Nations Unies A/CONF.203/L.4/Add.4

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

Bangkok, 18-25 avril 2005

Distr.: Limitée
23 avril 2005

Français
Original: Anglais

Rapport du Comité II: point 5 de l'ordre du jour et Ateliers 4, 5 et 6

Additif

Atelier 6: Mesures de lutte contre la criminalité liée à l'informatique

Délibérations

1. Aux 9e et 10e séances du Comité II, les 22 et 23 avril 2005, s'est tenu l'atelier 6 intitulé " Mesures de lutte contre la criminalité liée à l'informatique", organisé en coopération avec l'Institut coréen de criminologie. Le Comité était à cette occasion saisi des documents ci-après:

a) Document de travail relatif à l'atelier 6: Mesures de lutte contre la criminalité liée à l'informatique (A/CONF.203/14);

b) Guide de discussion (A/CONF.203/PM.1);

c) Rapports des réunions préparatoires régionales du Congrès (A/CONF.203/RPM.1/1, A/CONF.203/ RPM.2/1, A/CONF.203/RPM.3/1 et Corr.1 et A/CONF.203/RPM.4/1).

2. À la 1re séance, le 22 avril, un représentant du Secrétariat a fait une déclaration liminaire, qui a été suivie d'une déclaration de l'observateur de l'Institut coréen de criminologie. Le Secrétaire permanent du Ministère thaïlandais des technologies de l'information et de la communication a fait un discours liminaire. Des exposés ont été faits sur la théorie et la pratique de la cybercriminalité. Au cours des débats, des déclarations ont été faites par les représentants du Canada, de l'Ukraine, de l'Autriche, de la Jamahiriya arabe libyenne, de la France, de l'Espagne, du Royaume-Uni, de l'Argentine, du Maroc et du Chili. Des déclarations ont également été faites par trois experts qui participaient au Congrès à titre personnel.

3. À la 2e séance, le 23 avril, des exposés ont été faits qui portaient sur les ressources et la coopération internationale dans la lutte contre la cybercriminalité. Au cours des débats, des déclarations ont été faites par les représentants de l'Italie,

V.05-83705 (F) 240405 240405

de l'Égypte, du Canada, de la Jamahiriya arabe libyenne, de l'Algérie, des États-Unis d'Amérique, du Royaume-Uni et de l'Argentine. Une déclaration a également été faite par l'observateur d'ECPAT International.

Débat général

4. Dans sa déclaration liminaire, le représentant du Secrétariat a donné des informations générales sur l'atelier et fait l'historique des activités de l'ONU pour ce qui est du domaine plus général de la prévention de la cybercriminalité et de ses liens avec la société de l'information, y compris les apports qui seront faits à la seconde partie du Sommet mondial sur la société de l'information qui se tiendra à Tunis du 16 au 18 novembre 2005. L'observateur de l'Institut coréen de criminologie a souligné que l'atelier serait un forum important pour favoriser la coopération internationale.

5. Au cours de l'atelier, les intervenants ont jugé qu'il importait de réagir de façon efficace aux problèmes que posait la cybercriminalité; ils ont constaté qu'elle évoluait rapidement et que les infractions y relatives étaient très diverses. On a fait observer que l'expansion du commerce électronique augmentait dans des proportions extraordinaires les possibilités d'un usage criminel. Deux experts ont exposé les nouvelles tendances de la cybercriminalité et les nouvelles menaces qu'elle faisait peser. Un certain nombre de faits nouveaux illustraient la complexité toujours plus grande de la cybercriminalité, notamment la rapidité avec laquelle les nouveaux virus et parasites informatiques se propageaient pour infecter des millions d'ordinateurs dans le monde entier en peu de temps, le développement de nouveaux outils de piratage, plus puissants et plus faciles à exploiter, la montée du "phishing", qui consiste à envoyer des courriels provenant de pages Web conçues de manière à apparaître comme des sites commerciaux légitimes, la propagation de fausses nouvelles et le vol électronique de données relatives aux cartes de crédit et à d'autres informations personnelles. On a souligné que les nouvelles formes de technologie ouvraient la voie à de nouvelles formes d'agissements criminels, y compris l'exploitation de réseaux sans fil. Les progrès de la cryptographie et de la stéganographie permettaient aux particuliers de dissimuler leur identité en ligne ou d'usurper celle d'un autre. Un nouveau phénomène a été signalé: l'association de diverses activités répréhensibles aux fins d'une seule entreprise criminelle (par exemple, le "phishing" conjugué à l'utilisation d'une fausse identité et à l'extorsion).

