Nations Unies A/54/213

Assemblée générale

Distr. générale
10 août 1999
Français
Original: anglais/arabe/
russe/espagnol

Cinquante-quatrième session
Point 71 de l'ordre du jour provisoire*
Les progrès de la téléinformatique dans le contexte de la sécurité internationale

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

Rapport du Secrétaire général

Table des matières

* A/54/150.

I. Introduction

1. Aux paragraphes 2 et 3 de la résolution 53/70 adoptée le 4 décembre 1998 sous le titre «Les progrès de la téléinformatique dans le domaine de la sécurité internationale», l'Assemblée générale a invité tous les États Membres à 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; c) L'opportunité d'élaborer des principes internationaux susceptibles de renforcer la sécurité des systèmes télématiques mondiaux et d'aider à combattre le terrorisme et la criminalité dans le domaine de l'information; et a prié le Secrétaire général de lui présenter un rapport à ce sujet à sa cinquante-quatrième session.

2. Le 19 mars 1999, le Secrétaire général adressait une note verbale aux États Membres par laquelle il les priait, à la demande de l'Assemblée, de lui faire part de leurs observations. Les réponses reçues des gouvernements sont reproduites ci-après.

II. Réponses reçues des gouvernements

Arabie saoudite

[Original : arabe]
[27 mai 1999]

Un grand nombre d'organismes publics et d'institutions privées dans les pays où les systèmes informatiques revêtent une importance croissante ont réalisé des progrès dans le domaine des technologies de l'information. Ces progrès s'accompagnent toutefois de tentatives de plus en plus nombreuses d'entités internationales visant à désorganiser, menacer et altérer les systèmes d'information à des fins destructrices et terroristes. Ces tentatives ont des répercussions sur l'économie, la société et la sécurité. Il importe au plus haut point d'adopter des principes et des instruments juridiques internationaux pour contrer la menace qui plane sur la sécurité de l'information et pour combattre et criminaliser ces tentatives internationales. Leurs auteurs doivent être traduits en justice et punis par les organisations internationales compétentes.

Australie

[Original : anglais]
[2 juin 1999]

1. L'Australie a présidé le groupe d'experts de l'Organisation de coopération et de développement économiques (OCDE) qui a élaboré les Lignes directrices régissant la sécurité des systèmes d'information. Elle assure également la présidence du groupe de travail de l'OCDE sur la sécurité de l'information et de la vie privée qui est notamment chargé d'évaluer les besoins en matière de sécurité de l'information. L'Australie participe à l'élaboration de normes dans le domaine de la sécurité de l'information dans le cadre de l'Organisation internationale de normalisation (ISO). Sur le plan national, elle a mis en place des procédures détaillées visant à assurer la sécurité des données administratives. Par ailleurs, Standards Australia et Standards New Zealand se sont inspirés d'un texte normatif britannique pour mettre au point une norme d'administration de la sécurité de l'information. Le Gouvernement australien et les entreprises informatiques s'efforcent ensemble d'introduire des mesures visant à protéger l'infostructure nationale. L'Australie a adopté des lois qui protègent les systèmes télématiques contre les interceptions, les intrusions et certaines formes d'utilisation malintentionnée.

2. Les lignes directrices de l'OCDE, telles qu'appliquées par l'Australie, stipulent ce qui suit : «La sécurité des systèmes d'information a pour objectif de protéger les intérêts de ceux qui comptent sur les systèmes d'information, contre les préjudices imputables à des défauts de disponibilité, de confidentialité et d'intégrité.»

3. Les différentes technologies étant de plus en plus interdépendantes, l'objectif ci-dessus peut être étendu à ce type particulier de système d'information que sont les systèmes de télécommunications. Toute intrusion ou utilisation malintentionnée des systèmes d'information aura des incidences sur la disponibilité, la confidentialité ou l'intégrité des données. Étant donné que l'environnement est en mutation permanente, il serait dangereux que les normes soient liées à une technologie spécifique.

4. L'Australie estime que le Département du désarmement du Secrétariat de l'Organisation des Nations Unies n'est pas l'organe compétent pour élaborer des principes internationaux sur la sécurité des systèmes télématiques au niveau mondial. La téléinformatique a des répercussions sur différentes questions : commerce, développement économique, bien-être des individus, application des lois et sécurité nationale. Des principes et des directives ont déjà été mis au point en la matière par d'autres instances – OCDE, ISO, Union

internationale des télécommunica-tions – dans une perspective plus vaste que celle qui est envisagée dans la résolution 53/70 de l'Assemblée générale. En outre, des organismes internationaux, comme l'Institut des Nations Unies d'Asie et de l'Extrême-Orient pour la prévention du crime et le traitement des délinquants (UNAFEI) et le Centre de prévention de la criminalité internationale s'occupent de la criminalité informatique. L'Australie estime inutile que d'autres organismes des Nations Unies marchent sur les brisées d'institutions qui se penchent déjà sur la question de la sécurité informatique et des utilisations frauduleuses. Elle est toutefois favorable à une initiative tendant à centraliser les éléments d'information disponibles sur les travaux entrepris par d'autres instances.

Bélarus

[Original : anglais]
[25 mai 1999]

1. La République du Bélarus approuve pleinement la résolution 53/70 adoptée par l'Assemblée générale le 4 décembre 1998 sous le titre «Les progrès de la téléinformatique dans le domaine de la sécurité internationale». Le développement irrésistible des nouvelles technologies de l'information et des moyens de télécommunication multiplie les chances d'accélérer l'avancée mondiale de la civilisation. Dans le même temps, comme il est noté dans la résolution 53/70, ces technologies et ces moyens risquent «d'être utilisés à des fins incompatibles avec le maintien de la stabilité et de la sécurité internationales et de nuire à la sécurité des États».

