Nations Unies A/61/161

# Assemblée générale

Distr. générale
18 juillet 2006
Français
Original : anglais/arabe/chinois/
espagnol

**Soixante et unième session**
Point 82 de l'ordre du jour provisoire*
**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

## Table des matières



* A/61/150.

06-43426 (F) 090806 110806

# I. Introduction

1. Au paragraphe 3 de sa résolution 60/45 sur les 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 questions suivantes : a) les problèmes généraux en matière de sécurité de l'information; b) les efforts engagés au niveau national pour renforcer la sécurité de l'information et les activités de coopération internationale menées dans ce domaine; c) la teneur des principes susceptibles de renforcer la sécurité des systèmes mondiaux dans le domaine de la téléinformatique; d) les mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial.

2. Dans une note verbale datée du 23 février 2006, les États Membres ont été invités à communiquer au Secrétaire général leurs vues et observations sur la question. Le texte des réponses reçues figure à la section II ci-après. Les autres réponses reçues feront l'objet d'additifs au présent rapport.

# II. Réponses reçues des Gouvernements

**Bolivie**

[Original : espagnol]
[13 juin 2006]

Dans sa résolution 60/45, l'Assemblée générale préconise l'examen multilatéral des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information, ainsi que des mesures susceptibles d'être prises pour limiter ces risques, compte tenu de la nécessité de préserver la libre circulation de l'information.

**Évaluation générale des problèmes de sécurité de l'information**

Les progrès considérables accomplis dans la mise au point et l'application des technologies de l'information et des communications, comme l'Internet, la télécopie, la téléphonie mobile et la téléphonie par satellite, font que l'information est diffusée de façon indiscriminée et sans restriction dans le monde entier, ce qui peut permettre d'accéder à des données confidentielles.

Ce processus comporte néanmoins de vastes possibilités favorables à l'évolution de la civilisation en multipliant les occasions de coopérer pour le bien commun des États et la réalisation de nouveaux objectifs au service de l'humanité.

Du point de vue de la défense, la sécurité de l'information est gérée à un niveau peu élevé (par l'entreprise qui offre le service). Il n'existe pas de politiques de sécurité interne dans ce domaine.

**Mesures prises au niveau national pour renforcer la sécurité de l'information et contribuer à la coopération internationale dans ce domaine**

Compte tenu des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des télécommunications entre autres mesures de coopération, nous nous sommes dotés d'un dispositif par lequel l'information obtenue est communiquée au Ministère de l'information et administrée par la Direction des télécommunications.

S'agissant de la défense, les mesures de sécurité prises sont insuffisantes compte tenu des progrès techniques actuels.

Aujourd'hui, on élabore des projets de télécommunication auxquels sont appliquées des normes maximales de sécurité de l'information grâce au codage de la transmission des données, en vue de combler les lacunes ou de remédier aux déficiences constatées.

**Teneur des principes visés au paragraphe 2 de la résolution 60/45**

On estime que l'étude de principes internationaux susceptibles de renforcer la sécurité des systèmes mondiaux dans le domaine de la téléinformatique servirait les buts des mesures énoncées au paragraphe 2.

**Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité informatique à l'échelle mondiale**

- Évaluer les problèmes de sécurité téléinformatique au niveau international
- Définir des critères de base concernant la sécurité téléinformatique, les accès non autorisés ou l'utilisation illicite des systèmes en question par le biais de l'Internet
- Élaborer des principes internationaux permettant d'accroître la sécurité des systèmes informatiques et télématiques au niveau mondial, contribuant ainsi à la lutte contre le terrorisme et le trafic de données confidentielles
- Se déclarer préoccupée par le fait que la téléinformatique risque d'être utilisée à des fins contraires à la stabilité et à la sécurité des États
- Dans le domaine militaire et dans celui de la défense, mettre en place des systèmes de télécommunication dotés de dispositifs de sécurité compatibles avec les progrès techniques mondiaux

**Recommandations**

La sécurité de l'information doit être vue comme une politique d'État, concrétisée dans la loi sur les télécommunication, réglementée et contrôlée par la Direction des télécommunications.

Pour ce qui est de la sécurité de l'information au niveau national, il faudrait mettre en place des projets de télécommunication de pointe qui incorporent dans leur système d'exploitation des normes de sécurité maximales.

## Chine

[Original : chinois]
[24 mai 2006]

### Vues de la Chine sur la question de la sécurité de l'information

Les progrès rapides accomplis actuellement dans le domaine des technologies de l'information constituent un atout important pour la promotion du développement économique et social et l'amélioration de la vie de tous les peuples. Parallèlement, le développement et l'essor de la téléinformatique présentent également des risques sans précédent pour la sécurité nationale et internationale. La question de la sécurité de l'information est devenue un élément important non seulement de la sécurité de chaque pays mais aussi de la sécurité et de la stabilité mondiales. Il incombe à la communauté internationale de régler la question comme il convient dans l'intérêt de tous les pays.

