



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

Bangkok, Thaïlande 18-25 avril 2005



Commission II
9^e séance* - après-midi

BKK/CP/19
22 avril 2005

Le onzième Congrès de l'ONU pour la prévention du crime étudie les moyens de remédier à l'impuissance des systèmes judiciaires face à la cybercriminalité

À la veille de la deuxième partie du Sommet mondial sur la société de l'information, qui se tiendra à Tunis, du 16 au 18 novembre 2005, le onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale a tenu, cet après-midi, au sein de l'une de ses deux Commissions, une discussion sur les moyens de remédier à l'impuissance des systèmes judiciaires face à la criminalité liée à l'informatique dite cybercriminalité. La discussion a été organisée en collaboration avec l'Institut coréen de criminologie.

La prolifération des nouvelles technologies de l'information et des communications (TIC) a suscité une multiplication de nouveaux types de délits qui constituent une menace non seulement pour la confidentialité, l'intégrité et la disponibilité des systèmes informatiques mais aussi pour la sécurité d'infrastructures critiques. La cybercriminalité montre aujourd'hui trois tendances, à savoir: la sophistication, la commercialisation et à l'intégration, a expliqué un professeur de l'Université nationale d'Australie qui a aussi dénoncé le danger du cyberterrorisme.

Le danger de la cybercriminalité ne concerne pas que les pays industrialisés, a alerté le Directeur de la Section des TIC du Département de la justice du Canada qui a d'abord souligné que les deux extrémités du fossé numérique se rapprochent depuis l'émergence des 12 « info-États » du Sud. Les pays en développement sont désormais exposés aux virus qui ne s'attaquent qu'aux téléphones mobiles. Si ces virus ne peuvent détruire les infrastructures mêmes, ils peuvent servir de vecteur à d'autres crimes comme l'usurpation d'identité.

La lutte contre cette cybercriminalité a été qualifiée de complexe, compte tenu de la grande difficulté à collecter des preuves intangibles et éphémères par nature. La difficulté vient aussi du fait qu'il faut souvent retracer l'activité criminelle et ses effets à travers toute une série de prestataires de services Internet ou d'entreprises parfois situées dans des pays différents. Cette difficulté a été illustrée par le Directeur adjoint de la Direction des crimes spécialisés d'Interpol qui a invoqué les cas de pornographie impliquant des enfants. Les solutions proposées aujourd'hui ont été résumées en sept points par le représentant de la France.

** Il n'existe pas de communiqué de presse pour la 8^e séance.*

(à suivre)

À l'instar des participants, il a préconisé l'établissement d'une typologie précise de la cybercriminalité pour en définir les moyens d'analyse et d'information; l'intensification de la formation des personnels concernés, services de détection et de répression, procureurs et juges compris; et le renforcement de la capacité d'enquête par la création d'organes spécialisés. Le représentant français a aussi prôné, la sensibilisation des particuliers et des entreprises, avec le concours des prestataires de services; la surveillance des contenus illicites véhiculés sur l'Internet; le décloisonnement des connaissances afin que chaque progrès profite à tous les services, et le renforcement de la coopération internationale par une adhésion aux conventions internationales dont celle du Conseil de l'Europe, spécifiquement sur la cybercriminalité, entrée en vigueur le 1^{er} juillet 2003, et son Protocole sur l'incrimination d'actes de nature raciste et xénophobe.

De tels efforts, a-t-il dit, encourageait l'adaptation de la législation nationale et faciliterait l'entraide judiciaire. Pour ce faire, le renforcement de l'assistance technique s'avère urgente, ont souligné de nombreuses délégations, en réclamant la mise à jour régulière du Manuel des Nations Unies sur la cybercriminalité, conformément à l'évolution rapide des TIC et à celle de la cybercriminalité.

