Nations Unies A/62/98

Assemblée générale

Distr. générale
2 juillet 2007
Français
Original : anglais/arabe/chinois/
espagnol/français

Soixante-deuxième session
Point 95 de la liste préliminaire*
Le progrès dans les domaines de l'informatique et des télécommunications et la question de la sécurité internationale

Le progrès dans les domaines de l'informatique et des télécommunications et la question de la sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/62/150.

07-40783 (F) 200707 250707

I. Introduction

1. Au paragraphe 3 de sa résolution 61/54 sur les progrès de l'informatique et de la télématique et la question 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 internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux; et 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 2007, 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

Brunéi Darussalam

[Original : anglais]
[23 juin 2007]

Le Brunéi Darussalam a présenté le rapport suivant, établi par la Police royale du Brunéi Darussalam.

I. Introduction

Évaluation générale des problèmes de sécurité de l'information

1. L'informatique, qui s'applique à tous les progrès dans le domaine de l'information et des télécommunications, joue désormais un rôle crucial dans tous les secteurs de la société. Elle transforme notre manière de créer, compiler, traiter, gérer et partager l'information. Les opérations et l'archivage électroniques se sont généralisés et sont essentiels dans tous les domaines, des échanges commerciaux aux soins de santé. Ces changements résultent de la mise en place des réseaux informatiques. La croissance exponentielle de l'Internet et du nombre de ses utilisateurs, d'année en année, illustre bien que l'on est en transition vers une société fondée sur les réseaux.

2. La sécurité de l'information est donc devenue un volet essentiel de l'informatique, en particulier dans le contexte de la société de l'information. Il s'agit toutefois d'un sujet complexe, et l'adoption de mesures appropriées dépendra souvent, dans une large mesure, du type de matériel et d'infrastructure informatiques et de l'endroit où ils se trouvent.

3. La mise en place des réseaux informatiques est à l'origine de nombre de ces changements, qui suscitent par ailleurs des préoccupations nouvelles quant à la sécurité et à la confidentialité des informations échangées sur les réseaux. Si ces inquiétudes ne sont pas apaisées, elles risquent de compromettre la pleine réalisation du potentiel des réseaux, en termes de participation aussi bien que d'utilité. Il est

donc indispensable d'associer les garanties institutionnelles et technologiques pertinentes à toutes sortes d'informations à caractère personnel, protégées par le droit d'auteur, sensibles ou exclusives.

4. Les menaces et les risques potentiels liés à la sécurité devront être soigneusement évalués dans toutes les situations, et il est absolument indispensable que tous les intéressés soient sensibilisés aux menaces et aux risques qui les concernent, et sur lesquels ils exercent un contrôle. Ce n'est qu'à ce moment-là qu'ils comprendront et appliqueront pleinement les procédures pertinentes en matière de sécurité.

5. L'accent sera ensuite mis sur la protection des informations non confidentielles sur les réseaux, sur la sécurité ou la surviabilité des réseaux et sur la fiabilité des services de réseau pour assurer l'accès à l'information.

6. Il convient de s'intéresser à trois domaines : a) les politiques en matière de cryptographie, notamment les normes relatives au traitement et au contrôle des informations émanant du Gouvernement; b) les directives relatives à la protection des informations non confidentielles dans les organismes gouvernementaux; et c) les questions juridiques et la sécurité de l'information, notamment le commerce électronique, la confidentialité et la propriété intellectuelle.

7. Les mécanismes de protection des données, en particulier ceux qui reposent sur la cryptographie, prennent une importance croissante. Les mesures de protection appropriées (contre-mesures) doivent tenir compte des mutations technologiques, institutionnelles et sociales en raison desquelles la responsabilité de la protection de l'information incombe de plus en plus aux utilisateurs finals. Si l'on ne résout pas les difficultés liées aux politiques en matière de cryptographie, les initiatives plus vastes engagées pour protéger les réseaux informatiques seront compromises. Pour protéger de manière appropriée le réseau d'information d'un organisme gouvernemental ou d'une autre organisation, la mesure la plus absolument essentielle suppose que la direction définisse les objectifs généraux de l'entité en question, énonce pour celle-ci une politique de sécurité correspondant à ces objectifs, et applique cette politique. Seuls les hauts responsables peuvent renforcer le consensus et utiliser les ressources nécessaires à une protection efficace des réseaux informatiques.

8. Il s'agit là d'essayer d'évaluer les menaces et les risques liés à l'activité criminelle dans le contexte informatique et de suggérer des avis que les services de police peuvent fournir quant aux procédures de sécurité et aux méthodes de prévention des délits informatiques. Les menaces qui visent les systèmes informatiques peuvent résulter d'actes intentionnels ou non, et avoir une origine aussi bien interne qu'externe.