6. Les participants ont débattu divers aspects de la fracture numérique. D'emblée, il a été constaté que cette notion recouvrait davantage que l'écart entre pays développés et pays en développement. Les travaux de recherche présentés lors de l'atelier ont fait apparaître un regroupement de pays informatisés entre les deux extrêmes de la fracture numérique. Il semblait que cette fracture se réduise dans la mesure où les pays qui se situaient au milieu de l'échelle faisaient des progrès rapides. Toutefois, ceux dont les infrastructures informatiques et technologiques étaient médiocres se retrouvaient en queue du peloton. En bref, la fracture s'aggravait au bas de l'échelle. On a noté que le caractère émergent de cette fracture ouvrait de nouvelles voies à la cybercriminalité. Ainsi, les pays du bas de l'échelle étaient utilisés comme tremplin pour des attaques ou comme plaque tournante pour brouiller les pistes. De plus, dans les pays où la fracture se réduisait rapidement, les consommateurs étaient plus exposés à des infractions telles que l'escroquerie au

télémarketing, le “phishing” et l’escroquerie aux ventes aux enchères en ligne. Il a été noté que lorsque les pays investissaient dans des technologies destinées à perfectionner les infrastructures publiques et autres infrastructures d’importance cruciale, comme dans la téléphonie mobile, ceci créait de nouveaux risques. Il également été noté que les différents secteurs d’un pays donné – tels que la nouvelle classe moyenne, le secteur privé de la haute technologie ou les pauvres ayant accès depuis peu au système bancaire – seraient exposés à différentes formes de criminalité si, dans ce pays, les autorités n’avaient pas les moyens d’y faire face. Pour toutes ces raisons, il était de la plus haute importance d’élaborer des cadres juridiques et de développer des compétences adéquates dans les pays en développement.

7. De nombreux participants ont souligné que la cybercriminalité évoluait à pas de géant et qu’il fallait que les services de répression et le secteur privé aient un temps d’avance sur les auteurs des infractions. Plusieurs intervenants ont souligné l’importance de l’échange d’informations sur les nouvelles tendances de la cybercriminalité et les nouvelles menaces de vulnérabilité qui en résultaient. Des participants ont rapporté les données d’expérience enregistrées dans des pays où les tendances de la cybercriminalité étaient observées. À cet égard, plusieurs intervenants ont insisté sur la nécessité de prévenir ce type de criminalité. L’une des mesures les plus importantes à prendre concernait la sensibilisation des services de répression, des milieux des affaires et des victimes potentielles. Un exposé fait par l’observateur d’Interpol a fait ressortir l’importance de la collecte, de l’analyse et de l’échange de données, notamment pour ce qui était de l’échange d’images pédophiles sur l’Internet. D’autres propositions ont été faites concernant la collecte de données et le suivi, y compris l’élaboration d’indicateurs et de critères à retenir pour surveiller le contenu des sites Web. Un orateur a proposé de créer, pour partager les données d’expérience et les connaissances les plus récentes, un réseau international d’experts.

