Nations Unies A/CONF.213/L.4/Add.1

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

Salvador (Brésil), 12-19 avril 2010

Distr. limitée
14 avril 2010
Français
Original: anglais

Rapport du Comité II sur le point 8 de l'ordre du jour et l'Atelier 2

Additif

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 (point 8 de l'ordre du jour)

Délibérations

1. De sa 1ère à sa 3e séance, les 12 et 13 avril 2010, le Comité II a procédé à un débat général sur le point 8 de l'ordre du jour, intitulé "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". Pour l'examen de la question, la Comité était saisi des documents suivants:

a) Un document de travail établi par le Secrétariat 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 (document A/CONF.213/9);

b) Un Guide de discussion (A/CONF.213/PM.1);

c) Les rapports des réunions régionales préparatoires au douzième congrès (A/CONF.213/RPM.1/1, A/CONF.213/RPM.2/1, A/CONF.213/RPM.3/1 et A/CONF.213/RPM.4/1).

2. A la 1ère séance, le 12 avril, le Président du Comité II a fait une déclaration liminaire. Un représentant du Secrétariat a présenté ce point. Des déclarations ont été faites par les représentants de la Chine, de l'Algérie, du Canada, de l'Argentine, des États Unis d'Amérique, de l'Arabie saoudite, de la Fédération de Russie, de l'Allemagne, du Botswana, de Cuba et du Chili. Les observateurs du Réseau ibéro-américain d'assistance juridique (IberRed), du Conseil de l'Europe et de la Société mondiale de victimologie ont également fait des déclarations, de même que l'observateur de la Norvège.

V.10-52734 (F)

Merci de recycler

3. À la 2e séance, le 13 avril, des déclarations ont été faites par les représentants de l'Espagne au nom de l'Union européenne, de la Pologne, de la République de Corée, de l'Azerbaïdjan, du Mexique, de l'Indonésie, de l'Angola et de l'Argentine.

4. À la 3e séance, le 13 avril, des déclarations ont été faites par les représentants de la Colombie, de l'Afrique du Sud, de l'Inde, du Pérou, du Zimbabwe, de l'Oman et du Brésil. Une déclaration a aussi été faite par un observateur de l'Association internationale des procureurs et poursuivants.

Débat général

5. Ouvrant le débat sur ce point, le Président a souligné les problèmes posés par la cybercriminalité et par l'aptitude des groupes criminels organisés à profiter des possibilités offertes par l'évolution constante de la technologie. Il a noté le caractère transfrontière de la cybercriminalité, le fait que l'on ignorait l'étendue du problème et les différences entre les systèmes nationaux.

6. Dans sa déclaration liminaire, la représentante du Secrétariat a dit que la cybercriminalité constituait un des plus grands défis actuels pour les services de détection et de répression et a signalé que des États Membres, des universitaires et d'autres parties prenantes avaient demandé que soit élaborée une convention internationale sur ce sujet. Les pays devaient développer leurs capacités dans ce domaine et l'UNODC pouvait les y aider en leur fournissant les compétences techniques requises et un soutien opérationnel. Un plan mondial de renforcement des capacités faisant intervenir les institutions et les partenaires clefs pourrait constituer un moyen efficace de permettre aux pays de mettre en place les capacités globales et durables requises afin de lutter contre la cybercriminalité.

7. Au cours du débat, les participants ont reconnu que la rapidité du progrès technologique présentait indéniablement de nombreux avantages mais qu'elle offrait aussi de nouvelles possibilités de commettre des infractions traditionnelles, comme la fraude et la diffusion de la pornographie mettant en scène des enfants et permettait de nouveaux types d'infractions comme l'intrusion, la transmission de courriels non sollicités, le "phishing" (l'utilisation de sites Web contrefaits – ou de messages dirigeant les utilisateurs vers ces sites – à des fins frauduleuses), le piratage, l'envoi malintentionné de virus et autres attaques contre l'infrastructure informatique. Il a été observé que les organisations terroristes et les groupes criminels organisés se servaient des progrès technologiques pour faciliter leurs activités criminelles. Les participants ont été d'avis que la cybercriminalité menaçaient les économies, les infrastructures essentielles, la crédibilité des institutions et le bien-être social et culturel.

