Nations Unies A/56/164/Add.1

Assemblée générale

Distr. générale
3 octobre 2001
Français
Original: russe

Cinquante-sixième session
Point 69 de l'ordre du jour
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

Additif

Table des matières

01-56158 (F) 121001 121001

II. Réponses reçues des gouvernements

Fédération de Russie

[Original : russe]
[21 juin 2001]

Examen général des problèmes liés à la sécurité de l'information

Menaces contre la sécurité internationale dans le domaine de l'information

Au paragraphe 1 de sa résolution 55/28, l'Assemblée générale a demandé aux États Membres de continuer de collaborer à l'examen des dangers réels et des risques dans le domaine de la sécurité de l'information. Dans le projet de document présenté par la Fédération de Russie, intitulé « Principes de la sécurité internationale de l'information » (voir A/55/140, chap. II), les menaces contre la sécurité de l'information sont définies comme étant les facteurs qui risquent de porter atteinte aux intérêts vitaux des individus, de la société et de l'État dans le secteur informationnel.

Parmi ces facteurs, il convient, de l'avis de la Fédération de Russie, de mentionner les suivants :

1. Élaboration, création et utilisation de moyens permettant d'affecter ou d'endommager les ressources informationnelles et les systèmes de télécommunications d'un autre État

- Moyens radioélectriques ou énergo-informationnels utilisés par des unités armées illégales (anticonstitutionnelles), des groupes terroristes et des individus, afin de neutraliser, provisoirement ou de manière définitive, les moyens et systèmes radioélectroniques;
- Moyens permettant d'intervenir dans les programmes des modules de gestion afin de les neutraliser ou de modifier l'algorithme de leur travail;
- Moyens d'agir sur le processus de transmission de l'information en vue de l'interrompre ou de le désorganiser, afin d'altérer la diffusion des signaux et des algorithmes de fonctionnement;
- Moyens de désinformation, création, dans le secteur informationnel, d'une image virtuelle distincte de la réalité ou la déformant;
- Moyens permettant d'agir sur le psychisme et le subconscient des individus en vue de les désorienter ou de réprimer leur volonté ou aux fins d'une neutralisation temporaire des systèmes.

2. Utilisation délibérée de l'information afin d'affecter les structures de base d'un autre État

Il est extrêmement dangereux d'utiliser l'arme informationnelle contre les installations, systèmes et institutions militaires et civils des États, et toute entrave à leur fonctionnement normal constitue une menace directe à la sécurité nationale.

Les intrusions dans les systèmes informatisés de gestion de la distribution d'énergie, par exemple, peuvent provoquer une paralysie complète de l'infrastructure d'approvisionnement d'un pays et, dans le cas des centrales nucléaires, déclencher une catastrophe analogue à la tragédie de Tchernobyl.

L'accès non autorisé à l'information concernant des travaux scientifiques et techniques liés à la défense ou touchant des technologies à double usage peut permettre à des groupes criminels et terroristes de fabriquer de nouveaux types d'armes à des fins criminelles ou de se livrer à des actes de chantage politique.

Les bases de données et autres ressources informationnelles des organes chargés d'assurer le respect des lois peuvent subir des altérations ou être complètement détruites à la suite d'une intervention extérieure, entravant de ce fait considérablement l'administration de la justice et la lutte effective contre la criminalité et compromettant le maintien de la légalité et de l'ordre.

Les interventions visant les ressources informationnelles dans les secteurs financier et bancaire, comme les transferts de fonds illégaux ou le pillage direct des ressources bancaires, l' « annulation » de comptes et le blocage, par des « attaques électroniques » des réseaux informatiques des banques centrales, peuvent, de toute évidence, non seulement créer des situations de crise dans ce domaine précis mais également entraîner l'effondrement de l'économie d'un pays et, partant, provoquer de graves difficultés dans ses relations internationales.

