Nations Unies A/60/95/Add.1

Assemblée générale

Distr. générale
21 septembre 2005
Français
Original: anglais

Soixantième session
Point 86 de l'ordre du jour
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

Additif

Table des matières

05-51878 (F) 051005 121005

II. Réponses reçues des États Membres

Brésil

[Original : anglais]
[24 juin 2005]

Lorsque l'on analyse les effets des progrès de l'informatique et de la télématique sur la sécurité internationale, force est de reconnaître, en premier lieu, que la relation entre les sociétés et le progrès technique ne peut se réduire à de simples influences à sens unique; elle repose sur un jeu complexe faisant intervenir les besoins, la créativité, l'esprit d'entreprise et l'utilisation collective des technologies. Le XXI^{e} siècle marque l'aube d'une ère nouvelle, au cours de laquelle l'essor de la « société de l'information » devrait déterminer des transformations profondes dans tous les domaines de l'activité humaine, des interactions entre personnes et sociétés aux schémas de production économique et de gestion des affaires de l'État.

L'information est d'ores et déjà un élément essentiel de la richesse et de la prospérité des nations et on la considère à juste titre aujourd'hui comme l'une de leurs ressources les plus précieuses. Les entreprises privées, les banques, les bourses et les institutions gouvernementales (y compris l'appareil de défense) sont tous reliés par des réseaux informatiques mondiaux qui sont devenus aussi essentiels pour le progrès économique que l'énergie électrique et l'alimentation en eau. Toutefois, ce degré élevé et sans cesse croissant de connectivité crée aussi de nouvelles vulnérabilités potentielles pour les gouvernements et les économies, lesquelles peuvent être exploitées aussi bien dans des conflits militaires que dans des activités criminelles et terroristes.

Au cours des dernières décennies, l'utilisation massive des technologies et de l'automatisation dans les opérations militaires a créé les conditions d'une concentration plus étroite des conflits entre États sur des objectifs militaires et d'un évitement des dommages collatéraux. Dans le même temps, l'influence croissante des médias et de la société civile organisée impose de nombreuses contraintes en matière de conduite des opérations militaires. La guerre moderne est censée être « propre » ou même « chirurgicale ».

Cela cadre bien avec les possibilités concrètes qu'offre la « guerre cybernétique ». Certaines forces armées déploient d'ores et déjà des unités militaires spécialisées, qui sont entraînées et équipées pour neutraliser ou même détruire les infrastructures essentielles en envahissant et sabotant les réseaux informatiques. Selon l'objectif et les moyens employés, les effets de telles attaques peuvent aller de la neutralisation de systèmes d'armes ou de capteurs ennemis à des perturbations cataclysmiques, des réseaux électriques à l'échelle d'un pays. L'efficacité de ce type d'opérations militaires se trouve accrue par le fait que nombre de capacités de ce genre peuvent être constituées moyennant des dépenses relativement réduites. Compte tenu de ces facteurs, la guerre cybernétique pourrait bien devenir dans un avenir proche la première étape des conflits militaires entre États. Les mêmes vulnérabilités pourraient aussi être exploitées par des organisations terroristes avec des conséquences potentiellement encore plus grandes et imprévisibles.

Bien qu'à une échelle moindre quant à l'amplitude des effets, de tels outils informatiques offensifs sont déjà communément utilisés par les criminels : chaque

année, les systèmes informatiques de nombreuses institutions financières, entreprises commerciales et organismes publics font l'objet d'actes de piratage et d'intrusions de la part d'individus ou de groupes cherchant à obtenir illégalement des avantages financiers et/ou des renseignements confidentiels.

Conscient de l'importance de cette question pour le maintien de la paix et de la sécurité internationales, le Brésil propose de l'aborder de deux manières : d'une part, la communauté internationale devrait s'efforcer d'élaborer des outils appropriés pour faire face aux activités criminelles et terroristes faisant appel à l'informatique. D'autre part, de manière complémentaire, elle devrait examiner les effets de l'émergence de la guerre cybernétique et la nécessité éventuelle d'en tenir compte dans les régimes de désarmement et de non-prolifération et le droit international de la guerre.

Considérant la possibilité d'actions terroristes et criminelles, nous proposons que l'ONU amène les États Membres à prendre coopérativement les mesures suivantes :

- Établir des réseaux de secours et de rechange pour protéger les infrastructures essentielles;
- Examiner la structure de leurs réseaux, en en analysant l'interdépendance et identifier des méthodes efficaces de protection;
- Promouvoir les échanges entre secteurs public et privé, dans le but de parvenir au niveau souhaité de sécurité quant aux flux d'informations qui les relient;
- Établir des systèmes de protection pour éviter ou réduire au minimum les effets des attaques cybernétiques;
- Mettre en œuvre des outils et des mesures permettant aux autorités de déterminer l'origine des attaques cybernétiques;
- Habiliter des institutions nationales à tester et évaluer le niveau de sécurité des systèmes informatiques;
- Négocier et adopter une convention internationale sur la cybercriminalité;
- Promouvoir et mettre au point des technologies concernant les moyens et méthodes d'assurer la sécurité informatique;
- Garantir l'accès à l'information et aux technologies de l'information pour l'ensemble du public;
- Éviter d'établir des mécanismes susceptibles d'empêcher des pays d'accéder aux technologies de pointe dans le domaine de la télématique et de l'informatique;
- Créer des procédures de notification mutuelle des menaces cybernétiques entre autorités nationales compétentes;
- Sensibiliser la population à l'importance de la sécurité cybernétique.