8. Des participants ont souligné les difficultés que présentait la lutte contre la cybercriminalité. Les technologies évoluaient si rapidement et étaient si rapidement disponibles sur le marché que les politiques et la législation n'arrivaient pas à suivre. Les différences entre les systèmes juridiques et le manque de coopération internationale entravaient les enquêtes et la poursuite des délinquants. Cette technologie complexe était devenue un phénomène de masse: le revers de la médaille était la cybercriminalité. Un intervenant a souligné que, souvent, les infractions informatiques n'étaient pas signalées parce que les victimes pensaient que les enquêtes n'aboutiraient pas et, lorsqu'il s'agissait de sociétés, craignaient pour leur réputation.

9. Plusieurs intervenants ont exposé les mesures prises par leurs gouvernements pour lutter contre la cybercriminalité: législation pénale et législation visant le blanchiment d'argent, réglementation visant les cybercafés, renforcement des capacités, sensibilisation, renforcement des mécanismes d'établissement de rapports et protection des groupes vulnérables. Ils ont aussi mentionné la création d'équipes d'intervention rapide, d'unités spécialisées et de plates-formes interinstitutionnelles à l'usage des services de détection et de répression, de l'armée, des milieux universitaires et du secteur privé. Des intervenants ont aussi fait référence aux possibilités offertes par les technologies de l'information en matière de détection et de répression: surveillance et suivi électroniques, intelligence artificielle et outils électroniques permettant de détecter les transactions financières suspectes et de repérer les adresses de protocole Internet. Cependant, les enquêtes et les poursuites dans le domaine de la cybercriminalité exigeaient de nouvelles compétences et de nouveaux outils, par exemple pour pouvoir recueillir et analyser des preuves numériques et les utiliser dans le cadre de poursuites pénales. Des intervenants ont souligné qu'il importait que la lutte contre la cybercriminalité ne porte pas atteinte à la vie privée ni aux droits de l'homme.

10. De nombreux intervenants ont dit que la coopération internationale était indispensable pour combattre la cybercriminalité. Plusieurs d'entre eux ont appelé les États à renforcer l'efficacité de l'entraide judiciaire et de la coopération. Il a souvent été dit que la Convention sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest) constituait le cadre juridique international le plus complet contre la cybercriminalité. Il a aussi été fait référence au Programme mondial cybersécurité lancé par l'Organisation internationale des télécommunications en 2007 et aux initiatives de l'Organisation des États américains, du G-8, d'INTERPOL et du Secrétariat du Commonwealth. Il a été noté que les réseaux de spécialistes étaient utiles pour les échanges d'informations et la mise en commun des données d'expérience et des enseignements tirés. Les réseaux régionaux existants devraient être renforcés et plus étroitement liés entre eux.

11. Les participants ont reconnu que les pays en développement étaient les plus vulnérables face à la cybercriminalité. Il fallait absolument que les pays développés proposent une aide accrue dans le domaine du renforcement des capacités, en particulier en ce qui concernait les agents des services de détection et de répression et les procureurs et juges. Le secteur privé et en particulier les prestataires de services devraient assumer leurs responsabilités. Il a été fait référence à un certain nombre d'outils disponibles, y compris un forum virtuel à l'intention des pays d'Asie, établi avec l'aide de l'UNODC, un programme de formation en ligne réalisé par l'Association internationale des procureurs et poursuivants et un dossier sur la législation relative à la cybercriminalité établi par l'Union internationale des télécommunications. Des intervenants ont mentionné les travaux de l'UNODC dans le domaine de la criminalité liée à l'identité ainsi que les recommandations d'un groupe restreint d'experts sur cette question. Plusieurs intervenants ont demandé que soit mis en place, avec la participation de toutes les parties prenantes, un plan d'action pour le renforcement des capacités au niveau international.