La destruction de l'infrastructure des télécommunications au moyen de l'arme informationnelle entraîne une paralysie des structures administratives et des organes décisionnels.

Toute intervention hostile dans le domaine de l'information visant des systèmes de communication et de contrôle des systèmes de défense antiaérienne et antimissile et autres systèmes de défense désarme l'État face à un agresseur potentiel et l'empêche d'utiliser des moyens légaux à des fins de légitime défense.

De même, la désorganisation délibérée du processus de production peut avoir des conséquences désastreuses sur les entreprises présentant des risques technologiques et écologiques élevés (production chimique, biologique et de combustible).

La désorganisation des moyens de communication, de contrôle et de transport des services chargés de sauver les personnes et d'atténuer les effets des catastrophes naturelles ou d'autres situations d'urgence, peut fréquemment accroître les dégâts matériels et les pertes en vies humaines dans de telles situations.

3. Utilisation de l'information en vue de saper les systèmes politique, économique et social d'autres États et de manipuler psychologiquement la population afin de déstabiliser la société

L'utilisation délibérée de l'information contre un adversaire (concurrent ou opposant) n'est pas un procédé très nouveau. Mais aujourd'hui, du fait de la très vaste diffusion des nouvelles technologies dans le domaine des télécommunications et de la création de réseaux d'information mondiaux, ce moyen d'action acquiert un potentiel qualitativement différent. La possibilité de lancer des actions massives dans le domaine de l'information transfère l'arme informationnelle de la catégorie des moyens auxiliaires dans celle des instruments de combat de première importance.

En même temps, le domaine informationnel devient un facteur systémique fondamental dans la vie de toute société et affecte dans une large mesure pratiquement tous ceux qui constituent la sécurité d'un État. En conséquence, à mesure que les technologies de l'information progresseront, cette dépendance se renforcera. La forte pression résultant de la prédominance d'un nombre limité de sources d'information peut servir à exercer une action psychologique négative sur la population d'un pays, sur le personnel des structures d'importance cruciale, les institutions administratives et gouvernementales et les organes législatifs.

La suggestion d'une incapacité de régler ses propres problèmes, d'une méfiance à l'égard des organes du pouvoir et d'un état de désespoir, la neutralisation de la volonté et la provocation de conflits pour des motifs religieux, ethniques ou d'autres raisons d'ordre social sapent les fondements de l'État et déstabilisent la société. Somme toute, une telle situation peut entraîner une stratification antagonique des groupes sociaux, déclencher une guerre civile ou aboutir à une désintégration complète de l'État.

4. Intrusion dans les systèmes et ressources téléinformatiques et utilisations illégales de l'information

Pratiquement tous les États se heurtent ou sont susceptibles de se heurter aujourd'hui à des problèmes de pénétration dans leurs systèmes d'information, et le nombre de cas de ce genre a nettement tendance à augmenter. Ces intrusions présentent des dangers dans la mesure où elles peuvent avoir toute une série de conséquences néfastes; l'expérience des pirates informatiques sert aux groupes criminels et les « succès » obtenus risquent d'être appliqués au niveau intergouvernemental à des actions nuisibles, d'ordre militaire notamment.

Les conditions actuelles du développement économique et social accentuent les contradictions entre, d'une part, les besoins de la société concernant l'élargissement de l'accès à l'information et sa libre circulation et, d'autre part, la nécessité évidente d'appliquer des limites réglementaires à cet égard.

En même temps, les intrusions dans les systèmes informatiques et les utilisations illégales de l'information – dans la mesure où elles sont prévues dans les dispositions législatives et réglementaires nationales – varient beaucoup et relèvent du domaine administratif et du domaine pénal. D'une manière générale, de nombreux pays ne sont pas entrés dans de telles distinctions.

Ainsi, le délinquant, qui opère à partir du territoire de son pays sur des réseaux informatiques internationaux et ne viole pas les lois nationales, peut rester en dehors de la juridiction de l'État à l'égard duquel l'infraction a été effectivement commise.