II. Difficultés

9. Il est préoccupant de constater que l'on n'accorde qu'une place secondaire à la préparation en matière de sécurité dans l'élaboration au niveau national d'initiatives liées au cybergouvernement.

10. Jusqu'à présent, la Police royale n'a pas été sollicitée aux fins des préparatifs liés à l'entrée dans l'ère de l'information, et n'y a pas participé. Au cours des trois années écoulées, de nombreuses lois ont été adoptées pour préparer le pays à cette

transition, et de nombreux organismes gouvernementaux et de réglementation mis en place ou sur le point de l'être lanceront les initiatives de cybergouvernement.

11. La sécurité en termes de préparation des autorités de police n'a jamais fait l'objet d'une campagne active et n'a jamais non plus eu la même priorité que d'autres questions d'intérêt national. Elle joue pourtant un rôle très important au regard des aspirations nationales à entrer dans la société de l'information.

12. La sécurité est cruciale pour l'ère de l'information, et l'on ne saurait trop insister sur l'importance d'une infrastructure sûre et fiable.

III. Initiatives prises par la Police royale du Brunéi Darussalam

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

13. La Police royale est le principal service de répression du pays : elle souhaite donc offrir son assistance dans la recherche des solutions nécessaires aux problèmes en matière de sécurité afin d'entrer véritablement dans l'ère de l'information.

14. À cette fin, de nombreux agents sont allés suivre à l'étranger une formation à la lutte contre les délits commis sur l'Internet, en particulier la cybercriminalité et la criminalité transnationale. Faute de financement, aucun progrès n'a d'abord pu être fait quant à l'acquisition du matériel et des logiciels nécessaires aux enquêtes sur les actes de piratage visant des systèmes informatiques, mais la Police royale est à présent dotée des moyens voulus pour ouvrir des enquêtes dans les affaires de cybercriminalité.

15. La Police royale a pris des mesures pour intensifier la coopération internationale dans ce domaine en participant activement à diverses rencontres sur le renforcement des capacités en matière de répression. Son système informatique est relié aux réseaux régionaux et internationaux de répression, ce qui accroît sa capacité de poursuivre les fugitifs.

IV. Propositions et recommandations

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

16. La Police royale du Brunéi Darussalam fait les propositions suivantes à titre de mesures préliminaires visant à promouvoir la sécurité dans le contexte de la protection des données d'information :

A) Signalement et suivi des menaces et points faibles

1) Depuis la constitution de l'équipe d'intervention informatique d'urgence du Brunéi Darussalam en 2004, un certain contrôle est exercé. Ce contrôle n'est toutefois pas total, du fait que l'équipe d'intervention n'est liée d'aucune manière à la Police royale et qu'il n'existe pas de mécanisme d'action rapide (surveillance ou interception d'une intrusion réelle, par exemple).

B) Éducation et mécanismes de sécurité pour une informatique sans risque

1) Il faut encourager l'élaboration de supports pédagogiques et de programmes éducatifs sur la cybercriminalité destinés à tous les utilisateurs, en vue de les initier aux pratiques et aux comportements sûrs dans le cadre de l'utilisation de l'Internet;

2) Il faut investir dans des campagnes de sensibilisation axées sur la nécessité de dispenser une formation en matière de sécurité aux administrateurs de systèmes et de réseaux et aux responsables de l'informatique;

3) Il faut faciliter la conception et le fonctionnement de mécanismes de sécurité liés à l'information circulant sur le cyberespace, ces mécanismes devant permettre à chaque partie à une transaction de décider des précautions et des restrictions applicables.

C) Recherche-développement

1) Il faut allouer des fonds à la recherche-développement dans les domaines de sécurité et de la surviabilité pour les architectures informatiques ouvertes associées à des systèmes de commande répartie;

2) Il faut mettre au point des outils permettant d'aider les administrateurs de réseaux à exploiter des systèmes sécurisés;

3) Il faut mettre au point des techniques associées à des programmes exhaustifs permettant d'identifier et d'atténuer les risques en permanence.

D) Utilisation de normes

1) Il faut instaurer des normes de sécurité applicables aux logiciels et en encourager l'adoption en tant que moyen de faire démarrer à court terme le processus de renforcement de la sécurité des produits Internet;

2) Il faut instituer une politique gouvernementale aux termes de laquelle le matériel et les logiciels acquis par le Gouvernement doivent répondre à des normes de sécurité précises incluant obligatoirement un dispositif d'alerte qui permettent de signaler au client les défaillances et la manière d'y remédier.