12. Les participants ont débattu de la recommandation faite lors des réunions régionales préparatoires selon laquelle il conviendrait d'envisager favorablement et avec attention l'élaboration d'une convention mondiale contre la cybercriminalité. Certains intervenants se sont déclarés très favorables au lancement de négociations

en vue de l'élaboration d'un nouvel instrument international pour harmoniser les approches juridiques nationales et favoriser la coopération internationale. Certains ont fait valoir que les initiatives existantes n'avaient qu'une portée bilatérale ou régionale limitée. Un nouvel instrument, qui pourrait consister en un protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée ou en une convention distincte, s'inspirerait des traités ou accords bilatéraux et régionaux existants sur la cybercriminalité, y compris la Convention de Budapest, et les compléterait. Un intervenant a proposé qu'un nouvel instrument soit négocié dans le cadre de la Commission du droit international aux travaux de laquelle l'UNODC serait associé.

13. D'autres intervenants se sont déclarés opposés à l'ouverture de négociations sur un tel instrument. Ils ont estimé que la Convention de Budapest constituait un cadre adéquat, qui était utilisé, y compris par des États non parties, comme modèle de législation permettant aux États de procéder avec succès à des enquêtes. Certains ont craint que les normes fixées par un instrument mondial ne soient moins exigeantes et que les efforts de modernisation en cours ne soient freinés pendant la durée de la négociation d'un nouvel instrument. Il a été estimé que les problèmes rencontrés dans la lutte contre la cybercriminalité étaient surtout d'ordre opérationnel, ce qui demandait une amélioration des échanges d'informations et un renforcement des capacités. Il a été dit que les pays devraient affecter les compétences limitées dont ils disposaient dans le domaine de la cybercriminalité à ces questions opérationnelles et non à la négociation d'une nouvelle convention.

14. Plusieurs intervenants ont été d'avis qu'il était trop tôt pour prendre position concernant une nouvelle convention étant donné qu'un certain nombre de questions fondamentales devaient être examinées au préalable. Plusieurs intervenants ont demandé des précisions sur l'objectif et la portée d'un tel instrument et l'un d'entre eux a recommandé que soit réalisée une analyse pilote des normes en vigueur. Les questions qu'il faudrait régler pour négocier une nouvelle convention étaient notamment les suivantes: juridiction extraterritoriale et problèmes de souveraineté nationale qui en découlaient; droits de l'homme, vie privée et sécurité nationale; et nécessité de faire participer le secteur privé à un processus de négociation intergouvernemental.

Conclusions et recommandations

15. Au cours des échanges de vue sur la cybercriminalité, les participants se sont accordés sur un certain nombre de conclusions et de recommandations et sur la nécessité pour les États et les organisations internationales de donner suite à ces recommandations en prenant rapidement des mesures concrètes.

16. Les participants ont été d'accord pour dire que le progrès technologique se traduisait à la fois par des avantages et des menaces pour la société et que la lutte contre la cybercriminalité exigeait une attention immédiate. Les liens et les interactions entre technologie et criminalité devaient être soigneusement analysés pour que l'on puisse élaborer des stratégies efficaces.

17. Les États devraient mettre en place et renforcer à long terme des capacités durables. L'octroi d'une assistance technique aux pays en développement était urgente, en particulier en matière de renforcement des capacités et d'élaboration de textes de loi, ainsi que d'apports de ressources et d'experts compétents. L'UNODC

devrait poursuivre sa coopération avec ses principaux partenaires pour fournir une assistance technique dans ces domaines, notamment avec le Conseil de l'Europe en tant que dépositaire de la Convention de Budapest. La question de l'élaboration d'un plan d'action en matière de renforcement des capacités au niveau international devrait être examinée avec soin.

18. Les États devraient s'efforcer de renforcer la coopération entre les institutions nationales, entre eux et avec le secteur privé, et apporter leur soutien politique sans réserve à ce processus. L'échange de renseignements et de bonnes pratiques entre les États devait être intensifié, notamment grâce au renforcement des réseaux compétents.