2. La résolution 53/70 a été adoptée fort opportunément dans la mesure où elle appelle l'attention de la communauté internationale sur le fait que la téléinformatique peut être utilisée pour faire la guerre et sur la nécessité d'empêcher que les nouvelles technologies et moyens informatiques soient employés à des fins militaires avec des effets comparables à ceux des armes de destruction massive. Par ailleurs, la résolution 53/70 permet de s'attaquer spécifiquement à la question de la sécurité de l'information sur le plan international, et notamment à l'utilisation frauduleuse des systèmes téléinformatiques et aux problèmes d'intrusion. En dernier lieu, il est souhaitable de s'entendre sur ce que doit être la sécurité de l'information au niveau international et sur les principes juridiques internationaux à adopter en vue de renforcer la sécurité des systèmes téléinformatiques au niveau mondial et de lutter contre le terrorisme et la criminalité informatiques.

Brunéi Darussalam

[Original : anglais]
[7 juin 1999]

La Mission permanente du Brunéi Darussalam auprès de l'Organisation des Nations Unies a l'honneur de faire tenir les vues du Ministère de la défense de son pays, conformément à la résolution 53/70 adoptée le 4 décembre 1998 par l'Assemblée générale sous le titre «Les progrès de la téléinformatique dans le domaine de la sécurité internationale» :

> «En tant que responsable de la défense nationale, le Ministère de la défense a conscience qu'en une époque placée sous le signe des technologies de l'information, la sécurité de l'information est une question importante. Il attache une grande importance à toutes les informations dont la transmission peut constituer une menace pour la sécurité nationale. Étant donné que les technologies de l'information intéressent également d'autres ministères, il coopérera avec les instances compétentes afin d'oeuvrer dans le sens prévu par la résolution. Pour que la sécurité des communications internationales puisse être protégée et garantie, il importe de considérer qu'il s'agit d'une question entrant dans les attributions de la Cour internationale de justice.»

Cuba

[Original : espagnol]
[28 juin 1999]

Appréciation générale sur la question de la sécurité de l'information

1. L'emprise très large des technologies de l'information, dont dépendent désormais sur presque toutes les sphères de l'activité humaine, qui a inspiré l'expression «informatisation de la société» et amène souvent à parler de «l'ère de l'information», pose de nouveaux problèmes de sécurité qui méritent d'être examinés avec attention non seulement par chaque État mais aussi par l'ensemble de la communauté internationale.

2. Pour cette raison, l'Organisation des Nations Unies est à même de débattre des méthodes et moyens appropriés à la lutte contre les dangers que peut faire peser sur la sécurité internationale l'utilisation des nouvelles technologies téléinformatiques à des fins autres que pacifiques.

3. Par ailleurs, il faut faire le nécessaire pour que les nouvelles technologies puissent servir au développement de tous les États, notamment des pays sous- développés qui ne disposent pas de ressources suffisantes pour mettre au point de telles technologies par leurs propres moyens.

4. Toutefois, la mondialisation est déjà une réalité dans le domaine de l'information et des télécommunications et les

distances ne constituent plus un obstacle à l'échange de données; dans le même temps, les systèmes qui rendent possibles les échanges d'informations sont sans cesse plus vulnérables. Il faut souligner que la mondialisation entraîne un certain niveau d'homogénéisation qui facilite les intrusions dans les systèmes.

5. Il ne faut pas oublier qu'il s'agit de technologies qui ont vu le jour dans les pays développés, parmi lesquels les États-Unis d'Amérique. La plus grande puissance hégémonique du monde, notamment dans le domaine de la téléinformatique, jouit d'une position prééminente grâce à laquelle elle impose des normes technologiques qui facilitent l'utilisation des systèmes téléinformatiques comme moyens d'agression.

6. À l'inverse, les pays sous-développés n'ont d'autre solution que d'adopter ces technologies afin de survivre dans les conditions ainsi créées. La plupart du temps, ces pays n'ont pas pleinement conscience des risques et dédaignent les arrangements, services ou mécanismes de sécurité. Les systèmes informatiques sont ainsi plus vulnérables, ce qui, compte tenu de la présence de la téléinformatique dans toutes les sphères du développement, peut donner naissance à des situations qui mettent en danger la sécurité internationale.

7. Cuba se félicite d'avoir la possibilité de faire part de ses vues à l'Assemblée générale, suite à l'initiative qui a conduit à l'adoption par consensus de la résolution 53/70. Cuba a pleinement conscience de l'importance que revêt cette question et participera activement aux travaux prévus pour donner suite à cette résolution.

Définition des notions fondamentales relatives à la sécurité de l'information, y compris les incursions illicites dans les systèmes téléinformatiques et les utilisations illégales de ces systèmes et des données auxquelles ils donnent accès

8. La téléinformatique connaît un essor sans précédent, ce qui malheureusement permet de l'exploiter à des fins hostiles au service de la politique d'agression que certains États ont adoptée à l'égard d'autres États.

9. À cet égard, il faut souligner que le développement et la popularité des réseaux mondiaux, notamment d'Internet, ont eu des conséquences notables. Bien que leur usage soit très répandu, les systèmes téléinformatiques sont encore gérés sur une base purement coopérative, ce qui a son importance, car le caractère non contraignant des règles qui régissent l'Internet est à la fois son principal atout et sa plus grande faiblesse.

10. Les règles communes visant à améliorer et renforcer la sécurité des réseaux mondiaux ne sont pas contraignantes parce que les pays n'ont pas une législation uniforme concernant l'exploitation des réseaux d'information.

11. Toutefois, comme le raccordement aux réseaux mondiaux n'est en rien obligatoire, on peut légitimement affirmer que les règles de conduite en vigueur doivent faire partie du contrat d'accès au réseau et que tout manquement doit pouvoir être sanctionné dans tous les systèmes juridiques.

12. Protéger l'information signifie notamment en assurer la confidentialité (les données ne devraient être accessibles qu'aux personnes qui sont autorisées à les utiliser) et l'intégrité (protéger les données contre toute modification non autorisée), et veiller à que les systèmes demeurent accessibles (l'accès ne doit pas être refusé sauf s'il s'agit de tentatives d'accès frauduleuses).