Le perfectionnement des moyens techniques de défense des réseaux informatiques peut constituer une solution, mais uniquement dans le cas des États qui possèdent les ressources nécessaires sur le plan technique et surtout financier.

Il est évident que cette situation conduit logiquement à la nécessité de codifier la législation nationale applicable et de créer une base universelle de droit international pour la responsabilité à l'égard des infractions commises.

5. Actions visant à dominer et contrôler le secteur de l'information

Le processus de mondialisation à l'égard du secteur de l'information se caractérise en outre par un niveau accru de normalisation, qui rend plus facile pour les pays ayant une économie développée et une structure informatique avancée la pénétration des marchés des télécommunications des pays en développement. Ceux-ci sont contraints d'adopter ces normes et d'autoriser l'utilisation des nouvelles technologies dans le secteur de l'information. Étant donné la libéralisation du marché de l'informatique et la libre circulation de l' information, ces pays se trouvent dans l'orbe de domination d'autres États, ce qui peut porter atteinte à leur sécurité nationale.

6. Actions visant à empêcher l'accès aux technologies informatiques de pointe et à créer une situation dans laquelle les autres États se retrouvent technologiquement dépendants en la matière

Les raisons qui expliquent la résistance au transfert des technologies de l'information les plus récentes, de même que l'imposition de limites à cet égard, sont manifestement analogues à celles qui concernent toutes les autres technologies de pointe. Ces limitations peuvent, d'une part, être liées à des considérations purement économiques et au désir d'exercer un monopole dans tel ou tel secteur du marché et, d'autre part, correspondre à des motifs politiques (sanctions, ripostes à l'égard de pays « non amis », sécurité nationale, etc.). Dans un cas comme dans l'autre, il n'est pas exclu que l'intention soit de préserver ou de créer une dépendance technologique de certains pays par rapport à d'autres dans le domaine informatique.

Quoi qu'il en soit, au XXIe siècle, il y va de la survie de tous les États d'accéder aux technologies de l'information.

Il faut également prendre en considération le caractère spécifique de la mise au point d'une arme de l'information, qui réside dans le fait que les technologies utilisées à cet effet apparaissent initialement, en règle générale, dans le secteur civil, pour passer ensuite éventuellement dans le domaine militaire.

Compte tenu de ces facteurs, la question de la limitation de l'accès aux technologies informatiques doit être de toute évidence résolue exclusivement sous l'éclairage de l'interdiction de leur emploi en tant qu'arme et de la mise au point, de nouveaux types d'armes de destruction ou de leur utilisation à des fins illicites ou contraires à la sécurité générale. Il convient de considérer comme inacceptable tout autre motif de limitation dans le cadre d'un régime futur de sécurité informatique internationale.

7. Incitation à l'action d'associations, organisations ou groupes terroristes, extrémistes ou criminels ou de malfaiteurs qui constituent une menace pour les ressources téléinformatiques des État et leurs structures essentielles

Le développement sans précédent des systèmes d'information des entreprises, des États et des acteurs internationaux en général et l'élargissement simultané des possibilités d'accès aux réseaux ont atteint un tel niveau que pratiquement tous les membres de la communauté internationale se heurtent aujourd'hui au danger réel d'une agression électronique de la part de criminels et de terroristes. Il est caractéristique que ce danger prendra de l'ampleur à mesure du développement de l'infrastructure mondiale de ces systèmes et acquerra en conséquence un caractère transfrontière.

Aussi bien la criminalité que le terrorisme informatiques constituent des actes illicites, qui se distinguent toutefois par les objectifs poursuivis. Tandis que les pirates informatiques agissent dans un but essentiellement intéressé ou en raison d'une mentalité de voyou, les terroristes opérant dans le secteur informatique sont quant à eux motivés d'une manière générale par des desseins politiques.