E) Législation et répression

1) Il faut soutenir l'action menée par les « cyberpoliciers » et allouer aux organismes de répression le financement voulu pour qu'ils disposent de la formation, des ressources matérielles et du personnel nécessaires au traitement des affaires de cybercriminalité;

2) Il faut faire en sorte que les mesures correspondent aux besoins en matière de répression en vue d'une action coordonnée à l'échelle internationale permettant d'élucider les affaires criminelles liées au cyberespace, et pour appuyer les activités des autorités de police grâce à des accords internationaux relatifs au droit de poursuite;

3) Il faut veiller à ce que les politiques publiques facilitent l'utilisation à grande échelle du chiffrement pour protéger les données d'information et les utilisateurs du cyberespace.

Burkina Faso

[Original : français]
[20 juin 2007]

1. Le Burkina Faso a affirmé très tôt sa volonté politique de développement des nouvelles technologies de l'information et de la communication considérées comme un outil stratégique de renforcement de la bonne gouvernance et du développement économique et social.

2. Dès 1996, il s'est en effet engagé dans une réflexion globale sur le développement des nouvelles technologies de l'information et de la communication. L'objectif était de mettre les technologies de l'information au service de la modernisation des services publics et d'améliorer l'efficacité de l'action de 1'administration.

3. En 1999, il s'est doté d'un plan de l'infrastructure nationale d'information et de communication 2001-2005 qui visait à favoriser la convergence des politiques nationales dans le domaine des télécommunications, de l'informatique et des médias de communication.

4. En 2004, le Gouvernement du Burkina Faso a adopté la stratégie d'opérationalisation du plan de développement de l'infrastructure nationale d'information et de communication. À travers ce plan, le Gouvernement prenait ainsi l'engagement de garantir la diffusion des technologies de l'information et de la communication dans toute la société, leur accessibilité et leur appropriation par toutes les couches sociales et la mobilisation de leur potentiel au profit des stratégies nationales de développement.

5. Mais considérant les risques issus de l'utilisation des systèmes d'information, le Gouvernement s'emploie à l'élaboration d'un cadre juridique qui vise la protection de l'information, la sécurisation du système d'information, la protection des droits fondamentaux des personnes, la mise en confiance des entreprises et des administrations.

6. Dans ce processus, la loi n°010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel a été adoptée. Elle protège les droits et libertés fondamentaux des individus, leur intimité dans le cadre des traitements informatisés ou non des informations contenant des données à caractère personnel. En application de cette loi, il a été créé par décret 2007-283/PRES/PM/MPDH du 18 mai 2007, une commission de l'informatique et des libertés. Cette commission est une autorité administrative indépendante chargée de veiller à ce que les traitements automatisés publics et privés d'informations nominatives soient effectués conformément à la loi. Disposant d'un pouvoir réglementaire et de sanction, elle intervient en amont et en aval de la mise en œuvre des traitements par ses avis et déclarations préalables et par son contrôle et ses sanctions.

7. Enfin, des organes de régulation ont été mis en place afin de répondre aux besoins sécuritaires de la société de l'information. Il en est ainsi du Conseil supérieur de l'information, de la Direction générale chargée de la coordination des programmes de développement des technologies de l'information et de la communication logée au niveau du Ministère des postes et des technologies de l'information et de la télécommunication.

8. Face cependant à une société de l'information qui n'admet pas de frontière, le Burkina Faso estime que la coopération internationale est fondamentale dans la problématique de la sécurisation des systèmes d'information. Au-delà de la fracture numérique, les pays du sud sont, en matière de sécurité, exposés au même titre que les pays du nord. La collaboration entre les pays est en conséquence capitale si l'on veut assurer la sécurité des États, des institutions, des entreprises et des individus comme des réseaux et des systèmes d'information. La lutte contre la cybercriminalité ne peut être efficace que par une coopération internationale renforcée.

9. Le Burkina Faso se félicite de l'intérêt porté par l'Organisation des Nations Unies à la question de la sécurité de l'information et estime qu'il est maintenant opportun d'œuvrer à l'élaboration d'un instrument international sur la sécurité informatique d'une part et sur la protection des données à caractère personnel d'autre part. En tout état de cause, les progrès de l'informatique, de la télématique et les questions de la sécurité internationale devront être envisagés sous le prisme des droits humains pour éviter de tomber dans une société mondiale de surveillance dominée par le réflexe déshumanisant du tout sécuritaire.

