Nations Unies A/59/116

Assemblée générale

Distr. générale
23 juin 2004
Français
Original: anglais, arabe, chinois et espagnol

Cinquante-neuvième session
Point 62 de la liste préliminaire*
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/59/50 et Corr.1.

04-40705 (F) 150704 220704

I. Introduction

1. Au paragraphe 3 de sa résolution 58/32 du 8 décembre 2003, consacrée 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 questions suivantes : 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; c) la teneur des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux. Au paragraphe 4, 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, de procéder à une étude, avec l'assistance d'un groupe d'experts gouvernementaux qu'il constituera en 2004, les experts étant 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 le résultat de cette étude. Le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale a commencé ses travaux le 12 juillet 2004.

2. Dans une note verbale datée du 18 février 2004, 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

Argentine

[*Original : espagnol*]
[*14 mai 2004*]

Situation actuelle

1. L'Argentine a accompli des progrès considérables dans les domaines relatifs à la protection et à la confidentialité des données. La loi n° 25326 sur la protection des données personnelles est l'une des plus progressistes au monde et son exécution est confiée à une direction tout spécialement créée par le Ministère de la justice. Le Congrès de la Nation a par ailleurs bien avancé l'examen de plusieurs projets de loi sur les délits informatiques.

2. L'Argentine a également progressé sur les questions relatives à la signature électronique et s'est attachée à définir la validité juridique des documents électroniques et à arrêter les mécanismes de sécurité applicables en la matière, l'objectif étant de garantir l'authenticité et l'intégrité des documents. Elle a joué un rôle de chef de file en la matière et elle met actuellement la dernière main au projet d'infrastructure nationale de clefs publiques.

3. L'Argentine a réalisé des progrès notables en matière de sécurité informatique. À cet égard, l'Office national des technologies informatiques a la responsabilité principale de suivre et de superviser tous les aspects ayant trait à la protection et à la confidentialité des données numériques et électroniques du secteur public national et d'apporter son concours en la matière.

4. L'Office comprend une cellule de coordination en cas de catastrophes dans les réseaux télématiques de l'administration publique nationale, qui est chargée de résoudre les incidents et de renforcer les dispositifs de sécurité dans le secteur public. La cellule passe au crible les incidents portés à sa connaissance, publie des bulletins d'alerte préventifs et correctifs, met au point des dispositifs de sécurité, propose des stages de formation aux agents et fonctionnaires de l'État et établit des politiques de sécurité types.

Évaluation globale des problèmes

5. Les problèmes qui se posent en matière de sécurité informatique sont nombreux et de plus en plus complexes du fait des progrès techniques.

6. Les principaux problèmes se divisent en trois catégories :

– Attaques contre les données;

– Usage illicite des moyens informatiques;

– Délits cybernétiques.

7. Les progrès techniques sont tels qu'il est de plus en plus difficile de protéger la confidentialité et l'intégrité des données et d'en assurer la disponibilité. Il faut distinguer deux grandes catégories de données : les données personnelles qui doivent être traitées avec la plus grande réserve afin de préserver la vie privée des intéressés et les données relatives aux organisations (données commerciales ou industrielles, données appartenant à des organismes publics) dont la diffusion, la modification ou la perte pourraient porter atteinte à des objectifs économiques, sociaux, politiques, etc.

8. Un autre problème qui est fréquemment sous-estimé est celui de l'usage illicite des moyens informatiques. On entend par là une utilisation à des fins autres que celles qui sont autorisées ou une utilisation abusive qui entraîne un gaspillage de ressources. Par exemple, la propagation massive de virus et les autres types d'intrusions par l'intermédiaire de l'Internet et les mesures à prendre pour parer aux dangers posés entraînent des coûts supplémentaires très supérieurs à ceux prévus à l'origine pour le fonctionnement des systèmes informatiques. Des mesures préventives permettraient de faire des économies importantes.

9. Les nouvelles technologies offrent de nouvelles possibilités pour commettre des délits, qu'il s'agisse de délits classiques ou de variantes découlant des progrès techniques.