La Commission poursuivra ce débat demain, samedi 23 avril, à partir de 10 heures, alors que commencera le débat de haut niveau au cours duquel de nombreux ministres de la justice commenteront les cinq questions inscrites à l'ordre du jour du Congrès, avant d'adopter, le 25 avril, la Déclaration de Bangkok. Placé sous le signe des « Alliances stratégiques », le Congrès tient ses travaux au sein de la Plénière, de ses deux Commission et de six ateliers pour étudier les questions de la lutte contre la criminalité organisée, de la coopération internationale contre le terrorisme, de la corruption et de l'application des règles et des normes de l'ONU en matière de prévention du crime et de la justice pénale.

Parmi les panélistes qui son intervenus aujourd'hui dans les discussions, il faut signaler la présence du Président de l'Institut coréen de criminologie, Taehoon Lee; du Secrétaire permanent du Ministère des technologies de l'information et des communications de la Thaïlande, Krainsorn Pornsutee; du Professeur à l'Université nationale d'Australie, Peter Grabosky; et du Directeur de la Section des politiques de justice pénale, de la technologie et de l'analyse du Département de la justice du Canada, Gareth Sansom. Il faut signaler également la présence de la Conseillère juridique à la Section de la propriété intellectuelle et de la criminalité liée à l'informatique du Département de la justice des États-Unis, Amanda Hubbard; de la Procureure attachée à la Haute Cour de justice de la Roumanie, Ioana Albani; et du Directeur adjoint du Directeurat des crimes spécialisés d'Interpol, Hamish McCulloch.

MESURES DE LUTTE CONTRE LA CRIMINALITÉ LIÉE À L'INFORMATIQUE

Présentations

M. TAEHOON LEE, Président de l'Institut coréen de criminologie, a dit que la criminalité liée à l'informatique est en hausse. L'espace cybernétique est de plus en plus le lieu où des millions de gens paient leurs factures, consultent des professionnels, font des recherches d'information, font leurs courses, et restent en contact avec leurs familles, leurs amis, des institutions publiques, ou leurs employeurs. La cybercriminalité pose des défis jusqu'ici inconnus du système judiciaire. La nature globale de la cybercriminalité pose des problèmes légaux difficiles à résoudre parce que les criminels peuvent agir en utilisant des serveurs situés en dehors des territoires où ils commettent leurs méfaits, sans courir le risque d'être arrêtés et soumis aux sanctions des règlements nationaux. Les différents crimes informatiques, comme le blanchiment d'argent, le jeu, la fraude par Internet, le harcèlement des personnes et le terrorisme cybernétique, peuvent être commis à tout moment de manière instantanée. Les prédateurs peuvent s'attaquer à des gens vivant à l'autre bout du monde sans que leurs actions soient tout de suite repérées et sans que la police puisse enquêter. L'espace cybernétique est aussi devenu la cible des organisations terroristes et des organisations du crime organisé, ce qui risque d'avoir des impacts désastreux sur les sociétés. Les questions à résoudre rapidement sont celles de la mise en place de cadres de justice pénale adaptés à la cybercriminalité; de la création de nouvelles méthodes d'enquête; et de saisie des informations électroniques, a dit M. Lee. Malheureusement, le monde dispose de très peu de traités ou conventions multilatérales traitant de la cybercriminalité, a-t-il déploré. Le Conseil de l'Europe est l'auteur de la seule convention contre la cybercriminalité existant à l'heure actuelle, a relevé le représentant.

M. KRAISORN PORNSUTEE, Secrétaire permanent au Ministère des technologies de l'information et des communications de la Thaïlande, a souligné qu'il convient d'abord de cerner les actes de cybercriminalité, en faisant observer que les délits varient d'un pays à l'autre. Ce qui serait considéré comme une entrave à la liberté d'expression ailleurs peut être un crime grave en Thaïlande, a-t-il dit en donnant l'exemple de propos offensants à l'égard de la famille royale. La cybercriminalité pose des défis énormes et les organes de détection et de répression ont du mal à suivre. Il est temps de réfléchir à des mesures ambitieuses pour rattraper les retards, a-t-il dit en espérant la création, au cours de ce Congrès, de partenariats solides.