8. Les participants ont examiné l’impact, en particulier celui de la fraude et de l’exploitation sexuelle, que la cybercriminalité avait sur les victimes. Un intervenant a souligné qu’il faudrait accorder une attention particulière au problème de l’exploitation sexuelle en ligne des enfants. Il a été proposé que l’industrie informatique combatte ce type de criminalité en sensibilisant l’opinion et en fixant de nouvelles normes de protection. Il a été avancé qu’il faudrait rechercher davantage les moyens de protéger et d’aider les victimes, y compris pendant les enquêtes, en particulier dans les cas d’exploitation sexuelle et de diffusion de documents pornographiques sur Internet. Il est ressorti de la discussion qu’il subsistait plusieurs zones floues, notamment la suite à donner aux images pornographiques créées numériquement et la difficulté qu’il y a à déterminer l’âge des victimes en cas de pornographie mettant en scène des enfants. On s’est interrogé, en outre, sur les activités qu’il faudrait incriminer. Dans le cas de la pornographie, par exemple, la question était de savoir s’il fallait incriminer le fait de visionner l’image ou celui de la stocker électroniquement.

9. Il a été souligné que la cybercriminalité avait un impact non seulement sur les individus, mais aussi sur les entreprises, les organisations, les gouvernements et l’ensemble de la société. La cybercriminalité représentait souvent une menace pour l’infrastructure critique qui, dans de nombreux pays, n’était pas contrôlée par le secteur public. Ce type de criminalité pouvait donc avoir des effets déstabilisants

sur tous les membres de la société. Ainsi, la technologie numérique pouvait aussi être utilisée à des fins terroristes.

10. Un participant a proposé qu'il soit réalisé un inventaire du niveau et des moyens technologiques dont disposent les pays pour faire face à la cybercriminalité. Il a aussi été proposé de créer, sous l'égide de l'ONUDC, un forum virtuel d'experts facilitant l'échange d'informations sur les nouvelles tendances et approches de la cybercriminalité. S'agissant de la recherche sur la cybercriminalité, il a été avancé que de nombreuses questions, y compris l'ampleur de l'implication des groupes criminels organisés, restaient sans réponse. Il faudrait approfondir les recherches dans ces domaines de façon à pouvoir déterminer les futurs risques d'activité criminelle. Il a été déclaré que même dans les pays développés, il n'y avait que relativement peu d'experts qui travaillaient dans ces domaines et que des initiatives telles qu'un réseau de recherche en ligne, soutenu par des organisations internationales et par le secteur privé, faciliteraient l'échange d'informations, l'analyse comparative et le transfert de connaissances.

11. Il a été noté que les pays devraient, pour pouvoir combattre efficacement la cybercriminalité, remplir quatre conditions: disposer de spécialistes de la cybercriminalité; pouvoir faire appel à ces derniers 24 heures sur 24; assurer une formation continue, y compris la formation de spécialistes d'autres pays; et disposer de matériel moderne. Le respect de ces conditions améliorerait aussi la qualité de la coopération interétatique.

12. De l'avis général, il faut accorder la priorité à l'offre d'assistance technique aux pays en développement. Cette assistance pourrait prendre différentes formes, comme l'offre de personnels expérimentés et de conseils par les États Membres et par le secteur privé; la mise au point de cours et de documents de formation; et l'adoption de mesures visant à faire en sorte que les agents des services de répression soient bien informés des progrès technologiques. Le Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique[1], publié en 1994, a été loué comme étant un outil utile. Cependant, a-t-il été souligné, il était urgent de disposer de documents nouveaux et actualisés. Plusieurs orateurs ont évoqué les activités bilatérales menées en matière d'assistance et de formation. L'un des points importants soulignés par de nombreux orateurs a été la nécessité de développer les compétences pour ce qui est de rassembler et d'utiliser les preuves de cybercriminalité. Lors d'un débat sur la mise au point de matériel de formation, il a été déclaré qu'il faudrait adapter la formation des praticiens de justice pénale et la dispenser sous une forme qui soit facilement accessible. S'il était indispensable que les fonctionnaires de police spécialisés et les procureurs reçoivent une formation, il fallait de plus en plus que tous les enquêteurs et agents des services de répression aient une connaissance plus poussée de certains aspects de la cybercriminalité, en particulier pour ce qui est de la conservation des preuves. Il a également été proposé d'étendre la formation, en particulier dans les pays en développement, aux législateurs et aux responsables politiques.