13. Dans ce contexte, il importe de tenir compte de quelques critères fondamentaux :

a) Tout utilisateur est responsable de ses actions; en d'autres termes, toute tentative d'accès illicite à un ordinateur ou d'utilisation illégale d'un réseau constitue une violation expresse des règles de conduite, même si les moyens de protection en vigueur sont insuffisants;

b) Les organismes qui utilisent les technologies de l'information sont responsables de l'utilisation qu'en font leurs employés et doivent donc mettre en place des mesures de sécurité appropriées, ainsi que des règles et des procédures de contrôle. De même, chaque pays doit adopter des instruments adaptés afin que les organismes présents sur son territoire respectent ces obligations;

c) Les fournisseurs de services informatiques ou d'accès à un réseau doivent garantir la sécurité des systèmes qu'ils gèrent. Ils sont également tenus d'informer les utilisateurs des procédures de sécurité en vigueur et de toute modification de ces procédures;

d) Les fabricants et les distributeurs de systèmes doivent répondre de la fiabilité de leurs produits et veiller à ce qu'ils soient munis de dispositifs de sécurité adéquats. Ils doivent évaluer la sécurité des systèmes avant leur commercialisation et veiller à ce qu'une description des dispositifs de sécurité soit livrée avec chaque système. Les fabricants et distributeurs sont tenus de réparer gratuitement les éléments défectueux des systèmes qu'ils vendent ou distribuent;

e) Les utilisateurs et prestataires de services, les éditeurs de logiciels et fabricants de matériel sont tenus de coopérer dans le domaine de la sécurité. Les responsables des différents sites devraient s'avertir mutuellement lorsqu'ils remarquent que des accès illicites se produisent et s'efforcer de coopérer pour prévenir les violations de sécurité par des

mesures telles que le suivi des connexions, la détection des violations et l'assistance juridique.

14. Les principaux objectifs d'une personne qui cherche à s'introduire frauduleusement sur un réseau sont les suivants :

a) S'approprier, altérer ou détruire des données. Il s'agit là du but principal de la plupart des pirates;

b) Utiliser frauduleusement l'ordinateur d'autres personnes en usurpant leur identité;

c) Établir une tête de pont pour lancer d'autres attaques. Une personne peut s'introduire dans un système dans le seul but de s'en servir pour lancer des attaques vers d'autres systèmes;

d) Empêcher l'accès à un service, c'est-à-dire faire en sorte qu'une personne qui est autorisée à utiliser des données ne puissent pas y accéder;

e) Faire une opération de publicité, ce qui est très efficace dans le cas des serveurs Web.

15. L'utilisation illicite des systèmes téléinformatiques et des données qu'ils abritent, surtout lorsqu'elle est le fait d'États qui exploitent cette méthode pour s'ingérer dans les affaires intérieures d'autres États, constitue une violation de la souveraineté et de l'indépendance des États cibles et est source de tensions dangereuses pour la sécurité internationale.

16. En s'attachant sans relâche à atteindre des fins politiques qui servent leurs intérêts nationaux, les États en viennent notamment à utiliser les stations de radio et de télévision en violation des normes internationales en vigueur pour miner l'ordre constitutionnel d'autres États considérés comme des ennemis.

17. Cuba est une des victimes de ce type de menées. Pour donner une idée de la gravité de la situation, Cuba est depuis des décennies l'objet des attaques de la radio et de la télévision américaines, en application d'une politique d'agression menée résolument par la première puissance militaire, économique et politique du monde dont l'objectif avoué est de renverser le Gouvernement cubain.

18. Par exemple, jusqu'en avril 1999, 17 stations diffusaient à partir du territoire américain des informations subversives à destination de Cuba.

19. Chaque jour, entre 288,5 et 306,5 heures d'émissions radiophoniques en ondes courtes et moyennes et en modulation de fréquence ont été diffusées, soit 2 084,5 heures chaque semaine et 2 089 heures si l'on ajoute les émissions télévisées.

20. Dans la plupart des cas, ces émission incitaient les citoyens cubains à commettre des actes de désobéissance civile et de subversion ou de terrorisme.

21. Cuba a toujours été partisane du règlement des différends entre États sur la base de l'égalité et du respect de la souveraineté et de l'indépendance nationales et s'est maintes fois publiquement exprimée en ce sens. Sa position demeure inchangée.

Avantages découlant de l'établissement de principes internationaux visant à améliorer la sécurité des systèmes téléinformatiques mondiaux et à lutter contre le terrorisme et la criminalité dans le domaine de l'information

22. Il est clair que l'essor des nouvelles technologies de l'information doit s'accompagner d'efforts visant à élaborer une législation internationale dans ce domaine, et en particulier à mettre en place un cadre juridique approprié qui renforcera la sécurité des systèmes d'information.

23. La tâche ne sera pas aisée compte tenu du fait que, dans certains domaines, il faut encore élaborer des définitions communément acceptées qui faciliteront la codification de nouveaux principes allant dans le sens d'une plus grande sécurité.

24. De par leur nature, les réseaux mondiaux dépassent les limites juridictionnelles des pays et, dans de nombreux cas, rendent vaines les frontières géographiques. Par ailleurs, étant donné les disparités de développement entre les pays, il est difficile d'imposer une réglementation internationale uniforme à l'ensemble des pays partageant ces technologies.

25. Toutefois, nous ne sommes pas totalement démunis dans la mesure où des principes et des instruments juridiques internationaux alignés sur les progrès technologiques récents ont été acceptés et adoptés par les États dans de nombreuses instances multilatérales. Nous pourrons nous en inspirer pour élaborer et mettre au point de nouveaux principes internationaux visant à renforcer la sécurité des systèmes téléinformatiques mondiaux et à lutter contre le terrorisme et la criminalité dans le domaine de l'information.