Chili

[Original : espagnol]
[13 juin 2007]

1. Le Chili attache une grande importance à la sécurité de l'information dans le contexte de la sécurité internationale. Il partage la préoccupation de la communauté internationale quant au fait que l'informatique 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, et considère qu'il est nécessaire d'empêcher l'utilisation de l'informatique à des fins délictueuses.

2. Sur le plan législatif, des avancées ont été réalisées quant à l'adoption de diverses lois et règlements relatifs à la sécurité et à la confidentialité des documents électroniques et à l'efficacité des communications entre les organismes de l'administration publique et entre ces organismes et les citoyens.

3. Compte tenu de l'importance de cette question, le Chili a participé activement aux travaux des deux phases du Sommet mondial sur la société de l'information, à Genève en décembre 2003 et à Tunis en novembre 2005.

Chine

[Original : chinois]
[15 mai 2007]

Les progrès fulgurants et l'utilisation généralisée des technologies de l'information contribuent aujourd'hui dans tous les pays à promouvoir le développement économique et social et à améliorer le bien-être de la population. Dans le même temps, la question de la sécurité de l'information est devenue un facteur important qui a des incidences sur la sécurité nationale, voire sur la sécurité et la stabilité de toute la planète. Trouver une solution appropriée à ce problème,

dans l'intérêt commun de tous les pays, est un devoir qui incombe à l'ensemble de la communauté internationale.

La Chine considère que la question de la sécurité de l'information n'a pas seulement trait à un risque lié à la faiblesse des équipements et à leur interconnexion, mais qu'elle englobe aussi les problèmes politiques, économiques, militaires, sociaux ou culturels qui résultent d'une utilisation abusive des technologies de l'information. Il importe de prêter sérieusement attention à ces deux enjeux.

De l'avis de la Chine, l'utilisation des technologies de l'information doit être conforme aux dispositions de la Charte des Nations Unies et aux règles régissant les relations internationales. La libre circulation de l'information doit être assurée dans le respect de la souveraineté et de la sécurité de chaque pays et dans le respect de sa législation, ainsi que de son histoire, de sa culture et de son régime politique particuliers. Tout pays a le droit d'administrer son cyberespace conformément à son droit interne. Étant donné les disparités entre pays en matière de développement des télécommunications, la communauté internationale se doit d'intensifier la coopération dans les domaines de la recherche sur les technologies de l'information et de l'utilisation de ces technologies, afin que chaque pays puisse avoir librement accès à ces technologies.

Le Gouvernement chinois, qui attache depuis toujours une grande importance à la question de la sécurité de l'information, a défini et met progressivement en œuvre une stratégie nationale en vue de garantir cette sécurité, a élaboré à cette même fin toute une série de lois, de règlements et de normes, et a déployé des efforts considérables pour améliorer la surveillance des incidents sur les réseaux, intensifier la coordination des mécanismes de répression, promouvoir la recherche sur les techniques de sécurisation des réseaux et mettre sur pied un système de réponse rapide aux situations d'urgence. Sa capacité de protéger la sécurité de l'infrastructure de l'information et des principaux systèmes d'information ne cesse de s'accroître.

La Chine prend une part active à la coopération internationale dans le domaine de la sécurité de l'information. En juin 2006, les signataires de la Déclaration des chefs des États membres de l'Organisation de Shanghai pour la coopération sur la sécurité de l'information ont décidé de créer un groupe international d'experts de la sécurité de l'information, aux travaux duquel la Chine a participé dans un esprit constructif.

L'Organisation des Nations Unies constitue aux yeux de la Chine l'enceinte appropriée pour discuter des solutions possibles à la question de la sécurité de l'information. En 2004 et 2005, un groupe d'experts gouvernementaux sur la sécurité de l'information s'était penché sur les différents aspects de cette question et avait formulé bon nombre de propositions utiles, jetant ainsi les bases d'une plus ample réflexion par la communauté internationale. La Chine est favorable à la création en 2009 au sein de l'ONU d'un nouveau groupe d'experts gouvernementaux en vue de procéder à un examen général et approfondi des risques et des défis qui se présentent dans le domaine de la sécurité de l'information et de réfléchir à une stratégie permettant d'y faire face. Comme par le passé, la Chine soutiendra les efforts de la communauté internationale pour résoudre la question de la sécurité de l'information et y participera activement.

Cuba

[Original : espagnol]
[16 mai 2007]

1. Les résultats que Cuba peut avancer dans le domaine de l'informatique et des télécommunications ont pour l'heure un caractère foncièrement social, sont étrangers à toute volonté de consumérisme et sont axés sur la formation de spécialistes d'un genre nouveau, pleinement engagés et attachés à des valeurs éthiques opposées à celles des modèles que promeut l'économie mondialisée et néolibérale.