13. Des orateurs ont souligné la nécessité de mettre en place, avec le secteur privé, un partenariat pour formuler et appliquer des mesures efficaces de lutte contre la cybercriminalité. Selon plusieurs praticiens, il faudrait développer les relations entre le monde commercial et les services de répression, non seulement pour réduire le niveau de cybercriminalité, mais aussi pour accélérer sa répression. Il a été souligné que le rôle des secteurs public et privé, y compris les fournisseurs d'accès à

l'Internet, dans la lutte contre la cybercriminalité évoluait constamment. Une stratégie de partenariat pourrait comprendre les activités suivantes: aide accordée par les entreprises pour déterminer les domaines dans lesquels la législation est insuffisante; développement des moyens, par exemple en proposant une formation aux services de répression et en sensibilisant aux nouvelles tendances et technologies; collaboration avec les services de répression aux fins d'enquêtes et partage d'informations générales; éducation des consommateurs sur les questions de sûreté en ligne; introduction d'éléments préventifs tels que des mécanismes de sécurité dans les produits; et mesures incitant le public à se renseigner sur les activités des auteurs d'actes de cybercriminalité.

14. De nombreux orateurs ont souligné la nécessité de mettre en place une coopération internationale efficace en matière de répression. Du fait de la dimension mondiale de l'Internet et du développement du commerce électronique, les frontières nationales ne s'opposaient plus à la cybercriminalité. Pour cette raison, la rapidité était essentielle à la réussite des enquêtes. Il fallait pour cela nouer d'étroites relations avec des partenaires clefs dans d'autres pays, avec le secteur privé et avec la société civile. Des participants ont décrit des initiatives de coopération internationales mises en œuvre actuellement, comme le réseau de contact initialement créé par le Groupe des huit et consistant en des services de lutte contre la cybercriminalité mis à la disposition des services de répression 24 heures sur 24 et sept jours sur sept ("24/7"). Le réseau de contact, qui est aujourd'hui opérationnel dans une quarantaine de pays, s'était révélé efficace contre la cybercriminalité. Un orateur a indiqué, cependant, que ce réseau n'était disponible que dans des pays qui avaient les moyens de traiter la cybercriminalité et qu'il fallait renforcer ces moyens dans les pays en développement.

15. Plusieurs orateurs ont indiqué qu'il fallait impérativement, pour combattre efficacement la cybercriminalité, développer et harmoniser les législations nationales. Cela s'appliquait en particulier aux lois et règles de procédure relatives au rassemblement et à la recevabilité des preuves. Il a été estimé, pour cette raison, qu'il faudrait également proposer des programmes de formation aux procureurs et aux juges. Il a été noté que la coopération internationale contre la cybercriminalité était compliquée par le fait que de nombreux pays n'avaient pas de législation concernant ce type de criminalité. Il a été proposé d'élaborer, à cette fin, des lois types en tenant compte des différents systèmes juridiques.

16. Plusieurs intervenants ont posé la question de savoir s'il était nécessaire d'élaborer un nouvel instrument international contre la cybercriminalité. Un intervenant a soutenu l'idée d'élaborer un tel instrument, citant la nécessité de disposer d'un cadre juridique mondial et de normes mondiales unifiées en matière de cybercriminalité. Il a été estimé que l'élaboration d'un tel instrument risquait de prendre du temps et qu'il était préférable de commencer rapidement les travaux. La plupart des orateurs, cependant, ont avancé qu'il était peut-être prématuré d'entamer la négociation d'une telle convention. Il a été avancé, à cela, de nombreuses raisons: le fait que la Convention sur la cybercriminalité du Conseil de l'Europe n'était que récemment entrée en vigueur et qu'il fallait du temps pour en évaluer les résultats; que la Convention était ouverte à la signature de tous les États, et pas seulement ceux d'Europe; et que le renforcement de la coopération internationale devrait, pour le moment, avoir la priorité absolue. Un orateur a noté que si l'assistance technique était un élément important de la Convention des Nations Unies contre la criminalité