26. Pour ne mentionner que quelques exemples, Cuba estime que les accords suivants méritent d'être pris en compte :

a) La résolution 110 (II) du 3 novembre 1947 par laquelle l'Assemblée générale a condamné la propagande destinée ou de nature à provoquer ou à encourager toute menace contre la paix, rupture de la paix ou tout acte d'agression;

b) La Convention internationale des télécommunications adoptée en 1982 à Nairobi, ainsi que les instruments juridiques internationaux connexes adoptés par l'Organisation des Nations Unies pour l'éducation, la science et la culture et l'Union internationale des télécommunications;

c) Les Principes régissant l'utilisation par les États de satellites artificiels de la Terre aux fins de la télévision directe qui ont été adoptés par l'Assemblée générale et qui stipulent que ces activités doivent être menées en conformité avec le droit international et d'une manière compatible avec le développement de la compréhension mutuelle et le renforcement des relations amicales et de la coopération entre tous les États et tous les peuples dans l'intérêt du maintien de la paix et de la sécurité internationales;

d) La Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction à laquelle sont annexées des dispositions sur la protection des informations confidentielles qui pourraient servir de référence lors de l'élaboration des principes susmentionnés.

27. En dernier lieu, et eu égard au rôle majeur que l'Organisation des Nations Unies devrait jouer dans l'examen de la question, Cuba estime que l'Organisation devrait notamment reconnaître que chaque pays a le droit de protéger ses systèmes téléinformatiques au moyen de dispositifs fiables et recommander que les États Membres adoptent des lois qui sanctionnent le développement et la dissémination de virus informatiques et autres programmes nuisibles. En outre, des accords multilatéraux ayant force obligatoire et interdisant les agressions contre les systèmes téléinformatiques pourraient être conclus dans le cadre de l'ONU. On pourrait aussi envisager des accords qui garantiraient que les nouvelles technologies mises au point à des fins pacifiques soient mises à la disposition de tous les États.

États-Unis d'Amérique

[Original : anglais]
[20 mai 1999]

Observations générales sur les questions de sécurité de l'information et définition de concepts fondamentaux

1. Les États-Unis estiment que la sécurité de l'information est un thème vaste et complexe qui touche à beaucoup de domaines et concerne autant les individus que les groupes et les gouvernements. Si à certains égards il concerne la paix et la sécurité internationales (qui relèvent de la Première Commission), il comporte aussi des aspects techniques intéressant les communications mondiales et des aspects non techniques intéressant la coopération économique et le commerce, les droits de propriété intellectuelle, l'application de la loi, la coopération contre le terrorisme et d'autres domaines relevant de la Deuxième ou de la Sixième Commission. Il ne faut pas s'en remettre aux seuls gouvernements pour appliquer les mesures et programmes nécessaires car la sécurité de l'information concerne aussi les individus, les associations, les entreprises et autres organisations du secteur privé.

Aspects relatifs à la sécurité internationale

2. Lors de conflits armés, des pays ont déjà eu recours à diverses techniques pour assurer la sécurité de l'information. On citera, par exemple, deux techniques depuis longtemps utilisées : le brouillage des fréquences radio et les contre-mesures électromagnétiques. À l'avenir, les armées devront protéger leurs liaisons et systèmes informatiques. En outre, les États Membres doivent se doter des moyens de réparer leurs systèmes d'information essentiels au cas où une catastrophe naturelle ou autre mettrait hors service leurs installations et réseaux publics et privés de communication. La sécurité de l'information concerne également la protection des informations relatives aux potentiels militaires et à d'autres aspects de la sécurité nationale.

Facteurs économiques, commerciaux et techniques

3. La sécurité de l'information comprend la protection des travaux de recherche scientifique à caractère commercial, ainsi que des technologies de production et autres types de données qui sont propriété industrielle (par exemple, les plans de commercialisation et les fichiers de clientèle).

4. Elle implique également que les accords internationaux concernant la propriété intellectuelle (comme le matériel audio-vidéo et les logiciels) soient effectivement appliqués afin d'empêcher toute reproduction et vente non autorisées. La confidentialité est un autre aspect de la sécurité de l'information : il importe de protéger les informations personnelles et commerciales transmises via le réseau international public ou des liaisons privées.

5. Sur le plan technique, les réglementations de l'Union internationale des télécommunications et les activités de ses homologues nationaux garantissent la compatibilité des signaux électroniques et la fiabilité du réseau international et l'utilisation ordonnée du spectre électromagnétique. Elles s'appliquent également aux satellites qui fournissent un large éventail de services, comme la transmission de données et de fréquences vocales ainsi que les systèmes de positionnement

et d'autres informations utilisées pour la navigation aérienne et maritime et pour les services de recherche et de sauvetage. En outre, les normes techniques et de sécurité offrent des garanties importantes aux fabricants et aux utilisateurs de dispositifs électroniques, y compris d'ordinateurs. On peut considérer que ces réglementations entrent dans le cadre général de la sécurité de l'information.

Application des lois et coopération dans la lutte contre le terrorisme

6. L'utilisation massive des technologies de l'information fait que l'on a atteint un degré sans précédent d'interconnexion et d'interdépendance au niveau mondial et qu'un grand nombre d'activités aux niveaux national et international, dans le secteur public comme privé, peuvent être détournées à des fins criminelles ou terroristes.

7. La dépendance à l'égard des technologies de l'information varie d'un pays à l'autre, mais l'éventail des activités (économiques, commerciales, industrielles, éducatives, juridiques) pour lesquelles on fait appel à ce type de technologies est si large que tous les pays sont potentiellement menacés par des actes criminels. En outre, cette dépendance ne peut que se renforcer car les technologies de l'information revêtent une importance croissante pour la stabilité des gouvernements ainsi que pour le bon fonctionnement du système commercial mondial et des systèmes de communications entre les pays.