2. Les améliorations substantielles de l'infrastructure technologique ou la formation massive et approfondie dispensée à ceux qui constituent le capital humain, dès leur plus jeune âge, sont des exemples des efforts énormes déployés par l'État cubain pour accélérer l'informatisation de la société, en tant que moyen d'améliorer la qualité de vie des Cubains et l'efficacité et la compétitivité du pays.

3. Sur la base de cette politique, Cuba a organisé l'utilisation rationnelle et efficiente des ressources informatiques, qu'il s'agisse de l'équipement ou de la connectabilité, dans une perspective largement sociale. Des secteurs clefs sont privilégiés, comme la santé, l'éducation, les centres de recherche scientifique, les instituts culturels et les entreprises, garants du développement économique et social de la nation.

4. Cependant, ce développement s'est heurté à un blocus économique, commercial et financier cruel et prolongé décidé par les États-Unis d'Amérique, dont l'administration actuelle a multiplié les mesures à cet égard.

5. Cuba est reliée à l'Internet depuis 1996, date à laquelle le Gouvernement américain l'a autorisée à y accéder. En réalité pourtant, des câbles internationaux à fibre optique sont posés tout près des côtes cubaines, mais les lois relatives au blocus ont empêché Cuba de s'y raccorder, et la nation est obligée d'avoir recours à un satellite d'une capacité d'à peine 65 mégabits par seconde à la sortie et 124 à l'entrée. Le raccordement aux câbles à fibre optique permettrait non seulement d'accéder plus rapidement à Internet, mais encore de faire des économies substantielles. Les lois disposent que tout ajout ou modification au canal de communication satellite exige l'obtention d'une licence auprès du Département du Trésor des États-Unis.

6. S'agissant de l'infrastructure technologique, le blocus imposé à Cuba par les États-Unis n'empêche pas seulement le pays d'acquérir du matériel et des programmes informatiques auprès de compagnies américaines : en raison de son application extraterritoriale, il vise aussi les activités commerciales avec les entreprises d'autres pays, et empêche le téléchargement de logiciels et d'informations, y compris lorsqu'ils sont gratuits, si le numéro de protocole Internet est associé à Cuba.

7. Internet étant un domaine mondial commun, de grands défis y sont associés : non seulement la gestion par l'humanité tout entière, impliquant la participation de tous les pays à son administration, mais encore l'élimination de fléaux universellement condamnés, comme la diffusion de la pornographie, l'incitation au terrorisme, le racisme, la fraude, la divulgation d'idéologies fascistes et toute manifestation de la cybercriminalité.

8. Mais l'autre grand défi à relever, que les pays riches passent sous silence, est l'élimination de son caractère sélectif et élitiste, qui transpose aujourd'hui dans l'espace cybernétique les inégalités et les barrières du monde réel, créant ainsi un « fossé numérique ».

9. Des millions de personnes dans le monde sont loin de devenir des « internautes » pour la bonne raison qu'elles ne savent ni lire ni écrire et que leur souci majeur est de survivre à la faim, à la soif et à la maladie. La volonté politique des gouvernements, la coopération internationale et un minimum de ressources, prélevées sur celles que le monde dit développé gaspille aujourd'hui dans la publicité, la surconsommation et la course à l'armement, permettraient à Internet de devenir l'instrument d'une révolution culturelle et éducative qui promouvrait le savoir, préconiserait l'éducation, la culture, la coopération et la solidarité en même temps que les valeurs éthiques et morales dont notre nouveau siècle a besoin, prônerait les sentiments humains les plus nobles et écarterait les comportements inhumains, égoïstes et individualistes.

10. Par ailleurs, les organismes de sécurité prêtent une attention particulière à cette question, et la majorité d'entre eux se font les conseillers du Gouvernement. Dotés de fonds considérables, ils ont mis au point divers moyens et programmes afin d'étayer les technologies existantes ou de créer de nouvelles possibilités d'accès aux communications, aux systèmes et aux bases de données, ainsi qu'aux systèmes d'identification et de surveillance des véhicules et des personnes. Ces réseaux complexes incluent des systèmes d'antennes, des stations d'écoute, des radars et des satellites, et sont appuyés par des sous-marins et des avions-espions, tous reliés à des superordinateurs et à des applications spéciales.

