sera chargé d'intercepter l'ensemble des échanges électroniques à l'intérieur du pays.

33. Le Gouvernement chinois a choisi, pour contrôler l'accès au réseau, le système des licences d'utilisation des modems, outre que tous les courants d'information par Internet y sont acheminés par l'intermédiaire d'un petit nombre d'opérateurs nationaux.

34. Les problèmes que pose la sécurité informatique sont notamment les suivants :

– Atteinte aux droits de propriété intellectuelle;

– Diffusion d'informations nuisibles pour la santé sociale de la population, et notamment problèmes posés par l'accès des enfants à Internet;

– Opérations commerciales illicites;

– Accès non autorisé à des données confidentielles (intrusion);

– Atteinte aux droits et intérêts légitimes des personnes lors des échanges d'informations;

– Diffusion de publicité de mauvaise qualité.

35. Internet présente encore un autre risque, celui d'une utilisation non autorisée d'informations confidentielles – or il est possible de collecter de telles informations en analysant les données dont la victime se sert sur Internet.

36. Internet est un moyen de communication très spécifique, sur lequel il est difficile de légiférer à cause de son caractère transfrontières. Toutes les entités présentes sur Internet sont soumises à la législation de leurs pays respectifs. Mais un contenu illicite peut être mis en évidence sur le territoire d'un pays qui n'est pas

celui où se trouve le serveur sur lequel il est conservé. Une législation d'Internet appelle donc des accords internationaux, dont l'adoption est rendue plus complexe du fait que les législations nationales ne procèdent pas de conceptions uniformes de tel ou tel délit, la « pornographie », par exemple, pouvant faire l'objet de définitions assez diverses. Les initiatives législatives actuelles visant Internet ont généralement pour but de rendre les prestataires de services d'hébergement responsables du contenu des données conservées sur leurs ordinateurs. Du point de vue technique, cette responsabilité est compliquée à établir, de sorte que la législation de certains pays ne les rend responsables que s'ils connaissent les contenus illicites.

37. Interpol, qui groupe les services de répression de 178 pays du monde, a fait savoir qu'il afficherait des informations sur les délits contre les réseaux sur le site de la société américaine Atomic Tangerine. Cette dernière doit pour sa part communiquer à Interpol les informations obtenues par le système d'alerte avancée NetRadar, qui lui appartient et qui est conçu pour assurer la surveillance sur le Web.

38. L'un des problèmes importants qui se posent est celui de l'anonymat des communications, qui complique, ou rend même impossible, l'identification du propriétaire des contenus illicites, et donc les poursuites contre lui. Aussi les experts de nombreux pays proposent-ils donc d'inscrire dans la législation l'interdiction des communications anonymes, tout en autorisant les communications sous pseudonyme (ce dernier permettant en cas de nécessité d'identifier l'auteur).

39. Le 21 décembre 1998, le Conseil européen a approuvé le plan d'action proposé par le Parlement européen, visant à promouvoir une utilisation plus sûre d'Internet, portant sur quatre années (1er janvier 1999 au 31 décembre 2002), et doté d'un budget de 25 millions d'euros. Il prévoyait la mise en place d'un système de niveaux de qualité des sites Internet, avec « labels de qualité » visibles. Ces dispositions devaient être inscrites dans les législations nationales et dans les codes de conduite (autoréglementation) des fournisseurs d'accès. En mars 1999, la Commission européenne a publié les résultats d'une consultation publique sur le Livre vert sur la convergence des secteurs des télécommunications, des médias et de la technologie de l'information, indiquant notamment, en ce qui concerne le rôle de la réglementation, le besoin de transparence, de clarté et de proportionnalité.