8. En conséquence, les États-Unis estiment que l'exploitation des technologies de l'information à des fins criminelles menace les intérêts de tous les pays et s'accordent avec d'autres pays pour reconnaître qu'il faut trouver des moyens appropriés, aux niveaux unilatéral et multilatéral, pour garantir l'intégrité des ressources qui reposent sur l'utilisation des technologies de l'information.

9. De même, les États-Unis considèrent toute intrusion ou tentative illégale visant à dérégler ou altérer leurs systèmes d'information comme un danger potentiel pour leurs infrastructures essentielles et, partant, comme une menace contre leurs intérêts nationaux. Les États-Unis, conscients de la gravité de cette menace, ont mis en place des programmes publics et privés visant à protéger leurs infrastructures essentielles. Toutefois, ils reconnaissent également qu'étant donné que ces infrastructures deviennent de plus en plus interdépendantes au niveau mondial, le succès de leurs programmes de protection repose en partie sur la sécurité des systèmes internationaux auxquels les États-Unis sont raccordés.

10. En conséquence, les États-Unis estiment que tous les pays doivent prendre des mesures pour assurer l'intégrité de leurs systèmes d'information nationaux et poursuivre en justice les criminels ou les terroristes internationaux qui opèrent à partir de leur territoire pour dérégler ces systèmes. Il incombe à chaque pays de veiller à ce que ses systèmes d'information soient fiables, ne puissent pas être utilisés à des fins criminelles ou être neutralisés et qu'ils puissent être rapidement remis en service en cas d'interruption.

11. Le droit pénal américain interdit toute intrusion dans les infrastructures d'information des États-Unis. Ceux-ci engagent tous les pays à revoir leur législation pour s'assurer qu'il est prévu de poursuivre en justice les personnes responsables d'avoir exploité les systèmes d'information à des fins criminelles ou terroristes. Les États-Unis ont jugé nécessaire à maintes reprises de modifier leurs règlements relatifs au secteur informatique afin d'y apporter les améliorations nécessaires et de régler les nouveaux problèmes.

Est-il opportun de définir des principes internationaux?

12. Comme on l'a noté plus haut, la sécurité de l'information est une question vaste et complexe. Elle revêt de multiples aspects qui sont liés les uns aux autres de manière extrêmement complexe. Étant donné la nécessité d'examiner tous ces aspects et de bien comprendre leurs interactions, il serait prématuré de définir des principes généraux concernant la sécurité de l'information sous tous ses aspects. La communauté internationale doit étudier à fond la question avant de passer à l'étape suivante. À cet effet, les États Membres devraient solliciter les vues d'un large éventail d'experts officiels et privés.

13. Cela étant, il est évident qu'une coopération internationale s'impose pour régler avec efficacité les problèmes nouveaux et complexes soulevés par le terrorisme et la criminalité dans le domaine de l'information. Plusieurs initiatives multilatérales de coopération sont en cours. Le Conseil de l'Europe examine un projet de convention sur la cybercriminalité; le Groupe du G-8 chargé de la criminalité faisant appel à la haute technologie étudie actuellement des mesures concernant une assistance juridique mutuelle ainsi que d'autres questions relatives à ce type de criminalité; l'Organisation des États américains a également créé un groupe de travail sur la question; et l'Institut des Nations Unies pour la prévention du crime et le traitement des délinquants en Asie et au Proche-Orient étudie plusieurs aspects de la question dans le contexte du système des Nations Unies.

14. Toutes les initiatives sont intéressantes et devraient être appuyées pour qu'elles puissent porter leurs fruits. Il serait très peu judicieux de la part de l'Assemblée générale de définir des stratégies ou d'entreprendre des activités qui

entraveraient les travaux actuels de la communauté internationale ou préjugeraient de leur issue.

Fédération de Russie

[Original : russe]
[9 juin 1999]

Généralités

28. La révolution de l'information, c'est-à-dire le développement rapide et l'application universelle de technologies de pointe d'information et de télécommunication, est un des aspects les plus marquants de l'actualité scientifique et technologique mondiale. Elle a des répercussions sur tous les domaines d'activité, offre de nouvelles perspectives de coopération internationale et crée une situation dans laquelle l'information devient un élément extrêmement précieux de la richesse et des ressources stratégiques des pays.

29. Il est évident que parallèlement aux aspects positifs de ce phénomène, il existe un danger réel que les progrès dans le domaine de l'information soient utilisés à des fins contraires aux objectifs de stabilité et de sécurité internationales et aux principes d'égalité souveraine des États, de règlement pacifique des conflits et des différends, de non-recours à la force, de non-ingérence dans les affaires intérieures des États et de respect des libertés et des droits fondamentaux.

30. Le fait que les pays utilisent les technologies d'information les plus récentes pour renforcer leur potentiel militaire compromet l'équilibre des forces aux niveaux mondial et régional et donne lieu à des tensions entre les anciens et nouveaux centres de pouvoir et d'influence.

31. Une nouvelle source d'affrontement se fait jour sur la scène internationale et les progrès technologiques et scientifiques dans le domaine de la téléinformatique risquent de conduire à une accélération de la course aux armements. Une telle situation a des répercussions tant sur la sécurité nationale des États que sur l'ensemble du système de sécurité collective aux niveaux régional et mondial.

32. L'information devient une arme dont l'utilisation, selon les progrès technologiques réalisés par un pays et la vulnérabilité de ses structures de base, peut avoir des effets dévastateurs comparables à ceux des armes de destruction massive. Il est évident que des groupes terroristes, extrémistes ou criminels, ainsi que des malfaiteurs peuvent se servir d'une telle arme.

33. En conséquence, le caractère universel, secret ou impersonnel de cette arme de l'information, la possibilité de s'en servir sans tenir compte des frontières nationales, sa rentabilité et son efficacité en font un moyen extrêmement dangereux d'exercer une influence. Le droit international n'offre pratiquement aucun moyen de contrôler le développement et l'application de cette arme.

34. Il importe donc d'adopter un instrument juridique international permettant de contrôler le développement mondial des technologies de l'information civiles et militaires et de mettre au point une politique internationale concertée de sécurité de l'information, qui réponde aux besoins de la sécurité internationale.

