UNITED NATIONS INFORMATION SERVICE

Douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale

Salvador (Brésil), 12–19 avril 2010

Ce document est destiné à l'information; il ne constitue pas un document officiel

UNIS/CP/605F
13 avril 2010

Comité II 2e & 3e séances
Matin & après-midi

LES DÉLÉGATIONS S'INTERROGENT SUR LA PERTINENCE D'UN NOUVEL INSTRUMENT INTERNATIONAL POUR LUTTER CONTRE LA CYBERCRIMINALITÉ

SALVADOR, 13 avril (Service d'information des Nations Unies) – Les délégations, réunies aujourd'hui dans la salle du Comité II du Centre de Conférences de Salvador, ont poursuivi l'examen entamé hier des moyens à privilégier pour renforcer la lutte contre un phénomène que le Secrétariat de l'ONU considère comme l'un des plus grands défis du monde moderne : la cybercriminalité.

À l'occasion d'un atelier thématique portant sur les « tendances récentes dans l'utilisation de la science et de la technique par les délinquants et par les autorités compétentes pour lutter contre la criminalité, notamment la cybercriminalité »*, une dizaine de pays ont ainsi partagé leurs initiatives nationales et souligné la nécessité de renforcer l'assistance technique en direction des pays en développement. Les intervenants ont exprimé des positions divergentes sur la nécessité d'élaborer ou non un nouvel instrument international de lutte contre la cybercriminalité, qui viendrait compléter la Convention de Budapest sur la criminalité adoptée en 2001 par le Conseil de l'Europe.

Premier texte international établi dans le cadre de la lutte contre ce fléau, la Convention a pour principal objectif d'encourager les États parties à prendre des mesures en matière pénale pour assurer une protection effective contre la cybercriminalité, notamment par l'adoption d'une législation appropriée et le renforcement de la coopération entre États

Pour le représentant de l'Espagne, qui parlait au nom de l'Union européenne, le renforcement de l'arsenal juridique international de lutte contre la cybercriminalité ne passe pas nécessairement par l'élaboration d'un autre mécanisme. Il a en effet estimé que l'utilisation des dispositions de procédure de la Convention de Budapest pour contrecarrer la fraude informatique, la pornographie impliquant des enfants ainsi que des infractions liées à la sécurité des réseaux, dépendait d'abord de la volonté politique des États.

« La Convention fixe le cadre dans lequel nous pouvons déjà coordonner les actions nationales et régionales », a-t-il fait remarquer, en invoquant l'importance de doter les pays les moins avancés, qui sont « par définition plus vulnérables que les autres à la criminalité organisée, de moyens technologiques de lutte adaptés à l'évolution de la cybercriminalité.

« Les populations de ces pays veulent qu'Internet contribue à leurs efforts de développement et non pas qu'il renforce les réseaux de corruption, de blanchiment d'argent et de pornographie impliquant des enfants », a-t-il affirmé.

« Détection, répression, renforcement des capacités et de la formation des personnels de police et des ministères compétents : ce sont les axes que privilégie la Pologne dans le cadre de sa plateforme sur la sécurité du territoire », a fait savoir de son côté le représentant polonais. Il a insisté sur la nécessité d'impliquer ensemble les secteurs d'activités de l'État et de la recherche compétents ainsi que les entreprises pour barrer la route aux cybercriminels, « qui ont actuellement un temps d'avance en matière technologique ».

« Notre plateforme tient ainsi compte de l'avis et de l'expertise des criminologues et entreprises spécialisées dans la conception de logiciels à double usage, sécuritaire et sanitaire, pour améliorer l'action politique, endiguer les attaques informatiques et la menace terroriste et mettre au service du grand public des innovations de pointe », a-t-il également précisé.

Il a aussi proposé aux délégations qui le souhaitent, de leur transmettre des recommandations fondées sur l'expérience de la Pologne en matière de lutte contre la cybercriminalité et sur les discussions sur la question qui se sont tenues dans le cadre du Conseil de l'Europe.

Le représentant de la République de Corée a, quant à lui, indiqué que son pays se concentrait sur la prévention des actes cybercriminels. « D'un point de vue politique, il faut mettre l'accent sur la nécessité de préserver les formidables avancées sociales et économiques que représentent les nouveaux réseaux d'information », a-t-il estimé. Il a cependant reconnu l'urgence de freiner le développement d'infractions qui permettent à leurs auteurs de circuler sans entrave dans le temps et dans l'espace. »

« La réglementation de l'espace cybernétique est indispensable pour empêcher que l'Internet ne continue de générer de nouveaux types de violations difficiles à appréhender et qui, comme la diffamation, le vol d'identité et les crimes sexuels, sont particulièrement traumatisantes pour les individus qui en sont victimes », a-t-il poursuivi. Il a par ailleurs évoqué la mise en place d'un Centre national coréen concentrant différents services, militaires et de police scientifique notamment, qui est chargé d'anticiper et d'enrayer les tentatives d'attaques électroniques contre les particuliers, les banques, les entreprises ou l'État. « Le concours technique de l'Office des Nations Unies contre la drogue et le crime (UNODC) a été précieux pour créer ce Centre », a-t-il indiqué avant de plaider en faveur de négociations sur un instrument international de lutte contre la cybercriminalité.