M. PETER GRABOSKY, professeur à l'Université nationale d'Australie, a dit que le fossé numérique et l'absence de lois contre la cybercriminalité dans les pays qui se trouvent de l'autre côté du fossé de l'univers informatique sont favorables aux criminels qui peuvent profiter de ces lacunes pour perpétrer leurs crimes. Le *phising*, qui consiste à utiliser des sites web légitimes pour tromper des gens et se procurer leurs informations personnelles à des fins criminelles est en train de se développer rapidement. Le commerce électronique est devenu la cible de toutes sortes d'attaques qui posent une menace à l'expansion des activités économiques. Les attaques cybernétiques se basant sur l'usage des ordinateurs personnels de personnes non averties afin de s'en prendre à des institutions ou à des individus sont devenues monnaie courante. Le cyberterrorisme comprend les activités informatiques illicites ayant pour objet final d'exercer des pressions ou des actes d'intimidation sur des personnes, des groupes, des institutions ou des pays, a dit M. Grabosky. L'Internet peut aussi être un puissant vecteur de propagande.

M. GARETH SANSOM, Directeur de la Section des politiques de droit pénal, de la technologie et de l'analyse du Département de la justice du Canada, a estimé que le fossé numérique ne devrait pas être présenté comme les deux falaises opposées d'un canyon, compte tenu de l'existence d'un groupe d'« info-États » d'une douzaine de pays qui se trouvent entre les deux extrêmes. Le fossé se réduit peu à peu, mais il faudra des générations pour que les pays en bas de liste parviennent au niveau des pays qui se situent aujourd'hui au milieu. La réduction du fossé numérique semble être le fruit de l'accès à de nouvelles techniques comme la téléphonie mobile. Des tendances différentes, en la matière, exposent les régions à des vulnérabilités différentes en matière de cybercriminalité. Dans les pays en développement, les nouvelles techniques peuvent susciter des nouvelles menaces jusqu'à ce que leur système s'affirme et les normes de sécurité soient introduites. En l'occurrence, une réponse unique n'est pas viable.

En 2001, des recherches ont été faites sur les virus et sur les *worms* –vers. L'étude épidémiologique a permis de déceler quelques tendances. Ainsi, selon cette étude, les virus varient dans leur vitesse et dans leur capacité de propagation et il semble que les pays industrialisés y sont plus vulnérables. Cela n'est plus vrai aujourd'hui, a prévenu le Directeur en mettant en garde les pays en développement contre les virus qui visent spécifiquement les téléphones mobiles. La nouvelle tendance est que ces vers-virus ne peuvent plus réellement attaquer les infrastructures, mais le danger est qu'ils peuvent servir de vecteur à un autre crime comme le vol ou l'usurpation. Cette nouvelle utilisation des vers peut exposer les pays en développement à de nouvelles menaces alors que leur croissance passe par l'accès aux nouvelles technologies de l'information et de la communication.

Mme AMANDA HUBBARD, Juriste à la Section du Ministère de la justice des États-Unis, chargée des affaires criminelles ayant trait à l'informatique et à la propriété intellectuelle, a déclaré que le 16 juillet dernier son service avait reçu un appel d'urgence venant d'un de ses fonctionnaires travaillant dans un pays d'Amérique du Sud. Le fonctionnaire transmettait une demande d'aide judiciaire de la police du pays concerné aux autorités américaines. Une personne avait été enlevée, et ses kidnappeurs demandaient le versement d'une rançon à travers un courrier électronique envoyé d'un serveur situé sur le territoire américain. Le Département américain de la justice a pu contacter les opérateurs du serveur après avoir identifié sa location. Le Département a pu obtenir une injonction légale permettant de saisir l'opérateur du serveur et d'obtenir le nom de la personne qui avait ouvert le compte e-mail à partir duquel la demande de rançon avait été envoyée. Les agents chargés de l'enquête ont pu déterminer que la personne se servant de ce compte d'adresse e-mail se trouvait dans le pays où avait eu lieu l'enlèvement, et que le courrier électronique exigeant la rançon avait été envoyé depuis un ordinateur situé dans un cybercafé de la capitale de ce pays. Les autorités américaines ont transmis ces informations à la police du pays où avait été perpétré le crime. Celui à qui appartenait l'adresse e-mail a été identifié et arrêté, a dit Mme Hubbard en indiquant que ce cas avait été résolu grâce à la rapidité des contacts entre le Département américain de la justice et les autorités du pays où le crime avait été perpétré. Malheureusement, la plupart des crimes informatiques ne connaissent pas ce genre de conclusion heureuse.