Mesures proposées

35. La résolution 53/70 de l'Assemblée générale, intitulée «Les progrès de la téléinformatique dans le contexte de la sécurité internationale» et adoptée par consensus le 4 décembre 1998, doit constituer la base de l'action de la communauté internationale. Le projet de résolution avait été présenté par la Fédération de Russie.

36. L'Assemblée générale doit adopter des résolutions sur la sécurité de l'information pour réduire le risque d'utilisation de l'information à des fins terroristes, criminelles ou militaires.

37. Il importe de continuer d'examiner conjointement la situation dans le domaine de la sécurité de l'information afin de recenser tous les points de vue et d'en tenir compte dans l'effort commun pour améliorer la situation.

38. À mesure que l'on aura dégagé les points consensuels et défini une démarche commune, il faudra définir des principes internationaux (par exemple, un régime ou un code de conduite pour les États), en vue de renforcer la sécurité de l'information au niveau international. Ces principes pourraient d'abord prendre la forme d'une déclaration multilatérale puis être intégrés dans un instrument juridique multilatéral. La Conférence du désarmement à Genève pourrait aussi s'occuper de la question.

39. Par ailleurs, la communauté internationale devrait examiner et adopter en bloc les principes susmentionnés, compte tenu des menaces tant d'ordre militaire que des risques d'activités terroristes ou criminelles, en vue de les appliquer à la fois au domaine militaire et au domaine civil.

Principales menace à la sécurité de l'information au niveau international

40. Les principales menaces qui planent sur la sécurité de l'information au niveau international sont les suivantes :

a) Création et utilisation de moyens permettant d'exercer une influence sur les ressources et les systèmes d'information d'un autre État ou de les endommager;

b) Utilisation délibérée de l'information en vue d'exercer une influence sur les structures de base d'un autre État;

c) Utilisation de l'information en vue de saper le système social et politique d'un État; manipulation psychologique de la population en vue de déstabiliser la société;

d) Initiatives prises par des États pour dominer et contrôler le secteur de l'information, empêcher d'accéder aux technologies de l'information les plus récentes et créer une situation dans laquelle les autres États se retrouvent technologiquement dépendants en matière d'information;

e) Action d'associations, organisations ou groupes terroristes, extrémistes ou criminels ou de malfaiteurs, qui font planer une menace sur les ressources d'un État en matière d'information et sur ses structures essentielles;

f) Élaboration et adoption par les États de plans ou de doctrines ouvrant la voie à une guerre de l'information, à une course aux armements et à des tensions entre les États, et qui risqueraient de provoquer une guerre de l'information;

g) Utilisation des technologies de l'information et des moyens de communication au détriment des droits de l'homme et des libertés dans le domaine de l'information;

h) Diffusion transfrontière sauvage de l'information, en violation des principes et règles du droit international et des législations nationales;

i) Manipulation des flux d'information, désinformation et dissimulation de l'information en vue de mettre en péril l'environnement spirituel et psychologique d'un pays et de saper les valeurs esthétiques, éthiques, morales et culturelles traditionnelles;

j) Développement et acquisition d'un monopole sur les infrastructures d'information et de télécommunication d'un autre État, y compris les moyens d'exploitation au niveau international.

Principaux objectifs et tâches à réaliser en vue de mettre en place un régime international de sécurité de l'information

41. Il importe d'adopter un cadre juridique international en vue de :

a) Déterminer les principales caractéristiques des guerres de l'information et procéder à une classification;

b) Déterminer les principales caractéristiques de l'information en tant qu'arme ainsi que des méthodes et moyens pouvant être considérés comme des armes de l'information, et procéder à une classification;

c) Contrôler le trafic des armes de l'information;

d) Interdire le développement, la diffusion ou l'utilisation des catégories les plus dangereuses des armes de l'information;

e) Conjurer la menace de guerres de l'information;

f) Interdire l'utilisation des technologies de l'information et des moyens de communication à des fins hostiles et notamment contre certains types de structures;

g) Reconnaître que l'utilisation des armes de l'information contre les structures fondamentales d'un pays est comparable à l'utilisation d'armes de destruction massive;

h) Créer les conditions nécessaires à l'échange équitable et sûr d'informations au niveau international, fondé sur un équilibre des intérêts entre les individus, la société et l'État;

i) Prévenir le risque d'utilisation des technologies de l'information et des moyens de communication à des fins terroristes ou criminelles;

j) Prévenir le risque d'utilisation des technologies de l'information et des moyens de communication pour influencer la conscience sociale en vue de déstabiliser une société et un État;

k) Élaborer une procédure de notification mutuelle et de prévention de l'utilisation non autorisée de l'information en vue d'influencer d'autres États;

l) Créer un mécanisme de règlement des différends dans le domaine de la sécurité de l'information;

m) Créer un système international de certification de la sécurité des technologies de l'information et des moyens de communication (y compris les logiciels et le matériel informatique);

n) Mettre en place un système de coopération internationale entre les organismes chargés de faire appliquer la loi en vue de prévenir les délits dans le domaine de l'information;

o) Créer un mécanisme chargé de veiller au respect du régime international de sécurité de l'information;

p) Harmoniser les législations nationales en matière de sécurité de l'information.