« Comment stopper plus d'un million d'ordinateurs qui sont utilisés chaque jour à des fins criminelles? », a demandé le représentant de l'Azerbaïdjan. Le nombre croissant de banques virtuelles, a-t-il estimé, explique l'avènement et l'aggravation de la cybercriminalité, qui, selon lui, est « un fléau qui ne peut être combattu qu'à travers des programmes communs. » « La cybercriminalité, en menaçant les systèmes bancaires des pays en développement, fragilise ainsi les avancées économiques qui avaient permis à ces pays de sortir du sous-développement », a-t-il constaté. Appuyant le renforcement de la Convention de Budapest pour « harmoniser les pratiques nationales les plus efficaces », le représentant a en outre souligné qu'il était nécessaire de moderniser le fonctionnement des polices nationales en recourant à l'expertise d'INTERPOL.

« N'oublions pas aussi de sensibiliser les familles qui utilisent Internet aux dangers de cette technologie », a réagi la représentante du Mexique, qui a préconisé de renforcer les mécanismes d'examen de mise en œuvre de la Convention de Budapest, « avant d'envisager l'élaboration d'un nouvel instrument juridique international ». « Nous devons assurer une utilisation optimale des instruments dont nous disposons, en tenant d'abord compte de ce qui fonctionne le mieux pour chaque pays », a-t-elle ainsi renchéri.

Le représentant de l'Indonésie a appuyé les propos de son homologue mexicain en appelant les États à mieux éduquer les utilisateurs privés et institutionnels d'Internet. La première mesure de prévention nationale qui doit être prise par les États doit viser à prendre conscience de l'impact potentiel de la cybercriminalité sur le tissu social, a-t-il estimé.

Concernant l'assistance technique en direction des pays en développement, il a appelé les fournisseurs de services d'Internet à faciliter le développement du réseau informatique dans ces pays. Il a appuyé l'idée d'élaborer un nouvel instrument international sur la cybercriminalité pour assurer une meilleure coopération dans ce domaine et souhaité que le rapport final du douzième Congrès sur la prévention du crime et la justice pénale prévoie une recommandation en ce sens.

La délégation colombienne a mis l'accent sur certaines mesures prises au niveau national, comme la création d'unités spécialisées. Il convient également, selon elle, d'utiliser la Convention de Budapest comme modèle. La cybercriminalité doit être combattue au niveau mondial, a-t-elle poursuivi.

L'Afrique du Sud a insisté sur la nécessité de mettre en place un système modernisé et doté de ressources adéquates. La lutte contre la cybercriminalité, a-t-il dit, a été identifiée par le Gouvernement sud-africain comme une priorité stratégique. Il faut, a-t-il préconisé, développer les compétences techniques au moyen de la coopération régionale et internationale et établir une législation qui couvre tous les aspects de la cybercriminalité. L'Afrique du Sud a appuyé l'appel du Botswana et de l'Angola en vue de fournir une assistance aux pays en développement concernant le renforcement de leurs capacités.

La représentante de l'Inde a estimé que bien que la coopération fût souhaitable et requise, il n'en demeure pas moins que celle-ci ne peut à elle seule tout résoudre. Certaines des questions sont fondamentales et méritent d'être traitées, a-t-elle expliqué, exprimant par exemple ses

préoccupations face à la publication et à la transmission de contenus pornographiques, punissables en Inde à la différence de bien d'autres pays. Elle a estimé qu'un examen approfondi des normes internationales en vigueur était nécessaire dans la perspective de l'élaboration d'une convention internationale efficace destinée à prévenir ou réduire la cybercriminalité.

Le représentant du Pérou a étendu le champ des questions débattues à celle de la protection du patrimoine culturel. Il a en outre indiqué que les autorités judiciaires péruviennes proposaient de retenir l'éducation comme outil principal de prévention.

Son homologue du Zimbabwe a affirmé que son pays avait besoin d'un appui sous forme de ressources financières et d'assistance technique afin de développer ses capacités nationales en matière de lutte contre la cybercriminalité. Un engagement ferme et convaincu de tous les pays est nécessaire pour renforcer la coopération régionale et internationale dans la lutte contre ce fléau, a-t-il dit. Il a cependant fait remarquer qu'un instrument juridique international tel qu'une convention ne devrait pas faire double emploi avec les mesures prises aux niveaux régional et national en vigueur mais, au contraire, devrait encourager leur utilisation.

L'Association internationale des procureurs a, quant à elle, préconisé l'adoption d'une approche prudente dans tout travail destiné à élaborer un nouvel instrument afin d'éviter de saper tout mécanisme existant dans ce domaine.

La délégation d'Oman a considéré, de son côté, qu'une convention internationale sur la cybercriminalité permettrait d'établir les bases nécessaires d'une coopération internationale.

Le représentant du Brésil s'est, lui aussi, déclaré favorable à l'élaboration d'un instrument international placé sous les auspices des Nations Unies, en se concentrant sur la nécessité de combler la fracture numérique entre les pays développés et les pays en développement.

* *** *