11. Il serait naïf de penser que les sociétés prestataires de services et de technologies, dans le cadre de leur collaboration avec les organismes susmentionnés, ne fournissent pas des informations propices à leurs activités en matière de renseignement et d'espionnage. Conformément aux dispositions du *Patriot Act* adopté par les États-Unis, le Gouvernement américain est habilité à exiger de toute entreprise qu'elle lui communique des informations, qu'elles aient un caractère secret ou non, s'il estime qu'elles intéressent la sécurité nationale.

12. La connaissance est le patrimoine de l'humanité tout entière : il faut donc démocratiser le capital d'information et sa distribution et le mettre au service de la paix et du développement, qui sont indispensables à la poursuite du progrès dans le nouveau millénaire.

Liban

Les lettres ci-après ont été reçues de la Mission permanente du Liban auprès de l'Organisation des Nations Unies et représentent des communications échangées par la Mission et les Ministères libanais des télécommunications, de l'intérieur et de la défense.

Ministère des télécommunications

[Original : anglais]
[4 juin 2007]

1. Nous sommes en train d'adopter une nouvelle loi concernant les technologies de l'information et des communications qui est en dernière phase d'approbation par la Chambre des députés. Cette loi portera notamment sur la sécurité et sur toutes les questions relatives à la criminalité informatique.

2. Une fois que la loi susmentionnée sera entrée en vigueur, le Ministère des télécommunications se penchera sur les questions b), c) et d) avec les autres ministères et les administrations compétents.

Ministère de l'intérieur

[Original : arabe]
[23 mai 2007]

1. Sur le plan national

L'échange d'informations entre les divers secteurs des Forces de sécurité intérieure s'effectue à l'aide des moyens de télécommunication (téléphone, fax et centres d'opérations dans les différentes régions). Ces moyens continuent de faire l'objet de violations telles que l'interception des communications ou l'écoute téléphonique, sachant que la Direction générale a depuis quelque temps commencé à élargir le réseau TETRA adopté au sein des Forces de sécurité intérieure, en l'utilisant dans certaines régions libanaises avant de l'étendre à tout le pays. Les Forces de sécurité ont en outre été équipées récemment d'un réseau de lignes cellulaires fermées, conformément à la décision n° 47 du 15 septembre 2006 du Conseil des ministres.

2. Sur le plan international

L'échange d'informations, sécuritaires notamment, entre les Forces de sécurité intérieure et les divers organismes internationaux s'effectue par l'intermédiaire de la Division des communications internationales à la Direction générale des Forces de sécurité intérieure qui comporte une station d'émission et de réception des données sécuritaires par l'intermédiaire du bureau d'Interpol à Beyrouth qui relève de cette division. On y utilise actuellement un système de communications régulières dont le fonctionnement est basé sur la technologie de l'Internet et qui se caractérise par la vitesse de circulation des informations et par la capacité de protéger la confidentialité grâce à des réseaux spécialisés qui en assurent l'entretien en accord avec l'Organisation internationale de police criminelle (Interpol) chargée de surveiller la gestion et l'amélioration du système.

3.

- S'agissant de la question a) relative aux problèmes généraux en matière de sécurité de l'information A/C.1/61/L.35, les Forces de sécurité intérieure s'efforcent d'utiliser les moyens techniques efficaces en matière de sécurité de l'information et des télécommunications. De nombreux défis sont à relever dans ce domaine, le plus important étant la normalisation de la structure sécuritaire et de l'environnement protecteur des données en fonction de

critères convenables et satisfaisants en vue de mettre en place, appliquer et renforcer la gestion des systèmes d'information en matière de sécurité ainsi que contrôler ces systèmes.

- S'agissant des questions b) et c) concernant les efforts engagés au niveau national pour renforcer la sécurité de l'information et les activités de coopération internationale menées dans ce domaine, nous avons eu des expériences concrètes et réalistes en matière d'évaluation des risques d'intrusion en fonction de l'état du réseau informatique dont nous disposons. Nous avons réalisé des progrès dans l'amélioration des conditions de sécurité de notre réseau de données en nous appuyant sur les nouvelles techniques et sur les solutions et mesures d'application établies dans les domaines de la protection des systèmes, de l'évaluation de leur immunité face aux intrusions et aux virus, de l'adoption de plans permettant la poursuite du travail en cas d'attaque des systèmes et de la formation de personnel compétent pouvant intervenir chaque fois qu'il y a urgence.