Concepts fondamentaux en matière de sécurité internationale de l'information

42. On trouvera ci-après quelques définitions de concepts fondamentaux en matière de sécurité internationale de l'information :

a) *Secteur de l'information*. Domaine d'activité comprenant la création, la consommation et l'utilisation de

l'information, y compris la conscience individuelle et sociale, les infrastructures téléinformatiques et l'information elle-même;

b) *Ressources d'information*. Infrastructure de l'information (matériel et systèmes permettant de créer, de traiter, de stocker et de transmettre l'information), y compris les fichiers et bases de données et les flux d'information;

c) *Guerre de l'information*. Affrontement entre États dans le domaine de l'information, en vue d'endommager les systèmes et ressources d'information et les structures fondamentales, et de saper le système politique et social d'un autre État, manipulation psychologique de la population d'un État et déstabilisation de la société;

d) *Arme de l'information*. Moyens et méthodes utilisés pour endommager les ressources et systèmes d'information d'un autre État; utilisation de l'information au détriment du système de défense et des structures administratives, politiques, sociales, économiques ou autres structures de base d'un État, et manipulation de la population d'un État en vue de déstabiliser la société et cet État;

e) *Sécurité de l'information*. Protection des intérêts fondamentaux de la société et d'un État dans le secteur de l'information, y compris les infrastructures téléinformatiques et l'information elle-même (intégrité, objectivité, accessibilité, confidentialité, etc.);

f) *Menace à la sécurité de l'information*. Facteurs qui mettent en péril les intérêts fondamentaux des individus, de la société et de l'État dans le secteur de l'information;

g) *Sécurité internationale de l'information*. État des relations internationales tel qu'il n'y a pas de violation de la stabilité internationale ni de menace à la sécurité des États et de la communauté internationale dans le secteur de l'information;

h) *Utilisation illégale des systèmes téléinformatiques et des ressources d'information*. Utilisation des systèmes et ressources téléinformatiques sans autorisation ou en violation des règles applicables, de la législation ou des normes du droit international;

i) *Intrusion dans les systèmes et ressources téléinformatiques*. Intrusion dans les activités de collecte, de traitement, de stockage, de recherche, de diffusion ou d'utilisation de l'information en vue d'entraver le fonctionnement normal des systèmes d'information ou de violer l'intégrité, la confidentialité ou l'accessibilité des ressources d'information;

j) *Structures fondamentales*. Installations, systèmes et institutions d'un État dont les ressources d'information doivent être protégées parce que toute influence délibérée sur ces ressources peut avoir des conséquences directes pour la sécurité nationale (transports, approvisionnement en énergie, crédit et finance, communications, administration, système de défense, organismes chargés de faire appliquer la loi, ressources stratégiques d'information, établissements de recherche et progrès scientifiques et technologiques, installations présentant des risques technologiques et écologiques, et organismes chargés de parer aux conséquences des catastrophes naturelles ou d'intervenir dans des situations d'urgence);

k) *Terrorisme international en matière d'information*. Utilisation des systèmes et ressources d'information ou de télécommunication, ou influence exercée sur ces systèmes ou ressources à des fins terroristes;

l) *Délit international en matière d'information*. Utilisation des systèmes et ressources d'information ou de télécommunication, ou influence exercée sur ces systèmes ou ressources à des fins illicites.

Oman

[Original : arabe]
[22 juin 1999]

43. La Direction des télécommunications du Sultanat d'Oman n'a pas pour mission de fournir des informations aux usagers, mais seulement de mettre à leur disposition des réseaux et des technologies qui facilitent l'accès aux systèmes d'information.

44. En sa qualité de fournisseur de réseaux et de technologies, la Direction est consciente des problèmes que pose la sécurité de l'information. On ne peut écarter le risque que des parties non autorisées détournent les technologies fournies par la Direction pour accéder aux données et que ces intrusions aient des conséquences néfastes.

45. En tant que fournisseur de services de télécommunications, la Direction n'est normalement pas tenue de garantir la sécurité des données des usagers; il incombe à ces derniers d'établir les protections nécessaires. La Direction peut toutefois restreindre l'accès à l'information circulant dans les réseaux publics tels que l'Internet.

46. En ce qui concerne les concepts fondamentaux en matière de sécurité de l'information, l'information a une valeur matérielle et morale et bénéficie donc d'une protection juridique aux termes de la réglementation omanaise, en particulier des règlements concernant les droits d'auteur. Les concepts visés sont les suivants :

a) Interception illicite de données;

b) Intrusion dans les systèmes informatiques;

c) Violation de la confidentialité des données;

d) Violation de la vie privée et du droit à la vie privée;

e) Fourniture de données ou de documents électroniques de tout ordre;

f) Destruction, altération et détournement de données;

g) Collecte et détournement de l'information;

h) Fuite de données;

i) Modification frauduleuse ou contrefaçon de logiciels;

j) Copie illicite de programmes en violation des droits de propriété intellectuelle;

k) Vol et détournement d'adresses de réseau;

l) Altération, ajout ou suppression de données contenues dans un message avant qu'il ne parvienne à son destinataire;

m) Introduction de virus et altération des données circulant sur les réseaux;

n) Destruction matérielle des équipements et des bâtiments.

47. Parmi les moyens de renforcer la sécurité des systèmes informatiques, citons les suivants :

a) Sensibilisation du personnel aux risques et aux techniques de prévention;

b) Contrôle des accès, c'est-à-dire délivrance d'autorisations aux personnes habilitées à utiliser différents types de données;

c) Emploi de codes numériques (signatures et certificats numériques) visant à authentifier les communications entre utilisateurs autorisés;

d) Utilisation de techniques de chiffrement dans les matériels et les logiciels;

e) Emploi de gardes-barrières pour bloquer l'entrée de données qui ont été altérées;

f) Utilisation d'antivirus.

48. Le Sultanat exprime l'espoir que soient mis au point des principes internationaux visant à renforcer la sécurité des systèmes d'information mondiaux, d'autant plus que depuis l'introduction de l'Internet sur son territoire, il est désormais exposé aux dangers qui menacent la sécurité de l'information.