La Chine estime que la question de la sécurité de l'information recouvre non seulement les risques que présente la vulnérabilité de l'infrastructure téléinformatique mais aussi les conséquences politiques, économiques, militaires, sociales et culturelles du mauvais usage de ces technologies. Les deux aspects doivent bénéficier d'une attention égale.

La Chine est d'avis que l'usage fait de la téléinformatique doit être conforme aux dispositions de la Charte des Nations Unies et aux normes fondamentales qui régissent les relations internationales. Il faut assurer la libre circulation de l'information tout en préservant la souveraineté et la sécurité nationales, en respectant la législation interne et les différences historiques, culturelles et politiques entre les pays. Chaque État a le droit de réglementer son propre cyberespace conformément à ses lois internes. La communauté internationale doit coopérer davantage dans les domaines de la recherche téléinformatique et de l'emploi des technologies de l'information et protéger le droit qu'ont tous les États d'acquérir ces technologies.

L'Organisation des Nations Unies est l'instance idoine pour examiner et régler la question de la sécurité de l'information. Bien qu'aucun résultat concret n'ait été obtenu à la réunion du Groupe d'experts gouvernementaux tenue en 2005, des experts de différents pays ont procédé à des échanges de vues sur tous les aspects de la sécurité de l'information et présenté des propositions intéressantes, ce qui permettra à la communauté internationale d'examiner et de régler la question en s'appuyant sur des bases solides. La Chine est favorable à la création, en 2009, d'un autre groupe d'experts gouvernementaux qui sera chargé de mener une étude approfondie des menaces et des risques liés à la sécurité de l'information et d'envisager les mesures à prendre pour y remédier. Comme toujours, la Chine appuiera l'action menée à l'échelle internationale pour régler la question de la sécurité de l'information et s'y associera.

**Émirats arabes unis**

[Original : anglais]
[17 juin 2006]

Les Émirats arabes unis ont conscience que la cybercriminalité représente une menace croissante et qu'elle ne s'arrête pas aux frontières traditionnelles des États. Les moyens modernes d'information et de communication offrent la possibilité d'exercer, à partir de n'importe où, des activités illégales dirigées contre n'importe quelle personne, où qu'elle se trouve.

Une action efficace s'impose aux niveaux national et international pour faire échec à la cybercriminalité.

Les Émirats arabes unis ont consenti des efforts considérables pour renforcer la sécurité de l'information au niveau national, notamment dans les domaines suivants :

• **Loi sur la cybercriminalité**

La loi sur la cybercriminalité a été approuvée et publiée au début de 2006. Elle porte sur les infractions suivantes :

– Infractions liées à l'accès (accès non autorisés, diffusion de virus, piratage informatique, usurpation d'identité)

– Infractions visant les données (interception, modification, vol, atteinte à la confidentialité)

– Infractions visant les réseaux (interférence, modification, destruction)

– Infractions connexes (facilitation de la commission d'infractions, trafic de drogues, traite d'êtres humains, blanchiment de capitaux, actes de terrorisme).

La loi aborde également la question de la censure et des contenus répréhensibles. Les violations de la loi sur la cybercriminalité sont passibles de peines d'emprisonnement, de pénalités financières ou des deux à la fois.

• **Équipe nationale d'intervention informatique d'urgence**

L'autorité des Émirats arabes unis chargée de la réglementation des télécommunications examine actuellement la possibilité de mettre sur pied une équipe nationale d'intervention informatique d'urgence qui aurait pour mission d'améliorer la sécurité, de lutter contre les cyberattaques, de diffuser des alertes rapides et des informations sur les cybermenaces, de coordonner l'ensemble des interventions menées en cas d'incident et de renforcer la sensibilisation dans le pays au moyen d'actions de formation et d'éducation.

• **Code de conduite à l'intention des fournisseurs d'accès à l'Internet**

Les Émirats arabes unis s'apprêtent à élaborer à l'intention des fournisseurs d'accès à l'Internet un code de conduite qui leur fera obligation de s'employer efficacement et plus activement à réduire le nombre de messages non sollicités, qui sont susceptibles de contenir des virus. Les fournisseurs d'accès devront prendre l'initiative de sonder systématiquement le trafic en ligne à la recherche de relais ouverts, de réseaux de robots logiciels («botnets ») et de réseaux d'ordinateurs compromis utilisés pour envoyer des messages non sollicités. Ils auront aussi

l'obligation d'inclure dans leurs contrats une clause les autorisant à exclure les utilisateurs qui, intentionnellement ou non, relaieraient des messages non sollicités. Toute violation des dispositions du code sera passible de pénalités ou de sanctions.