Mme IOANA ALBANI, Procureure attachée à la Haute Cour de justice de la Roumanie, a déclaré que devant l'impuissance de l'appareil judiciaire face à la cybercriminalité, son pays a d'abord créé une Section chargée d'enquêter sur ce type de criminalité ainsi qu'une structure sur les fraudes par Internet, au sein de la police. C'est en 2000 que la Roumanie a lancé ses premières enquêtes qui ont conduit, l'année suivante, à des condamnations qui, faute de loi spécifique, se sont fondées sur les articles relatifs à la fraude ou à l'usurpation prévues par le Code pénal. Le caractère étendu de ce type de crimes conjugué à l'absence de cadre juridique a conduit à un conflit de juridiction. La Roumanie a alors décidé d'adopter la Convention sur la cybercriminalité du Conseil de l'Europe et en juin 2002, et promulgué une loi sur le commerce électronique pour sanctionner la fraude par cartes de crédit, puisque l'article du Code pénal sur la fausse monnaie ne pouvait s'appliquer. La loi, qui s'est avérée un outil très efficace pour les services de détection et de répression, pénalise aussi l'accès illégal à des données sur l'Internet ou leur effacement.

En 2003, a poursuivi la Procureure, la Roumanie a enfin adopté sa loi sur la lutte contre la cybercriminalité. Elle définit les concepts et précise les procédures et a permis la création d'un Bureau chargé des demandes d'entraide judiciaire au sein de la Haute Cour de justice. Par ailleurs, un Service permanent de lutte contre la cybercriminalité a été établi au sein du Bureau chargé de la criminalité transnationale organisée et du terrorisme, de la police nationale. La Roumanie a aussi jugé utile d'ouvrir un site Internet pour recevoir des plaintes sur les violations éventuelles des dispositions prévues mais surtout pour diffuser la législation pertinente ou encore lancer des avertissements quant aux nouveaux types de fraude. Avec les institutions mises en place, la Roumanie est désormais capable de répondre aux demandes d'entraide et de coordonner ses actions avec d'autres pays, a assuré la Procureure.

M. HAMISH MCCULLOCH, Directeur adjoint du Directeurat des crimes spéciaux d'Interpol, a déclaré que les abus contre les enfants, notamment la pornographie, avaient connu une expansion extraordinaire à travers l'usage de l'Internet. Plus de trois millions d'images de pornographie enfantine circulant sur le web sont stockées dans la base de données d'Interpol, a-t-il indiqué. Les images représentent 20 000 victimes différentes, a-t-il dit. La première question qui se pose à un enquêteur, a dit M. McCulloch, est de chercher à identifier l'enfant dont l'image circule dans le cyberspace. Ensuite, il faut chercher à savoir où se trouve géographiquement l'enfant, et si les images qui circulent ont été vues auparavant ou font partie d'une série de photos dont certaines ont auparavant fait l'objet d'enquêtes. S'il s'agit de nouvelles images, on cherche à identifier l'enfant et l'environnement dans lequel la photo a été prise. La base de données d'Interpol ne peut être utilisée que par des personnels autorisés, a dit Hamish McCulloch. Deux agents sont responsables de sa gestion. Quatorze pays participent à l'enrichissement de cette base de données, alors que les services spécialisés savent que les enfants sont victimes d'abus dans un plus grand nombre de pays. Interpol espère donc que d'autres États se joindront à la tâche qui doit être menée au niveau international, a dit le responsable d'Interpol.