- S'agissant de la question d) relative aux mesures qui pourraient être prises par la communauté internationale pour renforcer la sécurité de l'information à l'échelon mondial, nous proposons d'abord d'adopter une politique préventive pour faire cesser les activités d'intrusion individuelle et de coopérer à l'échelle internationale dans ce domaine; d'élaborer ensuite une loi relative à la lutte contre les actes de sabotage et d'intrusion visant les réseaux informatiques, et d'ériger ces actes en infractions passibles de sanctions; et enfin d'échanger des données d'expérience entre États Membres et d'en profiter pour réaliser des progrès qualitatifs dans ce domaine.

À cet égard, il convient de préciser que la Direction générale a pris les mesures suivantes sur ce plan :

a) Elle a créé un bureau consacré à la lutte contre la criminalité informatique au sein de la Direction de la sécurité intérieure dont les tâches principales consistent notamment à signaler les délits informatiques et les dangers qui menacent la sécurité des données numériques, à mener les enquêtes et à poursuivre les coupables de tels délits;

b) Les forces de sécurité ont participé (par le biais d'un certain nombre d'officiers spécialisés) aux travaux d'élaboration d'un projet de loi sur la lutte contre la criminalité informatique avec la Commission parlementaire de la technologie. Le projet de loi attend d'être approuvé par le Parlement;

c) Les Forces de sécurité participent aux activités de l'Organisation internationale de police criminelle (Interpol) et contribuent aux travaux du comité régional d'Interpol pour le Moyen-Orient et l'Afrique du Nord chargé de la lutte contre la criminalité informatique, le Vice-Président et un des membres du Comité étant des officiers des Forces de sécurité intérieure spécialisés dans l'informatique. Par ailleurs, le chef du bureau de la lutte contre la criminalité informatique assure la liaison avec Interpol en ce qui concerne les questions relatives à la sécurité des informations et à la lutte contre la criminalité informatique, notamment lorsqu'elle touche la sécurité des informations.

Compte tenu des dangers qui menacent, aux plans national et international, la sécurité en général et celle des systèmes d'information et de communication en particulier, il importe d'élaborer une stratégie tournée vers l'avenir qui prenne en

considération les progrès techniques pour protéger les informations et trouver les moyens de lutter contre toute violation. À ce propos, il convient de noter ce qui suit :

1. La dynamique des informations et les critères de sécurité

Les moyens de transfert et de conservation des données évoluent de façon considérable grâce aux progrès technologiques, mais les difficultés que pose le contrôle des systèmes, des instruments et des contenus ont nécessité l'application de mesures de protection à tous les niveaux. Des normes internationales ont été élaborées pour la gestion de la sécurité de l'information (ISO17799).

2. Le Liban et la sécurité des informations

Le Liban manque de nombreux moyens sur les plans législatif et exécutif pour assurer un environnement protecteur des informations. Il n'existe aucune loi ou procédure administrative qui oblige les administrations et institutions publiques à appliquer les normes (ISO17799), mais certaines instructions semblables aux normes internationales sont appliquées par la Banque centrale et quelques banques privées. Il n'existe pas non plus de législation concernant les principes de base du codage des réseaux de communication privés.

La question de l'application

La circulaire n° 4/2 du 19 décembre 2005 du Ministère des télécommunications sur la conservation des dossiers relatifs à la circulation des données n'est pas respectée. Il n'existe aucune législation qui réglemente le travail des cybercafés et le contrôle des communications par satellite n'est pas efficace.

Il faut noter à ce propos que les États-Unis d'Amérique, à la suite des attentats terroristes du 11 septembre, ont créé le Département de la sécurité intérieure et adopté un système de contrôle de tous les réseaux d'un bout à l'autre du pays qui assure l'analyse et la surveillance. Ils ont aussi élaboré des lois strictes en matière de codage des données et d'entrée et de sortie des réseaux.

3. Moyens de lutte et de prévention

Il s'est avéré que le cyberespace, en tant que réseau géré suivant le Protocole de communication TCP/IP, étant un milieu fragile et peu sûr que les groupes criminels ont pu agresser et parfois même détruire, en raison du fait que la priorité était donnée aux objectifs de vente et de commercialisation. Par ailleurs, la cybercriminalité s'est caractérisée par la vitesse et l'absence de contrôles et de limites alors que les mesures de lutte sont lentes, la coordination inexistante et les lois adoptées insuffisantes.

De nombreuses améliorations ont été apportées au fonctionnement des protocoles d'Internet en ce qui concerne à la fois les utilisateurs et le codage (le protocole IPv6 notamment) et des recherches sérieuses sont menées pour mettre au point des techniques de sécurité des réseaux informatiques à même de combattre les actes d'intrusion et de destruction.