Les moyens de concrétiser ces desseins peuvent inclure divers types d'armes de l'information.

En utilisant des logiciels, matériels et technologies spéciaux, les terroristes peuvent :

- Détruire, altérer ou manipuler divers éléments de l'infrastructure informatique;
- Se saisir d'informations importantes;
- Modifier des informations officielles et factuelles pour répondre à leurs propres desseins;
- Saisir ou bloquer les médias afin de pratiquer la désinformation, de diffuser des rumeurs alarmantes, de propager des menaces d'actes terroristes et de faire connaître leurs propres exigences;
- Mettre hors service des systèmes de télécommunications par téléchargement frauduleux;
- Diffuser des menaces d'actes terroristes dans le secteur informatique, entraînant de lourdes conséquences sur les plans politique, économique, social et autres.

La tactique du terrorisme informatique consiste à provoquer des conséquences dangereuses, à faire connaître son existence et à susciter un large écho dans le public. Les systèmes informatiques non protégés offrent malheureusement de très grandes possibilités à cet égard.

8. Élaboration et adoption par les États de plans ou de doctrines ouvrant la voie à une guerre de l'information, et pouvant déclencher une course aux armements et susciter des tensions entre les États, ou risquant de provoquer une véritable guerre de l'information

L'un des principaux objectifs de la stratégie actuelle de nombreux États technologiquement développés en matière de défense consiste à accroître leur puissance informationnelle, ce qui requiert l'existence d'un potentiel d'information tant défensif qu'offensif. Une telle stratégie s'ancre dans des doctrines nationales correspondantes. Compte tenu du renforcement du rôle de la guerre de l'information et des moyens de résistance dans ce domaine, on procède actuellement à une révision des notions traditionnelles concernant les menaces contre la souveraineté nationale, le respect des principes et normes du droit international, la nature de la souveraineté économique et le rôle des États dans les affaires internationales. À ce sujet, une attention croissante est accordée à un nouveau type de conflit, à savoir la guerre stratégique dans le secteur de l'information.

La combinaison de la puissance économique et du potentiel informationnel permet, en renonçant aux formes traditionnelles « cruelles » de coercition par la force militaire, d'influencer, de manière tout aussi efficace, le déroulement d'une situation en politique internationale.

Ces nouvelles stratégies se fondent sur les aspects suivants :

- Le développement des technologies de l'information ne suscite pas, de la part de l'opinion, de réactions négatives aussi vives que l'accroissement des arsenaux d'armements classiques, et en particulier des armes de destruction massive;
- L'appui au développement des systèmes d'information est avantageux, dans la mesure où ces systèmes correspondent le mieux à la notion de technologie à double usage et peuvent souvent être utilisés simultanément à des fins militaires aussi bien que civiles et commerciales;
- Le rôle de premier plan joué par l'État dans l'élaboration et l'application des technologies informationnelles renforce le monopole qu'il exerce sur l'information stratégique et, partant, la possibilité d'intervenir de la manière la plus opérationnelle en cas d'aggravation des tensions internationales.

On estime à ce sujet que l'utilisation de l'arme informationnelle peut réduire sensiblement les pertes en vies humaines et les dommages par rapport aux interventions militaires de type traditionnel. Il est évident que, de la sorte, on s'efforce de donner l'impression que les opérations menées dans le secteur de l'information ont un « caractère humain ».

On comprend toutefois que tous les États connaissent les avantages et les menaces liées au développement des technologies de l'information et qu'ils s'efforceront de réagir de manière adéquate à tout changement de situation. La mise au point de plans et de doctrines concernant la guerre de l'information peut contribuer à augmenter considérablement le nombre de pays dotés d'un arsenal informationnel et, partant, à lancer une course aux armements dans ce nouveau domaine technologique. En fin de compte, la situation en

matière de contrôle des armements peut revenir à celle caractérisant la période de la guerre froide.