Chine

[*Original : chinois*]
[*24 mai 2004*]

Point de vue de la Chine sur les questions relatives à la sécurité de l'information

1. Les découvertes scientifiques et techniques doivent beaucoup aux progrès rapides accomplis dans les domaines de l'informatique et de la télématique. Compte tenu de la nouvelle donne, de la multiplication des menaces pesant sur la sécurité, de l'apparition de nouvelles menaces et des activités terroristes internationales, la sécurité informatique s'impose comme une question de plus en plus importante dans le contexte de la sécurité internationale. La Chine appuie les initiatives internationales visant à assurer et à promouvoir la sécurité informatique dans tous les pays et soutient le Groupe d'experts gouvernementaux chargé de la question.

2. La Chine est d'avis que les technologies de l'information doivent être utilisées dans le respect des principes énoncés dans la Charte des Nations Unies et des autres principes reconnus sur le plan international et servir à garantir et à promouvoir la paix, la stabilité et le développement aux échelons international et régional. Au vu des nouvelles menaces qui pèsent désormais sur la sécurité, les pays devraient s'intéresser de près à la cybercriminalité et au cyberterrorisme. La communauté internationale devrait également renforcer la coopération dans les domaines de la recherche et de l'utilisation de l'informatique du fait que tous les pays n'en sont pas au même point en la matière.

3. La Chine estime que toutes les parties devraient examiner les menaces existantes et potentielles en matière de sécurité informatique et réfléchir à des solutions pratiques dans le cadre du Groupe d'experts gouvernementaux. Elle s'associera activement aux travaux du Groupe et espère que celui-ci obtiendra des résultats concrets.

Costa Rica

[*Original : espagnol*]
[*15 mars 2004*]

1. L'Assemblée législative a approuvé le 24 octobre 2001 une loi portant modification du Code pénal, qui était intitulée « Ajout des articles 196 *bis*, 217 *bis* et 229 *bis* à la loi n° 4573 du Code pénal en vue de réprimer les délits informatiques ». Il s'agit là de la réforme la plus importante entreprise ces dernières années par le Costa Rica dans le domaine de la sécurité informatique.

2. La réforme vise trois délits informatiques – la violation des communications électroniques, les fraudes informatiques, et l'altération des données et le sabotage informatique – et répond aux besoins actuels en matière de sécurité informatique.

On trouvera ci-après le texte de loi dans son intégralité.

Appendice

Ajout des articles 196 *bis*, 217 *bis* et 229 *bis* à la loi n° 4573 du Code pénal en vue de réprimer les délits informatiques

8148

L'Assemblée législative de la République du Costa Rica

Promulgue ce qui suit :

Ajout des articles 196 *bis*, 217 *bis* et 229 *bis* à la loi n° 4573 du Code pénal en vue de réprimer les délits informatiques

Article unique – Sont ajoutés à la loi n° 4573 du Code pénal, en date du 4 mai 1970, les articles 196 *bis*, 217 bis et 229 *bis* dont le texte est ainsi libellé :

Article 196 *bis* – Violation des communications électroniques

Est puni d'une peine d'emprisonnement d'une durée comprise entre six mois et deux ans quiconque s'approprie, se procure, modifie, altère, supprime, intercepte, utilise, diffuse ou détourne des messages, des données ou des images copiés sur des supports électroniques, informatiques, magnétiques et télématiques ou y porte atteinte sans le contentement de l'intéressé afin de prendre connaissance de données personnelles appartenant à autrui ou de violer l'intimité d'autrui. La peine d'emprisonnement est comprise entre un an et trois ans si les actes susvisés sont commis par des personnes chargées de la garde des supports électroniques, informatiques, magnétiques et télématiques.

Article 217 *bis* – Fraude informatique

Est puni d'une peine d'emprisonnement d'une durée comprise entre un et dix ans quiconque modifie le traitement des données ou les résultats issus d'un système informatique au moyen de programmes informatiques, de données erronées ou incomplètes, de l'usage non autorisé de données ou de toute autre action qui a une incidence sur le traitement des données dudit système afin d'obtenir un bénéfice patrimonial pour son propre compte ou pour celui d'un tiers.