Qatar

[Original : anglais]
[10 juin 1999]

Les autorités compétentes de l'État du Qatar ont communiqué les vues et observations suivantes en application des dispositions énoncées aux paragraphes 2 et 3 de la résolution 53/70 de l'Assemblée générale :

a) *Problèmes généraux en matière de sécurité de l'information*. Un échange de vues entre spécialistes du domaine et une meilleure compréhension du risque d'intrusion et de ses conséquences pour la sécurité et les coûts peuvent permettre de mieux cerner les problèmes existant dans ce domaine;

b) *Définition des concepts fondamentaux en matière de sécurité de l'information*. Les concepts fondamentaux en matière de sécurité de l'information peuvent être ramenés d'une part aux mesures qui doivent être mises en place pour assurer la transmission de l'information et d'autre part aux problèmes qui peuvent se poser (voir aux tableaux 1 et 2 une liste de mesures visant à renforcer la sécurité de l'information à tous les stades et une liste des nouveaux problèmes possibles).

c) *Principes internationaux susceptibles de renforcer la sécurité des communications*. Pour renforcer la sécurité de l'information, il faudrait améliorer les modes de transmission. Compte tenu des coûts élevés, les mesures suivantes semblent s'imposer en priorité :

i) Utilisation de protocoles de communication atypiques spécialement conçus pour l'échange de certaines données;

ii) Adoption de systèmes de codage conçus pour répondre à des objectifs précis et non de programmes disponibles dans le commerce;

iii) Mise au point de programmes exploitant différents modes de synchronisation et de codage.

Tableau 1
Moyens de renforcer la sécurité des réseaux

Mesures de sécurité

Menace	*Solution*	*Fonction*
Interception, lecture ou modification illicites de données	Chiffrement (normes de chiffrement DES, algorithme Rivest, Shamir, Adleman)	Chiffrement des données pour empêcher qu'elles ne soient altérées
Accès d'un utilisateur agréé à des données auxquelles il n'est pas autorisé à accéder	Logiciel de contrôle d'accès	Attribution de droits d'accès aux utilisateurs et gestion de ces droits
Usurpation d'identité à des fins frauduleuses	Authentification	Technique faisant intervenir un logiciel de chiffrement et un mécanisme de validation pour vérifier l'identité de l'expéditeur et du destinataire
Accès d'un utilisateur non autorisé d'un réseau à un autre réseau	Garde-barrière	Mécanisme de filtrage permettant d'empêcher certains utilisateurs de s'introduire sur un réseau ou sur un serveur
Exploitation par un pirate des mécanismes de lacunes de sécurité du système d'exploitation du serveur pour s'introduire sur ce dernier et en altérer les données	Outils livrés avec le système d'exploitation	Programmes permettant de remédier aux lacunes qui ont été identifiées dans le système d'exploitation

Tableau 2
Problèmes potentiels

Les changements	*Les problèmes*
Les réseaux actuels :	*La sécurité est menacée parce que :*
Regroupent un plus grand nombre d'ordinateurs portables	Il est aisé de voler des ordinateurs portables
Font de plus en plus appel à des liaisons sans fil	Il est plus facile de pirater des liaisons sans fil
Raccordent des sites sans cesse plus dispersés	Il est plus difficile de protéger des sites éloignés les uns des autres
Relient des systèmes hétérogènes	Les utilisateurs oublient leurs mots de passe ou les consignent par écrit
Sont de plus en plus connectés à des réseaux publics tels que l'Internet	Les pirates envahissent les réseaux publics
Fonctionnent de plus en plus sous Unix	Unix présente certains points faibles

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

[Original : anglais]
[30 mai 1999]

Généralités

1. Les possibilités d'interconnexion mondiale entre les systèmes informatiques sont telles que des éléments importants des infrastructures de base de la plupart, voire de la totalité des États, peuvent faire l'objet d'attaques informatiques lancées par des criminels et des terroristes. Si ces risques sont probablement faibles à l'heure actuelle, ils vont s'accroître au fil du temps car les secteurs public et privé utilisent de plus en plus des systèmes informatiques interconnectés. En outre, comme les systèmes sont raccordés au niveau international, la menace dépasse les frontières nationales. Les criminels et terroristes qui tentent de s'introduire dans nos systèmes informatiques à des fins malveillantes posent donc un problème à tous les États Membres de l'ONU. En conséquence, le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord est favorable à toutes les initiatives, unilatérales ou multilatérales, visant à étudier les moyens de protéger l'intégrité des systèmes informatiques essentiels.

Mesures nationales

2. En janvier 1999, le Gouvernement britannique a annoncé diverses mesures visant à réduire au minimum les risques d'attaques contre les systèmes informatiques essentiels du Royaume-Uni. Ces mesures sont notamment les suivantes :

a) S'assurer que dans les administrations publiques tous les systèmes essentiels soient répertoriés et que leur protection soit bien assurée;

b) Collaborer avec le secteur privé pour définir des mesures adaptées à l'ampleur des risques pour assurer une protection adéquate des systèmes essentiels qui font partie de l'infrastructure nationale de base;

c) Mieux sensibiliser le secteur privé au problème de la sécurité de l'information et relever les normes dans ce domaine en poursuivant les initiatives visant à promouvoir les meilleures pratiques.

Mesures internationales

3. Étant donné les possibilités d'interconnexion mondiale, les attaques lancées contre les systèmes d'autres États peuvent avoir des répercussions sur l'infrastructure de base britannique et les terroristes et les criminels qui opèrent à partir d'un pays tiers peuvent tenter d'attaquer les systèmes britanniques. En conséquence, le Royaume-Uni estime qu'une coopération internationale est essentielle pour combattre les menaces d'attaques et entend renforcer le dialogue sur ces questions avec ses partenaires internationaux. Il collabore notamment avec le Groupe du G-8 chargé de la criminalité faisant appel à la haute technologie aux fins de la fourniture d'une assistance juridique mutuelle et avec le Conseil de l'Europe aux fins de l'élaboration d'une convention sur la cybercriminalité.

4. Le Royaume-Uni estime que l'Organisation des Nations Unies devrait suivre les travaux de ces entités et d'autres instances en vue de définir en temps voulu le type de contributions concrètes qu'elle pourrait apporter. Elle pourrait notamment élaborer des principes internationaux visant à renforcer la sécurité des systèmes mondiaux et à lutter contre le terrorisme et la criminalité dans le domaine de l'information.