9. Utilisation des technologies de l'information et des moyens de communication au détriment des droits de l'homme et des libertés fondamentales dans le domaine de l'information

Dans le domaine de l'information, l'individu doit pouvoir exercer son droit – et être libre – d'accéder à l'information, de l'utiliser aux fins d'une activité légitime, et de son développement spirituel et intellectuel, et avoir la garantie que les informations le concernant et touchant sa famille demeureront confidentielles, de même que la correspondance et les autres échanges par voie de télécommunication et que son honneur et sa dignité seront protégés.

Le développement et la vaste utilisation des technologies de l'information et moyens de communication les plus récents offrent aujourd'hui des possibilités sans précédent concernant la réalisation du droit à l'information. Toutefois, du fait des progrès réalisés dans l'informatisation de la vie sociale et du développement des réseaux d'information, un nombre croissant de données sur la vie personnelle des citoyens devient accessible par le biais de bases de données ouvertes. D'un autre côté, apparaît le danger d'une limitation illégale, par les autorités, de l'accès des citoyens aux ressources informationnelles des organes fédéraux, des services de l'administration locale, des archives et à d'autres informations importantes sur le plan social.

Le futur régime de sécurité de l'information au niveau international devra garantir l'interdiction générale de la collecte, de la conservation, de l'utilisation et de la diffusion d'informations sur la vie personnelle de toute personne sans son consentement, et prohiber la limitation de l'accès des citoyens à l'information, sauf dans les cas prévus par la loi.

10. Diffusion transfrontière de l'information, en violation des principes et règles du droit international et des législations nationales

La mondialisation du secteur de l'information sape les notions traditionnelles de frontières géographiques et nationales et de limites administratives ou de zones de juridiction, liées à la garantie de la sécurité nationale. Dans ces conditions, se pose le problème d'une détermination précise des sources de menaces, et la question de savoir s'il s'agit de sources internes ou extérieures. Par exemple, une intervention militaire contre un autre État dans le domaine de l'information peut être dissimulée sous les agissements de criminels « locaux ».

Autrement dit, les États qui pouvaient auparavant garantir le régime de droit des échanges informationnels sur le plan intérieur se trouvent, dans les nouvelles circonstances, désarmés devant la pénétration sur leur territoire d'informations en provenance de l'extérieur, dont la diffusion est interdite, ou qui ont un caractère destructeur (pornographie, désinformation, informations contenant des éléments de discrimination raciale et d'intolérance, visant à attiser la haine dans les domaines social, national et religieux, ayant un caractère subversif, ou publiées et utilisées au profit de groupes criminels et terroristes internationaux).

11. Manipulation des courants d'information, désinformation et dissimulation de l'information en vue d'altérer l'environnement psychologique et spirituel d'une société, et de saper les valeurs culturelles, morales, éthiques et esthétiques traditionnelles

Le caractère du milieu informationnel et des interventions dans le domaine de l'information peut modifier considérablement la conscience et la conduite collectives des grands groupes sociaux. Un moyen d'action comme la manipulation – type d'action psychologique qui éveille, chez un individu ou un groupe social, des intentions ne correspondant pas à la réalité, présente à ce sujet un danger particulier. Toute situation politique instable et tendue renforce « l'efficacité » de la manipulation de l'information. Le lancement de vastes campagnes de désinformation ou, au contraire, la rétention d'informations réelles dans une telle situation rend impossible toute évaluation objective des événements et des facteurs. C'est l'opinion publique qui est la plus réceptive à ce type d'opération.

Renforcées par la puissance des structures informationnelles actuelles, de telles opérations peuvent entraîner la destruction de l'environnement psychologique d'une société et de ses valeurs culturelles et autres valeurs spirituelles (guerre des cultures). La démoralisation de la société, quant à elle, crée des conditions propices à l'érosion de la conscience nationale et à la neutralisation de la volonté de résister à un agresseur éventuel.