Article 229 *bis* – Altération des données et sabotage informatique

Est puni d'une peine d'emprisonnement d'une durée comprise entre un et quatre ans quiconque efface, supprime, modifie ou rend inutilisables sans y être autorisé et par quelque moyen que ce soit des données enregistrées sur un ordinateur.

Si un programme informatique, une base de données ou un système informatique est rendu inutilisable à l'issue des actes susmentionnés, la peine d'emprisonnement encourue est comprise entre trois et six ans. Si le programme informatique, la base de données ou le système informatique contiennent des données à caractère public, la peine d'emprisonnement encourue est portée à huit ans.

Cuba

[*Original : espagnol*]
[*1er juin 2004*]

Vues de la République de Cuba présentées comme suite à la demande figurant au paragraphe 3 de la résolution 58/32 intitulée « Progrès de la téléinformatique dans le contexte de la sécurité internationale »

1. Au paragraphe 3 de sa résolution 58/32, en date du 8 décembre 2003, 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 questions suivantes : 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; c) la teneur des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux.

2. Selon Cuba, l'utilisation malintentionnée de la téléinformatique avec pour objectif déclaré ou non de porter atteinte à l'ordre juridique et politique des pays constitue une violation des principes reconnus en la matière sur le plan international, qui est de nature à susciter des tensions et des situations qui vont à l'encontre de la paix et de la sécurité internationales. Il s'agit d'un exemple négatif et irresponsable de l'usage qui peut être fait de ces moyens, et d'une violation flagrante des principes énoncés dans la Charte des Nations Unies.

3. Au huitième alinéa du préambule de la résolution 58/32, l'Assemblée générale s'est déclarée une nouvelle fois préoccupée par le fait que la téléinformatique risquait 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 civils que militaires. Cuba partage pleinement cette préoccupation.

4. Les systèmes informatiques et télématiques peuvent se convertir en armes dès lors qu'ils sont conçus ou utilisés pour porter atteinte à l'infrastructure d'un État.

5. Cuba réaffirme que tous les pays doivent respecter les instruments internationaux applicables en la matière. L'accès aux systèmes informatiques et télématiques d'un autre État ne peut se faire que dans le respect des accords de coopération internationaux et avec le consentement de l'État concerné. Les modalités et la nature des échanges doivent être conformes à la législation de l'État dans lequel se trouvent les systèmes.

6. Les attaques menées par un État contre les systèmes informatiques et télématiques d'autres pays peuvent porter atteinte à la sécurité et à la paix internationales. Malheureusement, on constate que certains ont recours à pareils procédés pour poursuivre des visées hostiles.

7. Cela fait presque 20 ans que Cuba est la cible d'agressions encouragées, autorisées et exécutées par le Gouvernement américain. Depuis 1985 et 1990, dates auxquelles le Gouvernement américain a commencé à transmettre en toute illégalité

une émission radiophonique et une émission télévisée, les émissions de radio et de télévision cubaines sont victimes de brouillages et de dysfonctionnements.

8. Chaque semaine, les États-Unis émettent 2 227 heures et demi d'émissions radiophoniques et télévisées en direction de Cuba, qui véhiculent des messages subversifs contre l'ordre constitutionnel. Ils se servent à cette fin de 18 émetteurs de radio (à ondes courtes et moyennes et à modulation de fréquence) et de télévision qui émettent sur 29 fréquences.

9. Au total, ce sont entre 312 et 315 heures d'émissions quotidiennes qui sont consacrées à une programmation politiquement fallacieuse qui est en contradiction avec la libre circulation des informations et des idées puisqu'elle sert à transmettre des accusations mensongères, des allégations fabriquées de toutes pièces et des messages visant à ébranler l'ordre constitutionnel du pays.