Discussion

En lançant la discussion, le représentant du Canada s'est demandé s'il serait utile de publier des documents d'informations techniques tels que le Manuel des Nations Unies sur la prévention et la répression de la criminalité liée à l'informatique. Il a aussi demandé s'il était possible d'incorporer des appareils de prévention dans les technologies de l'information et des communications (TIC) avant leur lancement sur le marché. Qui devrait financer une telle initiative? Le secteur public ou le secteur privé, s'est-t-il interrogé. Techniquement, peut-on, utiliser les mêmes technologies pour combattre la cybercriminalité? Les intervenants ont jugé important de réviser régulièrement le Manuel de l'ONU, en arguant de l'évolution rapide des technologies et des nouvelles formes de criminalité. Un représentant de Microsoft a reconnu le rôle du secteur privé dans la protection des usagers. Ce secteur, a-t-il dit, doit aussi collaborer avec les services de détection et de répression pour dissuader la cybercriminalité et là, les vendeurs ont une responsabilité à assumer. Le Secteur privé pourrait aussi former les services spécialisés. La collecte de preuves exige une formation très poussée, a prévenu le Directeur du Département de la justice du Canada, en insistant sur la complexité de la tâche. Les services spécialisés, a ajouté le représentant de Microsoft, auraient tout intérêt à développer des relations de travail avec les fournisseurs de services qui sont les meilleurs informateurs en cas de délits.

Le représentant de l'Ukraine a dit que son pays qui avance dans la voie de la démocratie, était en train de mettre en place des réglementations contre les crimes informatiques et cybernétiques. Ce qui s'est passé au cours des récents scrutins politiques en Ukraine a montré combien il était important de créer un cadre législatif sain sur l'usage des outils informatiques. L'Ukraine espère que la communauté internationale parviendra à s'accorder sur la mise en place d'un cadre de lutte contre la cybercriminalité qui soit applicable de manière universelle. Le représentant de l'Autriche a demandé aux panélistes quel était le principal obstacle se posant aux enquêtes sur les crimes cybernétiques. Que devraient faire les pays pour lever cet obstacle? Le représentant de la Jamahiriya arabe libyenne a dit que son pays venait d'entrer dans l'ère des paiements bancaires électroniques. La Libye s'inquiète des dangers qui pourraient menacer cette pratique et aimerait que les victimes d'actes criminels soient protégées.

Répondant à la question de l'Autriche, M. Gareth Sanson a dit que le principal obstacle aux enquêtes contre les actes de cybercriminalité se trouvait dans l'absence de lois et de procédures au niveau national des pays. La recherche de preuves est généralement difficile, à cause de l'absence d'environnement légal adapté au monde informatique. M. McCulloch a pour sa part indiqué qu'Interpol avait du mal à mener ses enquêtes parce que de nombreux pays sont réticents à reconnaître que des actes de pornographie infantile sont perpétrés sur leur territoire. Certains gouvernements refusent même de transmettre des photos à la base de données d'Interpol, a-t-il dit. **Mme Iona Albani**, a dit que les fournisseurs et prestataires devraient mieux coopérer avec les institutions de recherche policière et d'enquêtes contre les crimes liés à l'informatique.

Le représentant de la France a estimé que la réponse à la cybercriminalité devait être conduite de manière globale. La France a décidé d'accroître les moyens d'analyse et d'information consacrés à la lutte contre ce crime. Elle renforce ses services d'enquête et d'investigation. Son administration et ses entreprises sont de plus en plus sensibilisées aux crimes cybernétiques, et des actions sont menées pour sensibiliser l'opinion quant au contenu illicite de certains sites Internet. La France estime qu'il faut d'autre part développer la coopération internationale en demandant aux États de signer et ratifier les conventions contre les crimes liés à l'informatique, a dit le représentant.

À son tour, le représentant de l'Espagne a annoncé le projet de créer un observatoire pour mettre au point une série d'indicateurs sur le réseau Internet dans sa partie publique et privée, comme Intranet. Il sera question de faire l'inventaire des technologies mais aussi de recenser tous les programmes d'innovation, de mise au point et de développement existants pour devancer les utilisations criminelles éventuelles de ces technologies nouvelles. À ce titre, il a posé une question aux présentateurs consistant à en savoir un peu plus des autres programmes existants. Il a proposé que l'ONU DC envisage la création de points de contacts d'experts qui pourraient échanger leurs expériences et les enseignements qu'ils ont pu en tirer.

