ANNEXE VII

PROPOSITION SOUMISE AU
GROUPE D'EXPERTS GOUVERNEMENTAUX SUR LA CYBERCRIMINALITÉ

Document de travail présenté par la
Mission permanente des États-Unis d'Amérique

I. CONTEXTE

Selon une société de recherche concernant Internet, la population mondiale branchée sur ce réseau atteindra 709,1 millions de personnes en 2004, alors que, l'année passée, elle s'établissait à 445,9 millions de personnes. On prévoit que la croissance de la population d'internautes proviendra principalement des pays en développement. En particulier, l'Amérique latine devrait contribuer à cette croissance pour près de 40% annuellement entre 2000 et 2004. On observe une tendance similaire dans les pays des Caraïbes. Internet, et les réseaux et technologies connexes, ont provoqué une croissance spectaculaire dans l'économie mondiale et permis des gains énormes aux chapitres de l'efficacité, de la productivité et des communications. Dans de nombreux États membres de l'OEA -- particulièrement dans les pays où les industries liées à Internet sont encore naissantes et où les lois relatives aux crimes informatiques sont dépassées ou non existantes -- il existe un besoin urgent d'assistance technique pour cerner efficacement ces problèmes et favoriser l'expansion de l'utilisation d'Internet.

II. VERS LA MISE EN PLACE DE RÉSEAUX PROTÉGÉS ET FIABLES

Les pays en développement, partout dans le monde, considèrent à juste titre Internet comme un outil potentiellement utile pour favoriser le développement économique et humain. En même temps, toutefois, des criminels tels que les pirates informatiques, les groupes criminels organisés et les terroristes se servent d'Internet pour commettre et faciliter leurs crimes. La cybercriminalité nuit aux consommateurs, aux entreprises et aux gouvernements : les consommateurs hésitent à transmettre des données personnelles et des données relatives à leurs cartes de crédit par le biais d'Internet parce qu'ils ont des craintes au sujet de la protection de leurs renseignements personnels; les entreprises s'exposent à des pertes importantes de données protégées par des droits exclusifs, de propriété intellectuelle et d'accès en ligne à des clients et à des fournisseurs en raison de défaillances dans le système de sécurité, et les services gouvernementaux peuvent être perturbés par des intrusions dans leurs systèmes informatiques. Sans lois et règlements appropriés, et sans coopération entre gouvernements et entre les secteurs public et privé, les pays qui ne sont pas dotés d'une législation adéquate constitueront des sanctuaires pour les criminels qui utilisent Internet pour commettre ou pour faciliter leurs crimes. De plus, l'absence d'un cadre légal adéquat -- surtout en ce qui concerne la sécurité de l'information et de l'infrastructure et la criminalité informatique -- empêchera les pays en développement de tirer profit des possibilités offertes par Internet, où freinera leurs progrès en ce sens.

Pour qu'Internet contribue à la croissance économique, au développement humain et à la démocratisation, il faut que l'accès au réseau soit protégé et fiable. L'absence de fiabilité et de sécurité porte préjudice à de nombreux objectifs de développement, tels: la croissance du commerce électronique; l'expansion des investissements étrangers; l'établissement d'infrastructures essentielles fiables, et la protection de la vie privée et des données protégées par des droits exclusifs.

Tout cadre légal visant à assurer la fiabilité et la protection des réseaux informatiques doit comporter deux éléments:

1. **Droit substantiel en matière de criminalité informatique.** Chaque pays devrait ériger en infractions au droit criminel les attaques visant la sécurité et l'intégrité des systèmes informatiques -- piratage, interception illégale, interférence avec la disponibilité de systèmes informatiques, et vol et sabotage de données.

2. **Droit de procédure pour la collecte de preuves électroniques.** Chaque pays doit également se doter de procédures claires, conformes aux normes internationales, pour permettre au gouvernement d'avoir accès aux communications et aux données mises en mémoire lorsqu'il en a besoin dans le cadre d'une enquête criminelle. Il est tout aussi important -- surtout dans les pays qui émergent de régimes légaux caractérisés par l'arbitraire, l'absence de primauté du droit, ou la répression -- que les entreprises et les consommateurs soient assurés que le gouvernement ne surveillera pas indûment leurs communications, et que les consommateurs soient certains que les données fournies aux commerçants ne seront pas utilisées à mauvais escient. Le droit des États-Unis constitue un modèle important.

III. PROPOSITION POUR UNE FORMATION RÉGIONALE EN MATIÈRE DE CYBERLÉGISLATION

Nous proposons que l'OEA, par l'intermédiaire du Groupe d'experts gouvernementaux sur la cybercriminalité, cible les États membres en développement en vue de la fourniture d'une assistance théorique et technique. Ce programme aidera les États membres de l'OEA à établir des lois et règlements relatifs à la cybercriminalité et à la cybersécurité, ou à améliorer les lois et règlements existants. Une telle assistance fournirait une base pour accroître la disponibilité des technologies de l'information et des communications (TIC) dans ces pays et pour encourager l'utilisation de ces TIC. Le programme sera axé sur la nécessité de mettre en place 1) un droit substantiel approprié pour décourager le mauvais usage criminel des réseaux informatiques et les attaques contre ces réseaux, et 2) un droit de procédure approprié pour régir l'accès du gouvernement à l'information dans le cadre d'enquêtes sur toutes sortes de crimes « assistés par ordinateur » et dans le cadre de mesures visant à empêcher de tels crimes.

À partir de l'automne 2003, les États-Unis fourniraient du matériel de formation, tiendraient des ateliers régionaux et des consultations, et offriraient une assistance technique pour l'élaboration de politiques gouvernementales et de lois qui contribueraient à assurer la fiabilité et la sécurité des systèmes de communications et d'information. Le Secrétariat de l'OEA aiderait à coordonner les efforts de sensibilisation. La collaboration serait axée sur la modernisation des lois et règlements afin de permettre aux pays de mieux relever les défis des technologies des communications numériques mondiales. Par le biais d'ateliers régionaux, le programme aidera les responsables des États membres de l'OEA en développement à comprendre la nécessité d'aborder les problèmes de la cybercriminalité d'une manière qui suscite la confiance des entreprises, des particuliers et des gouvernements et qui facilite la coopération entre les pays confrontés à des incidents internationaux faisant intervenir les ordinateurs et les réseaux. L'un des principaux objectifs de ce programme est de faire connaître aux États membres de l'OEA en développement les lois pénales et les mécanismes de protection de la vie privée nécessaires pour protéger leurs systèmes d'information et susciter la confiance des utilisateurs de ces systèmes.

Les ateliers régionaux seraient organisés de manière à encourager une forte participation des États membres de l'OEA. À cette fin, nous examinons diverses options pour obtenir des fonds afin de financer la tenue des ateliers et d'aider les États membres à envoyer des participants.