10. Quinze des 18 émetteurs utilisés dans le cadre de l'agression radiophonique et télévisée contre Cuba appartiennent à des organisations liées ou appartenant à des éléments terroristes qui résident, opèrent ou agissent en territoire nord-américain, avec le consentement de l'administration fédérale des États-Unis.

11. Douze de ces émetteurs sont tout particulièrement dirigés contre Cuba, y compris la bien mal nommée télévision et radio Martí, propriété d'un Gouvernement américain qui consacre annuellement 35 millions de dollars à la guerre radio-électronique contre Cuba.

12. N'en étant plus à une provocation près, le Gouvernement américain a annoncé en mai 2004 qu'il déploierait un avion de type EC-130 Comando Solo et qu'il consacrerait des fonds supplémentaires à l'achat et à la transformation d'un avion à partir duquel il relaierait les émissions de la télévision et de la radio Martí.

13. La réalité de notre pays est déformée dans les programmes émis en toute illégalité à destination de Cuba. On y encourage nos concitoyens à émigrer illégalement au péril de leur vie, on y appelle à la désobéissance civile, on y incite à commettre des actes de violence et des actes terroristes et à renverser l'ordre institutionnel et juridique établi par la Constitution de la République de Cuba plébiscitée par plus de 96 % de la population.

14. Le fait de se servir de l'information afin de porter atteinte en toute connaissance de cause à l'ordre d'un État, de violer sa souveraineté et de s'ingérer dans ses affaires intérieures est illégal au plan du droit international et va à l'encontre du droit à l'autodétermination des peuples.

15. Les émissions susmentionnées constituent non seulement une atteinte à la souveraineté de Cuba mais également une violation flagrante des règlements établis par le Comité international d'enregistrement des fréquences de l'Union internationale des télécommunications, en particulier de l'article 23.3 de son règlement des télécommunications internationales, qui interdit les émissions au-delà des limites du territoire national, et représentent donc une violation du droit international.

16. Ces émissions violent aussi le préambule de la Constitution de l'Union internationale des télécommunications, puisqu'il s'agit d'activités qui font obstacle aux relations pacifiques et à la coopération entre les peuples ainsi qu'au développement économique et social par le bon fonctionnement des télécommunications.

17. Cuba estime nécessaire d'appeler une nouvelle fois l'attention sur les aspects suivants, qui sont étroitement liés au renforcement des télécommunications en tant qu'instrument de consolidation de la paix et de la sécurité internationales :

a) Tous les États doivent s'abstenir de prendre unilatéralement des mesures de cœrcition contraires au droit international, qui imposent à l'État visé des restrictions en matière d'accès aux technologies et aux réseaux internationaux de communication et d'échange d'informations;

b) 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;

c) 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;

d) Il faut adopter sans tarder des mesures législatives et autres, aux niveaux national et international, en vue d'interdire la concentration entre les mains d'intérêts privés de la propriété et du contrôle des moyens de télécommunication – ainsi que d'autres moyens d'information et de communication – étant donné 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;

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

f) 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 atteintes à la souveraineté et à la sécurité de nombreux États et aux atteintes à la vie privée des particuliers que commettent les systèmes mondiaux d'espionnage mis au point par certaines puissances industrielles, en particulier les États-Unis;

g) Il faut encourager l'adoption de mesures de nature à garantir efficacement le respect de la diversité culturelle et à éliminer toute forme de discrimination ou d'incitation à la haine dans les informations diffusées au niveau international.

Géorgie

[*Original : anglais*]
[*18 mai 2004*]

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

1. La situation en matière de sécurité informatique

1.1 Le système de sécurité informatique est en cours d'élaboration.

1.2 Le cahier des charges du système de sécurité informatique a été établi par le Ministère de l'infrastructure et du développement et la Commission géorgienne des communications nationales.

1.3 Le groupe chargé du projet ne dispose pas d'un budget qui lui est propre.

2. Composition du groupe de travail

2.1 Le groupe de travail se compose :

– De la Direction des politiques en matière de télécommunications et de technologies informatiques (Ministère de l'infrastructure et du développement);

– De la Direction technique de la Commission des communications nationales.