Interpol, a répondu son Directeur adjoint, a installé une Sous-Direction spécialisée sur la cybercriminalité financière. L'orateur a aussi fait part de l'organisation d'une réunion en la matière qui a bénéficié d'une audience internationale très large. Interpol, a-t-il poursuivi, est représenté dans le Groupe de liaison du G-8 par sa Centrale d'appels 24/7 qui permet de maintenir le contact. Quelque 39 pays participent désormais à cette Centrale, a précisé le représentant du Royaume-Uni avant de s'interroger sur le type de recommandation à faire sur les programmes de formation. Peut-on recommander l'établissement d'un réseau d'institutions? Est-il possible de créer une base de données à l'intention des services de détection et de répression? a-t-il encore demandé.

Le Directeur adjoint d'Interpol lui a répondu que des activités de formation ont déjà été lancées, il y a dix ans. Aujourd'hui, l'on envisage des stages de formation réguliers, conformes à l'évolution rapide de la cybercriminalité. La Conseillère spéciale du Département américain de la justice a attiré l'attention des participants sur le « Advocacy Center » qui a organisé un stage de formation à la lutte contre la cybercriminalité. Toutes ces initiatives disparates devraient peut-être être réunies au sein d'un programme d'action élaboré, sous les auspices des Nations Unies, a estimé la représentante de l'Argentine en demandant aux présentateurs s'ils pensent qu'un des programmes, fonds ou institutions des Nations Unies pourrait jouer le rôle de coordonnateur. Nous avons besoin de synergie, a-t-elle insisté, appuyé en cela par le représentant du Canada qui a appelé à plus de coordination, en matière de formation des différents agents du système judiciaire dont les procureurs.

Aucune base de données centralisée n'existe encore, a reconnu la représentante du Département américain de la justice qui a dénoncé les conséquences des restrictions budgétaires. Elle a invité les participants à établir des contacts et à partager les idées et les ressources disponibles. Beaucoup de personnes travaillent d'arrache-pied pour mettre en place des réseaux, a souligné le Directeur adjoint d'Interpol en rappelant une nouvelle fois la création de la Centrale d'appels 24/7. La cybercriminalité évoluant très rapidement, il faudra du temps pour avoir une réponse coordonnée au niveau international.

Le représentant du Maroc a dit que son pays avait lancé une réforme judiciaire visant à réprimer la criminalité informatique. Le Maroc se heurte en ce moment à la question des preuves. Il a besoin d'une assistance technique au niveau juridique et au niveau des avocats. La transposition des dispositions légales d'un système juridique à un autre étant parfois difficile, le Maroc, qui applique essentiellement des normes de droit latin, aimerait savoir quelle assistance pouvait être apportée aux pays pour les aider à intégrer dans leurs systèmes des concepts juridiques venus de systèmes différents.

Mme Iona Albani a indiqué que des programmes d'aide et d'assistance pouvant aider les pays qui ont besoin de soutien pour intégrer des notions de droit d'origine étrangère dans leurs systèmes juridiques existaient. M. Gareth Sansom a dit que des lois-types avaient été élaborées par certains pays du G-8 en ce qui concerne la cybercriminalité. Le représentant de la France a dit que son pays, qui a mené des études sur ces questions, pouvait répondre à la demande du Maroc.

M. Elson Baty, Juge et expert des questions liées aux abus contre les enfants, a dit que la pornographie mettant en scène des enfants devrait être érigée en infraction pénale. Même le fait de visiter des sites abritant ces photos devrait être criminalisé, a-t-il proposé. M. McCulloch lui a répondu qu'Interpol concentrait d'abord ses efforts sur la situation des enfants victimes de sévices sexuels. Concernant la criminalisation de la visite de sites pornographiques, jusqu'à maintenant, cette question relève des législations nationales, a dit M. McCulloch. Une autre difficulté vient du fait que les pays n'ont pas de définition commune de ce qui constitue de la pornographie, a-t-il poursuivi. D'autre part, l'introduction d'images virtuelles dans les iconographies pornographiques complique la tâche des enquêteurs. Le représentant de la Jamahiriya arabe libyenne a évoqué la difficulté de l'établissement des preuves dans les procédures concernant les poursuites contre la pornographie. Le représentant du Chili a souligné que sans une définition des crimes constitutifs de la cybercriminalité, tous les efforts seraient vains.