En ce qui concerne l'utilisation des armes informatiques dans les conflits entre États, nous estimons que l'ONU devrait évaluer la possibilité de promouvoir la signature de conventions portant sur les sujets suivants :

- Identification, caractéristiques et classification de la guerre informatique;

- Identification et classification des armes informatiques et des moyens utilisables comme armes informatiques;
- Prévention de l'utilisation d'armes militaires ou de connaissances cybernétiques par des groupes terroristes;
- Établissement d'un code de conduite pour l'utilisation des armes informatiques;
- Garantie à tous les États de droits égaux en matière de protection de leur territoire contre les attaques cybernétiques;
- Création de mécanismes internationaux pour la solution des conflits liés à des agressions cybernétiques;
- Établissement d'un glossaire de l'ONU contenant les définitions des principaux termes relatifs à la sécurité informatique.

Canada

[Original : anglais]
[4 août 2005]

L'infrastructure informatique est un élément essentiel de l'infrastructure critique du Canada, laquelle englobe les secteurs suivants : énergie et services, télématique et informatique, finances, soins de santé, alimentation, eau, transports, gouvernement et industrie manufacturière. Les défis que pose la sécurité de l'infrastructure informatique sont les mêmes pour tous les secteurs, dont 90 % peuvent être entre les mains du secteur privé ou opérés par lui. L'importance de l'infrastructure informatique canadienne pour l'ensemble des Canadiens a amené le Gouvernement à œuvrer au maintien de la sécurité, de la disponibilité et de l'intégrité de ses systèmes, à prendre des mesures pour prévenir les incidents cybernétiques et à réagir rapidement à toutes les perturbations signalées.

En décembre 2003, le Premier Ministre a annoncé la création d'un nouveau Ministère de la sécurité publique et de la protection civile, qui regroupe l'ancien Bureau de la protection des infrastructures essentielles et de la protection civile, la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité, qui sont trois des principaux services fédéraux ayant des responsabilités dans le domaine de la sécurité cybernétique. Le nouveau ministère est chargé de suivre et d'analyser les menaces cybernétiques à l'encontre des systèmes publics, et constitue le point central pour signaler les incidences cybernétiques; il est aussi chargé d'alerter les ministères en cas de menaces et vulnérabilités nouvelles. Le Service du renseignement de sécurité est chargé d'enquêter sur les incidents qui constituent une menace pour la sécurité nationale. La Gendarmerie est chargée d'enquêter sur tout incident cybernétique à caractère criminel ou potentiellement criminel. En outre, le Centre canadien de la sécurité des communications est l'agence technique responsable de l'élaboration des normes opérationnelles pour la certification et l'accréditation des systèmes, les analyses de risque et de vulnérabilité, l'évaluation des produits, la sécurité des systèmes et l'analyse de la sécurité des réseaux.

En avril 2004, le Canada a publié sa première *Politique de sécurité nationale*, qui définit une stratégie et un plan d'action intégrés visant à faire face aux menaces actuelles et futures. Ce plan confirme spécifiquement que la sécurité cybernétique constitue un défi sur le plan de la sécurité publique et propose l'établissement d'une cellule nationale de haut niveau chargée de la sécurité cybernétique où seront représentés les secteurs public et privé en vue de l'élaboration d'une stratégie nationale de la sécurité cybernétique. Cette cellule est en cours de formation.

En février 2005, le Ministère de la sécurité publique et de la protection civile a créé le Centre canadien de réponse aux incidents cybernétiques, qui est chargé de coordonner au niveau national les réactions aux incidents mettant en cause la sécurité cybernétique et de surveiller la situation en matière de menaces cybernétiques. Le Centre opère depuis le Centre d'opérations du Gouvernement, lequel fonctionne 24 heures sur 24 dans le cadre du Système national d'intervention en cas d'urgence (SNU).

Les provinces et territoires canadiens concentrent leur attention sur la protection de leurs propres infrastructures essentielles, notamment les systèmes et réseaux cybernétiques dont ils dépendent. Des initiatives ont été lancées au niveau interprovincial, notamment pour l'établissement d'une capacité de surveillance cybernétique conjointe.

Le secteur privé participe activement aux initiatives en matière de sécurité cybernétique. Les entreprises privées protègent leurs propres infrastructures informatiques essentielles et, par le biais d'associations professionnelles, échangent des renseignements sur les vulnérabilités, incidents et solutions d'ordre cybernétique concernant leurs secteurs. Ces associations collaborent avec le Ministère dans le cadre d'un forum qui permet un vaste échange de renseignements entre les divers secteurs d'activité industrielle.

Le Canada a également pris part à des initiatives multilatérales dans le domaine de la sécurité cybernétique. On peut citer le Sous-Groupe du G-8 sur la criminalité liée à la haute technologie, qui a été créé en 1997 et a adopté 10 principes de lutte contre la criminalité liée à l'informatique, la Convention relative à la cybercriminalité du Conseil de l'Europe qui vise à harmoniser les législations nationales pour ce qui est de la qualification des infractions et des procédures d'enquête et de poursuite dans le contexte des réseaux mondiaux et à rétablir un système rapide et efficace de coopération internationale, et l'Organisation des États américains (OEA), dont les membres sont convenus « d'envisager l'élaboration d'instruments juridiques et de législations modèles pertinents au niveau interaméricain afin de renforcer la coopération régionale dans la lutte contre la cybercriminalité, et d'envisager ce développement de normes en matière de confidentialité, de protection de l'information, de procédures et de prévention du crime ».