3. Principes de base

3.1 Les orientations communes en matière de sécurité informatique seront arrêtées dans le cadre du Programme d'informatisation, lequel est en cours d'élaboration.

3.2 La stratégie de sécurité informatique à suivre par les entreprises, les pouvoirs publics et les systèmes d'information ainsi que l'infrastructure de télécommunication seront fondées sur les normes arrêtées dans le cadre du système de sécurité informatique.

3.3 Le système de sécurité informatique géorgien repose sur les normes internationales harmonisées de l'Organisation internationale de normalisation (ISO), de l'Union internationale des télécommunications et de l'Institut européen des normes de télécommunications.

3.4 Les directives relatives à la sécurité informatique dans les entreprises reposent sur des recommandations et des règles qui cadrent avec la politique de certification facultative retenue dans la norme 17799 de l'ISO.

4. Avantages que la Géorgie pourrait tirer de sa participation dans la société de l'information

4.1 Création d'un espace d'information et d'une infrastructure unifiés dans le cadre de processus internationaux auxquels la Géorgie participerait, y compris la mise au point d'un système de gestion de la sécurité informatique à l'échelon international;

4.2 Adoption de mesures fondées sur les normes internationales régissant les données informatiques en vue de généraliser la protection de l'intégrité des données, la Géorgie faisant ainsi fond sur sa participation à l'Organisation mondiale du

commerce (OMC), à l'Organisation des Nations Unies et à d'autres organisations internationales;

4.3 Entrée dans la nouvelle économie mondiale sur la base des principes de coopération et du libre accès à l'information, compte tenu du fait que la Géorgie doit rattraper son retard en matière de technologies de l'information;

4.4 Renforcement de la sécurité informatique en Géorgie.

5. Principales tâches du Ministère de l'infrastructure et du développement dans le domaine de la sécurité informatique

5.1 Mesure du retard pris dans le domaine des normes télématiques, suivi et analyse des travaux des organismes de normalisation internationaux, adoption de systèmes d'assurance de la qualité, adoption de mesures en vue d'assurer la sécurité informatique et la protection de l'environnement.

5.2 Coordination des projets internationaux et locaux, mise au point d'une stratégie de communication qui cadre avec les normes arrêtées par les organisations internationales, coopération avec les initiatives internationales et les projets régionaux relatifs à la sécurité.

6. Renforcement de la sécurité informatique en Géorgie

6.1 Il importe d'arrêter le budget qui sera alloué au Programme d'informatisation et au système de sécurité informatique et d'obtenir l'appui de la communauté internationale.

6.2 Il est particulièrement important d'obtenir l'aide des organisations internationales dans les domaines suivants :

– Étude des infrastructures télématiques et modernisation des réseaux;

– Analyse et comparaison de différents systèmes et normes de sécurité informatique;

– Mise au point de programmes et de techniques de sécurité informatique applicables aux différents secteurs économiques et sociaux.

7. Coopération avec les organisations internationales

– Union internationale des télécommunications et Communauté régionale des communications (RCC);

– Organisation des Nations Unies;

– Commission économique et sociale pour l'Asie et le Pacifique, Conférence des Nations Unies sur le commerce et le développement et Organisation mondiale du commerce.

8. Projets, séminaires et autres activités

8.1 Union internationale des télécommunications - projet de protection contre les intrusions (Ministère de l'infrastructure et du développement). Organisateurs : Bureau de développement des télécommunications (UIT), société Utimaco, Gouvernement bulgare, Direction des politiques en matière de télécommunications et de technologies informatiques.

8.2 Ateliers de formation sur la mise au point de l'infrastructure des échanges financiers en Géorgie

– Problèmes rencontrés dans la mise au point d'un système fondé sur les nouvelles technologies de l'information et des communications;

– Commerce électronique et informatisation des échanges financiers, des opérations bancaires et des paiements;

– Examen des questions touchant la mise au point d'une infrastructure nationale d'échanges financiers.