Faisant part de son sentiment que l'accent a surtout été mis sur les victimes en tant qu'individus, le représentant du Centre international pour la culture scientifique a regretté que le débat soit passé à côté de la menace plus large qui pèse sur les sociétés. La cybercriminalité est surtout dangereuse, a-t-il estimé, pour les grandes entreprises privées: une attaque sur ces dernières pouvant avoir des répercussions sur l'ensemble de la scène internationale. Il a, en effet, souligné que dans presque tous les pays, ces sociétés contrôlent les infrastructures critiques dont les systèmes bancaires, les barrages hydrauliques, le contrôle du trafic aérien ou encore la production d'énergie qui utilisent toutes les techniques informatiques.

Ces sociétés investissent massivement dans la protection de leurs actifs, a rassuré le professeur à l'Université nationale de l'Australie, en rappelant qu'il s'agit d'une obligation juridique et surtout de bons sens. L'ONU a aussi fait un gros travail dans le domaine de la cybersécurité, au sein d'un Groupe d'experts dont le rapport sera présenté à la soixantième session de l'Assemblée générale, a indiqué, à son tour, la Conseillère spéciale du Département américain de la justice.

Documentation

Document de travail (A/CONF.203/14)

Le document souligne que la prolifération, partout dans le monde, des nouvelles technologies de l'information et de la communication (TIC) a suscité une multiplication de nouveaux types de délits liés à l'information. Ces derniers constituent une menace non seulement pour la confidentialité, l'intégrité et la disponibilité des systèmes informatiques mais aussi pour la sécurité d'infrastructures critiques. Les menaces reflètent les différences qui existent aux extrémités du « fossé numérique ». De leur côté les enquêteurs et les procureurs comme les juges se heurtent à un certain nombre de problèmes découlant de ce que les preuves numériques sont à la fois intangibles et éphémères. La difficulté vient aussi du fait qu'il faut souvent retracer l'activité criminelle et ses effets à travers toute une série de prestataires de services Internet ou d'entreprises parfois situées dans des pays différents, ce qui peut susciter d'épineuses questions de compétence et de souveraineté.

La complexité des défis engendrés par la criminalité liée à l'informatique exige inévitablement une coopération internationale, ce qui signifie qu'en définitive, les pays doivent se doter des outils nécessaires en matière de législation, de procédure et de réglementation. L'approche doit être large et inclusive et aller au-delà du droit pénal, des procédures pénales et de l'action des services de répression. L'accent doit être mis sur les conditions qui doivent être remplies pour qu'une cyberéconomie fonctionne en toute sécurité. Tous les États doivent néanmoins être encouragés à actualiser leur législation pénale. Ils doivent aussi moderniser leurs règles de procédure ainsi que les lois, accords ou arrangements relatifs à l'entraide judiciaire et, lorsqu'ils entreprennent d'élaborer de nouvelles lois, s'inspirer des dispositions de la Convention relative à la cybercriminalité du Conseil de l'Europe. Quant au onzième Congrès, il doit porter son attention sur la nécessité d'établir des mécanismes visant à promouvoir l'échange d'informations au plan international, l'alerte rapide, l'intervention policière et la limitation des dommages. Toujours au plan international, des efforts doivent être déployés pour établir des mécanismes de financement propres à faciliter la recherche appliquée.

Le document contient sept chapitres de fond expliquant les différents types de criminalité liée à l'informatique; les initiatives de l'ONU pour combler le fossé numérique; les difficultés rencontrées par les services de répression; les lacunes existant dans les législations nationales; les moyens de renforcer la coopération internationale; la recherche; et la coopération entre les secteurs public et privé.

* * * * *