Ce code de conduite vise à faire en sorte que la communauté des fournisseurs d'accès respecte des normes de conduite élevées et des pratiques commerciales d'une grande rigueur.

• **Accords bilatéraux**

Les fournisseurs d'accès à l'Internet des Émirats arabes unis se sont employés activement à conclure des accords bilatéraux avec les pays voisins en vue de lutter contre l'arrosage et ils ont réussi à réduire le nombre de messages non sollicités relayés vers l'étranger. Les Émirats arabes unis soutiennent et encouragent la coopération internationale contre la cybercriminalité et estiment qu'il y a lieu d'étudier la possibilité d'élaborer des protocoles d'accord portant sur le partage de l'information et la lutte transfrontière contre les infractions.

• **Campagnes de sensibilisation et d'éducation**

L'autorité nationale chargée de la réglementation des télécommunications et les professionnels du secteur travaillent côte à côte pour sensibiliser le public et l'informer des possibilités qu'offre la technologie ainsi que des dangers associés à la cyberdélinquance.

Par exemple, l'autorité chargée de la réglementation des télécommunications a récemment publié des lignes directrices sur la sécurité des réseaux sans fil (Wireless Security Guidelines) et une politique relative aux services d'hébergement de pages Web (Web Hosting Policy). Les premières expliquent comment installer un réseau sans fil et décrivent les étapes à respecter pour en assurer la sécurité. La seconde définit ce qui constitue une utilisation acceptable de ces services, et contient notamment des dispositions relatives à l'utilisation, au pollupostage, aux violations de la propriété intellectuelle et aux contenus illicites.

• **Importance des mesures techniques dans le contexte de la sécurité internationale**

Divers moyens technologiques existent déjà pour améliorer la sécurité du cyberespace, notamment :

– Déploiement d'infrastructures fondées sur la clef publique (ICP) et élaboration de protocoles de sécurité;

– Mise au point de solutions de qualité, de pare-feux, de logiciels antivirus, de systèmes de gestion électronique des droits de propriété intellectuelle, de systèmes de cryptage, etc.;

– Utilisation de cartes à puce, de l'identification biométrique, de signatures électroniques, de techniques de contrôle d'accès par la fonction, etc.

Toutefois, à mesure que le cyberespace devient plus complexe et que ses composants se perfectionnent, des menaces nouvelles et imprévues se font jour. D'où la nécessité de redoubler d'efforts pour mettre au point des technologies de sécurité et pour tenir compte systématiquement des impératifs de sécurité dès l'amorce de la conception d'une nouvelle technologie, quelle qu'elle soit.

• **Mesures envisageables pour renforcer la sécurité de l'information au niveau mondial**

– La coopération internationale est absolument indispensable, la cybercriminalité étant un type de délinquance qui ne connaît pas de frontières et contre lequel les moyens de lutte traditionnels sont sans effet;

– La mise en place d'un cadre juridique commun faciliterait l'échange d'informations et la collaboration entre les pays. Il faudrait en outre mettre au point une définition globale de la cybercriminalité, sans perdre de vue le fait que les définitions spécifiques varieront d'un pays à l'autre;

– Les autorités chargées de l'application des lois devraient s'habituer à traiter les infractions liées au cyberespace. Elles devraient être en mesure de rechercher et de saisir des données stockées dans des ordinateurs de façon à empêcher la destruction de preuves.

**Jordanie**

[Original : arabe]
[5 juin 2006]

La notion de sécurité de l'information est liée à celle de sécurité nationale et le régime de sécurité de l'information a un rapport direct avec la sécurité des communications dans la mesure où c'est par l'intermédiaire des réseaux télématiques que s'effectuent le transfert et l'échange d'informations. En outre, pour protéger et renforcer la sécurité de l'information et des communications, il faut :

a) Élaborer des législations, des lois et des règlements qui préservent le caractère confidentiel et l'intégrité de l'information et garantissent l'accès à ces données, lutter contre les activités qui contreviennent à ces règles et qui les utilisent à des fins criminelles;

b) Définir un plan national qui puisse servir de fondement aux activités visant à assurer la sécurité de l'information, des communications et des réseaux, et garantir avec la participation des parties concernées :

1. La confidentialité et la fiabilité de l'information, c'est-à-dire veiller à ce que l'information ne soit pas rendue publique et à ce que seules les personnes dûment habilitées puissent en prendre connaissance;