Les accords internationaux pour la lutte contre la cybercriminalité, notamment la Convention de Budapest, ont prévu une coopération rapide entre les États et entraîné :

– La création d'un réseau de communications (7/24) parallèle au réseau Interpol et spécialisé dans la criminalité informatique;

– La constitution d'un comité permanent et de groupes de travail régionaux pour stimuler la coopération technique et améliorer les compétences dans les bureaux de lutte contre la criminalité informatique.

Il semble toutefois que cette Convention n'a pas pu assurer une lutte rapide et immédiate contre les virus qui peuvent être lancés sur le réseau.

4. Propositions

- Appliquer et améliorer les législations relatives à la sécurité des informations et appliquer les normes de protection de la sécurité des informations;
- Relancer et améliorer les mesures de sécurité dans les divers services compétents afin de protéger les moyens et les systèmes d'information;
- Faire fonctionner les services spécialisés au sein du Ministère des télécommunications et les mettre en rapport avec les services et les institutions publics et privés dans le but de trouver un environnement sûr pour les systèmes informatiques;
- Suivre les progrès réalisés dans le monde en ce qui concerne notamment l'application de protocoles d'Internet tels qu'IPv6 et utiliser les moyens techniques nécessaires pour connaître l'identité de toute personne qui pénètre dans le réseau d'Internet et adopter le système d'identité numérique (certificat numérique);
- Renforcer la coordination entre les services de protection du droit dans le domaine de la sécurité des informations, établir des normes internationales unifiées sur le plan technique afin de faciliter le suivi, le contrôle et la coordination et uniformiser autant que possible les systèmes législatifs pour préserver la sécurité nationale en se conformant aux exigences de la sécurité internationale.

La Direction générale de la sûreté publique signale que ses communications relatives à la sécurité s'effectuent à l'intérieur du territoire libanais et qu'il n'y a pas de communications extérieures. En ce qui concerne les communications intérieures, les systèmes de protection sont en train d'être améliorés avec l'aide des compétences de certains organismes de sécurité amis. Toutefois, les équipements nécessaires ne sont pas encore en place à cause du manque de moyens tant financiers que techniques.

Ministère de la défense nationale

[Original : arabe]
[1er mai 2007]

Le Ministère de la défense nationale communique ce qui suit :

– Le Liban s'engage à ne pas utiliser la technologie informatique et les moyens de télécommunications à des fins incompatibles avec les notions de stabilité et de sécurité internationales;

– Le Liban prend les mesures nécessaires au plan national (amélioration et modernisation des systèmes et législations pertinents) pour renforcer la sécurité des informations et encourage l'échange des données disponibles entre les parties concernées;

– Le Liban respecte les résolutions des Nations Unies visant à protéger la sécurité et la confidentialité des informations et à empêcher leur utilisation abusive, de quelque manière que ce soit, et à interdire l'usage de sources ou de technologies informatiques à des fins criminelles ou terroristes.

Mexique

[Original : espagnol]
[22 mai 2007]

1. Le Mexique a appuyé la résolution sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale, présentée à l'Assemblée générale par la Fédération de Russie, et estime qu'il est très important de multiplier les échanges de points de vue sur cette question et les notions connexes. Il conviendrait de s'inspirer des travaux de la Première Commission, ou d'autres instances qui s'occupent du désarmement, en vue de la présentation d'exposés par des experts, ou de débats sur la question organisés en parallèle.

2. Le bon fonctionnement de la plupart des mécanismes de vérification internationale fondés sur des instruments juridiques internationaux ou des accords politiques relatifs au contrôle des exportations dépend des moyens d'information et de télécommunication; il est donc de première importance de s'intéresser à l'état d'avancement des progrès réalisés à cet égard. D'autre part, la mise au point de systèmes de missiles balistiques et la modernisation des arsenaux nucléaires supposent des avancées dans les domaines informatique et télématique qui sont nécessairement déjà une réalité. Les progrès en matière de technologies liées à l'espace extra-atmosphérique et aux satellites sont sans aucun doute liés à la sécurité internationale.

3. Le Mexique n'a cessé de rappeler, dans le cadre de la Conférence du désarmement, qu'il fallait d'urgence adopter un programme de travail dont l'un des thèmes principaux soit la prévention d'une course aux armements dans l'espace, en raison de son lien avec la vulnérabilité des technologies de l'information et des communications (TIC) utilisées dans l'espace.

4. Le Mexique juge importante la poursuite des travaux du Groupe d'experts gouvernementaux sur la question créé en application de la résolution 58/32, qui se réunira à nouveau en 2009. Il considère par conséquent qu'il faudrait encourager un large débat avant cette date.