Liban

[Original : arabe]
[27 mai 2004]

1. À la faveur des progrès considérables survenus dans le domaine du développement, des applications et des utilisations des technologies de l'information et de la communication, le Liban veille à ce que ces technologies et ces moyens de communication ne soient pas utilisés dans des buts contraires aux principes de la stabilité et de la sécurité internationales.

2. Le Liban estime nécessaire d'interdire l'utilisation de ces technologies à des fins criminelles ou terroristes et se déclare en faveur des résolutions des Nations Unies visant à assurer la protection des informations et de leur confidentialité et à empêcher tout usage illicite de ces technologies.

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

[Original : anglais]
[14 mai 2004]

1. Le Royaume-Uni accueille favorablement le fait que l'Organisation des Nations Unies examine les conséquences de la dépendance croissante envers les réseaux de communication, notamment la vulnérabilité des pays face aux menaces existantes. La sécurité informatique est un élément crucial de la croissance économique mondiale et son importance a été soulignée dans la Déclaration de principes et le Plan d'action adoptés à l'issue de la première partie du Sommet mondial sur la société de l'information.

2. Dans la Déclaration de principes, les participants ont estimé qu'une culture mondiale de la cybersécurité devait être encouragée, développée et mise en œuvre en coopération avec tous les partenaires et tous les organismes internationaux compétents et que ces efforts devaient être soutenus par une coopération internationale renforcée. Le Royaume-Uni est convaincu que la meilleure façon pour les pays d'atteindre leurs objectifs de sécurité est d'encourager une culture mondiale de la cybersécurité, comme décrit dans la Déclaration de principes du Sommet mondial sur la société de l'information et dans les principes du G-8 concernant la protection des infrastructures essentielles de l'information, qui sont repris dans la résolution 58/199 de l'Assemblée générale.

3. Le Royaume-Uni n'estime cependant pas nécessaire d'élaborer un instrument multilatéral qui limiterait la mise au point et l'utilisation de certaines techniques civiles ou militaires. En ce qui concerne les applications militaires des technologies de l'information, un instrument international est inutile. Le droit des conflits armés et en particulier les principes de nécessité et de proportionnalité régissent l'usage de ces technologies. Par ailleurs, un instrument international risquerait de restreindre la libre circulation de l'information, qui, de l'avis des participants au Sommet mondial sur la société de l'information, est un principe fondamental de la société de l'information.

Notions fondamentales

4. Il serait utile de définir les risques que courent les réseaux et les systèmes d'information sous forme de menaces et de points faibles. Les menaces évoluent en permanence et gagnent en complexité. Ce ne sont pas les pays qui représentent la plus grande menace, mais les terroristes, la criminalité organisée et les pirates informatiques, qui tentent d'accéder frauduleusement aux systèmes d'information et de nuire au bon fonctionnement des réseaux. Pour renforcer la cybersécurité mondiale, il faut que la loi punisse les attaques contre les systèmes d'information et les réseaux. La Convention sur la cybercriminalité du Conseil de l'Europe est un bon point de départ pour réprimer la cybercriminalité.

5. L'analyse des menaces ne constitue cependant qu'un seul aspect de la cybersécurité. Le Royaume-Uni estime qu'il ne suffit pas de savoir d'où viennent les dangers pour protéger les réseaux et les systèmes d'information. Il faut encourager la coopération internationale afin de remédier aux points faibles, sachant que ceux-ci peuvent être d'ordre technique, par exemple des imperfections logicielles ou des lacunes dans les protocoles, ou être dus à des erreurs commises par les usagers qui, victimes d'escroqueries en ligne (« phishing » ou « social engineering »), communiquent à autrui des données confidentielles. Faire évoluer la cyberculture, c'est-à-dire la façon dont les réseaux et les systèmes d'information sont mis au point, mis en service et utilisés, est une tâche ambitieuse. Les principes énoncés dans le document intitulé *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* constituent un bon point de départ pour amorcer le changement.