transnationale organisée et de la Convention des Nations Unies contre la corruption, le problème de la cybercriminalité était tel qu'il faudrait fournir une assistance technique et renforcer les moyens avant d'entreprendre la négociation d'une convention internationale contre la cybercriminalité, cela afin que tous les États puissent y participer pleinement. Selon un orateur, bien qu'il fût prématuré de parler de négociation, si des négociations devaient effectivement avoir lieu, il faudrait que la procédure suive, en règle générale, le précédent établi par la négociation de la Convention contre la criminalité organisée et de la Convention contre la corruption. Plusieurs orateurs ont souligné qu'il était important que les États ratifient la Convention sur la cybercriminalité.

17. Plusieurs orateurs ont évoqué les recommandations contenues dans le document de travail relatif à l'atelier 6 (A/CONF.203/14), jugeant qu'elles formaient une base de discussion utile. Aucune objection n'a été soulevée quant à ces recommandations et de nombreux participants ont déclaré les soutenir en principe.

Conclusions et recommandations

18. Les participants à l'atelier ont émis les conclusions et recommandations suivantes:

a) L'ONUDC devrait proposer aux États une assistance technique et une formation palliant le manque de moyens et de compétences dont ces États ont besoin pour combattre la cybercriminalité. Il faudrait envisager d'actualiser le Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique et de mettre au point des outils de formation correspondants. Il faudrait diffuser ces outils au plan international afin de mettre en commun les connaissances et informations nécessaires pour reconnaître, protéger, prévenir et traiter les nouveaux types de cybercriminalité;

b) Il faudrait développer la coopération internationale dans les domaines de l'échange, de la recherche et de l'analyse d'informations relatives à la cybercriminalité. L'Organisation des Nations Unies devrait contribuer de façon prépondérante à l'adoption d'une stratégie mondiale destinée à protéger le fonctionnement du cyberespace de façon à en interdire l'utilisation ou l'exploitation par des criminels ou par des terroristes. À cet égard, il faudrait envisager de créer un forum virtuel ou un réseau de recherche en ligne facilitant la communication entre experts du monde entier sur la question de la cybercriminalité;

c) Il faudrait renforcer encore la coopération internationale en matière de répression, notamment en améliorant les moyens et compétences des pays qui ne sont pas actuellement reliés aux réseaux existants de répression de la cybercriminalité;

d) Il faudrait inviter les États qui ne l'ont pas encore fait à actualiser et à harmoniser leur législation pénale pour pouvoir combattre plus efficacement la cybercriminalité, en tenant dûment compte des problèmes liés à la définition des infractions, aux compétences de l'instruction et au rassemblement des preuves. Le partage de données d'expérience entre pays étant indispensable à cette fin, les États devraient prendre en considération les dispositions de la Convention sur la cybercriminalité du Conseil de l'Europe;

e) Les gouvernements, le secteur privé et les organisations non gouvernementales devraient collaborer pour combattre la cybercriminalité, y compris en sensibilisant le public, en suscitant des activités de prévention et en renforçant les moyens et compétences des professionnels de la justice pénale et des responsables politiques. Cette collaboration devra être fortement axée sur la prévention;

f) Il faudrait que les résultats de l'atelier soient présentés lors de la deuxième phase du Sommet mondial sur la société de l'information, qui se tiendra à Tunis du 16 au 18 novembre 2005.

Notes

[1] *Revue internationale de politique criminelle*, n° 43 et 44 (publication des Nations Unies, numéro de vente: F.94.IV.5).