2. La complémentarité et l'intégrité de l'information, c'est-à-dire s'assurer que le contenu des informations est correct et n'a été ni modifié ni altéré et, en particulier, qu'il n'a, à aucun stade du traitement ou de l'échange d'informations, pu être détruit, modifié ou altéré, à la suite de manipulations internes ou d'ingérences illicites;

3. L'accès permanent à l'information et aux services, c'est-à-dire garantir le fonctionnement permanent du système informatique, la présence permanente de capacité d'interaction avec l'information ainsi que la fourniture de services aux sites informatiques, et veiller à ce que les utilisateurs de l'information ne se voient pas interdire l'utilisation ou la saisie de ces données;

4. Que les comportements en rapport avec l'information ne puissent pas être désavoués par leurs auteurs, c'est-à-dire faire en sorte que les personnes

responsables d'un comportement en rapport avec l'information ou avec l'endroit ou celle-ci se trouve ne puissent pas nier avoir eu un tel comportement, dans la mesure où il existe des moyens de prouver qu'un individu s'est, à un moment donné, comporté d'une façon bien précise;

c) Élaborer une stratégie visant à garantir la sécurité de l'information, en établissant, à l'intention de ceux qui sont amenés à s'occuper de questions de technologie et d'informatique au sein d'une installation donnée, des règles relatives à la saisie, à l'organisation et à la gestion des données. Cette stratégie visera à : a) identifier les utilisateurs, les gestionnaires et à définir les obligations et les tâches dont ces derniers doivent s'acquitter pour protéger le système informatique et les réseaux, b) protéger tous les types de données, au stade de la saisie, du traitement, du stockage et de la restitution des données.

**Liban**

[Original : arabe]
[21 juin 2006]

En réponse à la communication susmentionnée relative aux progrès de la téléinformatique dans le contexte de la sécurité internationale, le Ministère national de la défense tient à préciser ce qui suit :

Pour ce qui est de la sécurité des données, les réseaux informatiques de l'armée sont des réseaux fermés auxquels s'appliquent des mesures de sécurité passives dans la mesure où il est impossible pour des raisons financières d'avoir accès à la technologie moderne nécessaire. En revanche, il n'existe aucune mesure de sécurité qui s'applique aux réseaux télématiques, dans la mesure où ces réseaux s'appuient sur le système de communications civiles qui dessert l'ensemble du Liban.

S'agissant des efforts déployés à l'échelle nationale en vue d'améliorer la protection de l'information, on notera qu'au Liban le suivi juridique des technologies de l'information et des communications possède un trait distinctif, les technologies en question étant régulièrement régies par la loi N°140 du 27 octobre 1999 qui a trait au droit à la confidentialité des communications et stipule que ces dernières ne peuvent être interceptées que sur décision judiciaire ou administrative et conformément aux dispositions énoncées aux articles 2 à 13 de cette loi. À ce propos, on rappellera que la législation en vigueur ne dit mot sur la coordination entre les services de sécurité et les sociétés publiques (ISP-GSM), qui est nécessaire si l'on veut unifier les efforts visant à détecter, à surveiller et à parer les menaces éventuelles. Ceci montre qu'une coopération internationale s'impose dans ce domaine et que l'on a besoin de compétences techniques et juridiques pour combler les lacunes dont souffre la législation libanaise relative à la technologie.

## Qatar

[Original : arabe]
[12 juin 2006]

S'agissant des progrès de la téléinformatique dans le contexte de la sécurité internationale, le Gouvernement de l'État du Qatar déploie de gros efforts pour garantir complètement la sécurité de la téléinformatique afin de se prémunir contre les menaces qui pèsent ou risquent de peser sur la sécurité de l'information, et il a promulgué des lois à cet effet.

Récemment, l'État du Qatar s'est doté d'un conseil supérieur de la télématique ainsi que d'une administration juridique, chargés de mettre la dernière main à un projet de loi sur l'électronique qui sera soumis aux instances compétentes, puis une fois adopté, ratifié et mis en œuvre durant l'année en cours.

Ce projet de loi vise à interdire l'utilisation de ressources ou de technologies informatiques à des fins criminelles ou terroristes. En outre, il impose aux instances compétentes la charge de définir les objectifs criminels et terroristes, de sorte que les États Membres soient pleinement au fait de ces questions et puissent ainsi s'acquitter au mieux de leurs obligations. Le projet de loi demande aussi aux États de s'efforcer d'aboutir à une définition commune des notions qui n'ont pas encore fait l'objet d'un accord au plan international de sorte que ces notions puissent être débattues au sein des instances internationales.