La politique suivie par le Royaume-Uni

6. En 2003, le Royaume-Uni a adopté une stratégie nationale de sécurité informatique, qui porte sur la protection des systèmes essentiels et la tolérance aux pannes et aux attaques des réseaux. La stratégie vise à protéger les données et les systèmes du service public, met l'accent sur l'importance qu'il y a à collaborer avec le secteur privé et prévoit des activités de sensibilisation auprès des entreprises et des particuliers. Elle insiste également sur la collaboration avec les autres pays afin de renforcer la cybersécurité.

7. Le Gouvernement s'est doté de nouvelles structures afin de mettre en œuvre la stratégie, avec la participation active des Ministères de l'intérieur, de l'industrie et de la défense. Il a également nommé des responsables chargés d'évaluer les risques dans chaque ministère et s'attache à étoffer les qualifications techniques des spécialistes qui auront pour mission de prévoir les problèmes de sécurité et d'y porter remède. Le Gouvernement a également fait une large place à la recherche-

développement dans le cadre de la stratégie et a prévu de publier en juin 2004 une étude de grande ampleur sur les politiques visant à assurer la cybersécurité à long terme.

8. La stratégie se compose de trois grandes initiatives. Le Royaume-Uni a créé en 1999 le National Infrastructure Security Co-ordination Centre (NISCC), initiative interinstitutions qui jouit d'une excellente réputation au niveau international dans le domaine de la protection des infrastructures critiques. Le Centre encourage la mise en commun de l'information entre les différents groupes, coordonne la diffusion en temps réel des alertes signalées par son réseau de correspondants internationaux et joue un rôle majeur en décelant les carences des protocoles et en y remédiant.

9. Le Royaume-Uni a également pris une part active à la mise au point de normes relatives à la gestion de la sécurité informatique, notamment les directives sur la gestion de la sécurité de l'information (norme ISO/IEC 17799), inspirées d'une norme britannique, qui s'impose de plus en plus comme la principale norme en matière de sécurité. La démarche retenue consiste à mettre l'accent sur les points faibles et les risques, ce qui permet aux organisations de généraliser les mesures de gestion de la sécurité de l'information.

10. Le Royaume-Uni met actuellement au point une stratégie de lutte contre la cybercriminalité qui repose sur la Convention sur la cybercriminalité du Conseil de l'Europe et sur les directives de l'Union européenne. Conscients de la nature changeante de la cybercriminalité, les services de police se sont dotés d'une unité nationale spécialisée dans la lutte contre la criminalité informatique et d'unités spécialisées au sein des forces de police locales.

La coopération internationale

11. Les participants au Sommet mondial sur la société de l'information ont mis l'accent sur l'importance que revêtait la coopération internationale pour tirer le meilleur parti de la société de l'information. La résolution 58/32 de l'Assemblée générale donne l'occasion de jeter ~~les bases de la~~ cybersécurité afin de protéger les intérêts des gouvernements, des entreprises et des particuliers en réduisant les risques de désorganisation des systèmes et en protégeant la libre circulation de l'information. Les Lignes directrices de l'OCDE constituent un bon point de départ pour mieux comprendre les principes qui sous-tendent la cybersécurité et encourager l'instauration d'une culture de la cybersécurité.

12. Le Royaume-Uni se félicite de l'intérêt porté par l'Organisation des Nations Unies à la question de la sécurité de l'information et estime qu'elle peut faciliter l'instauration d'une culture de la cybersécurité en examinant les aspects ci-après :

- Élaboration et échange de pratiques de référence;
- Mise au point d'une politique commune fondée sur la Convention du Conseil de l'Europe afin de réprimer la cybercriminalité;
- Renforcement de la collaboration entre les autorités nationales afin qu'elles améliorent leur capacité de réaction, qu'il s'agisse des risques et des carences qui auront été décelés, de la conduite des enquêtes ou de la poursuite des responsables;
- Mise au point d'une démarche plus cohérente en vue de remédier aux carences des systèmes d'information.