Nations Unies E/CN.15/2011/19

Conseil économique et social

Distr. générale
2 mars 2011
Français
Original: anglais

Commission pour la prévention du crime et la justice pénale
Vingtième session
Vienne, 11-15 avril 2011
Point 6 de l'ordre du jour provisoire*
Tendances de la criminalité dans le monde, et nouvelles questions et mesures prises dans le domaine de la prévention du crime et la justice pénale

Rapport du groupe intergouvernemental d'experts à composition non limitée sur l'étude approfondie du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé

Note du secrétariat

1. En application du paragraphe 9 de la résolution 65/230 de l'Assemblée générale, le groupe intergouvernemental d'experts à composition non limitée créé par la Commission conformément au paragraphe 42 de la "Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux: les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation" (résolution 65/230 de l'Assemblée générale, annexe) a tenu sa réunion à Vienne du 17 au 21 janvier 2011. Conformément à son mandat, le groupe d'experts s'est penché sur la question suivante:

> Étude approfondie du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y répondre, notamment l'échange d'information sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, en vue d'examiner les options envisageables pour renforcer les mesures juridiques ou autres prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles.

* E/CN.15/2011/1.

V.11-80327 (F) 150311 160311

2. Au paragraphe 11 de la résolution 65/230, l'Assemblée générale avait prié le groupe intergouvernemental d'experts à composition non limitée de faire rapport à la Commission sur l'avancement de ses travaux. Le groupe d'experts a donc examiné et adopté les documents finaux joints en annexe, intitulés "Ensemble de thèmes à examiner dans le cadre d'une étude approfondie sur les incidences de la cybercriminalité et la lutte contre ce phénomène" (annexe I) et "Méthodologie de l'étude" (annexe II), dont la Commission est saisie pour examen à sa vingtième session.

3. Après que l'ensemble de thèmes à examiner dans le cadre d'une étude approfondie sur les incidences de la cybercriminalité et la lutte contre ce phénomène (annexe I) eut été adopté, le représentant de la Colombie a fait la déclaration suivante et demandé qu'elle figure dans le rapport du groupe intergouvernemental d'experts à composition non limitée:

> 1. Lors de la réunion du groupe intergouvernemental d'experts à composition non limitée, de nombreuses délégations se sont déclarées préoccupées par l'utilisation malveillante fréquente des nouvelles technologies de l'information et de la communication à des fins terroristes. Dans ce contexte, un représentant du Secrétariat a fait un exposé sur le travail accompli par l'Office des Nations Unies contre la drogue et le crime concernant ce problème, et en particulier l'utilisation malveillante d'Internet. Étant donné que l'étude de la cybercriminalité doit être approfondie et complète, elle devrait répondre à toutes les préoccupations exprimées. Il est donc essentiel que tous les aspects des liens entre terrorisme et cybercriminalité soient abordés dans l'étude. Les organisations terroristes utilisent ces technologies de différentes manières, et notamment:
>
> a) À des fins de propagande;
>
> b) Pour collecter des informations;
>
> c) Comme outil de formation;
>
> d) Pour organiser des activités illicites;
>
> e) Pour diffuser des informations à des fins de recrutement et d'incitation;
>
> f) À des fins de stockage et de transmission d'informations en toute sécurité;
>
> g) Pour s'attaquer aux réseaux informatiques eux-mêmes.

2. Dans l'intérêt du consensus, la Colombie accepte les propositions de la délégation de l'Argentine concernant cette question, mais demande qu'il soit pris note des points suivants dans le rapport du groupe intergouvernemental d'experts à composition non limitée sur les travaux de sa première réunion:

a) À propos du paragraphe 12 de l'ensemble de thèmes à examiner dans le cadre d'une étude approfondie sur les incidences de la cybercriminalité et la lutte contre ce phénomène (annexe I), où il est fait référence à un inventaire des actes qui ont été érigés en infraction, la Colombie considère que ceux-ci englobent le terrorisme;

b) À propos du titre qui précède le paragraphe 18 de ce document, la Colombie considère que les défis posés par la cybercriminalité englobent également le terrorisme;

c) La Colombie exprime aussi l'espoir que l'étude portera sur l'éventuelle utilisation malveillante, par des terroristes, d'outils pouvant être employés pour commettre des actes de cybercriminalité, tels que ceux mentionnés dans le paragraphe 25 de ce document.

Annexe I

Ensemble de thèmes à examiner dans le cadre d'une étude approfondie sur les incidences de la cybercriminalité et la lutte contre ce phénomène

I. Introduction

1. À l'occasion du douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale qui s'est tenu en 2010, les États Membres ont examiné de manière relativement détaillée la question de la cybercriminalité et décidé d'inviter la Commission pour la prévention du crime et la justice pénale à convoquer un groupe intergouvernemental d'experts à composition non limitée en vue de réaliser une étude approfondie sur le phénomène de la cybercriminalité et sur les mesures prises pour y faire face. Cette recommandation a été adoptée par la Commission pour la prévention du crime et la justice pénale, puis par le Conseil économique et social dans sa résolution 2010/18 et par l'Assemblée générale dans sa résolution 65/230.

2. Conformément au paragraphe 42 de la "Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux: les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation", l'étude approfondie portera sur ce qui suit:

> Le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé, y compris en matière d'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin d'examiner les options envisageables pour renforcer les mesures juridiques ou autres prises à l'échelle nationale et internationale face à la cybercriminalité et pour en proposer de nouvelles.

3. Le paragraphe 42 de la Déclaration de Salvador identifie donc les diverses questions de fond que l'étude devrait aborder (le phénomène de la cybercriminalité, les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale), ainsi que la perspective qu'elle devrait adopter (les mesures prises par les États Membres, la communauté internationale et le secteur privé) et l'objectif recherché (examiner les options envisageables pour renforcer les mesures prises et proposer de nouvelles mesures nationales et internationales, juridiques ou autres, face à la cybercriminalité).

4. Afin d'élaborer un projet de structure pour cette étude, ces trois dimensions (questions de fond, perspective et objectif) ont été déclinées en 12 thèmes en adéquation avec le mandat fixé dans la Déclaration. Ces 12 thèmes sont regroupés ci-dessous par catégories.

Le phénomène de la cybercriminalité (thèmes 1 à 3)

5. Dans la Déclaration de Salvador, les États Membres indiquent que l'étude devrait porter sur le phénomène de la cybercriminalité. Afin de traiter l'ensemble

des problèmes posés par la cybercriminalité, trois principaux domaines ont été identifiés, qui devront être analysés en détail:

a) Le phénomène de la cybercriminalité (thème 1);

b) Informations statistiques (thème 2);

c) Défis que pose la cybercriminalité (thème 3).

Mesures juridiques prises pour lutter contre la cybercriminalité (thèmes 4 à 9)

6. Dans la Déclaration de Salvador, les États Membres appellent de leurs vœux une étude sur les mesures juridiques prises pour lutter contre la cybercriminalité, y compris en matière d'échange d'informations sur les législations nationales, les meilleures pratiques et la coopération internationale. Outre les aspects généraux relatifs à l'harmonisation de la législation, des groupes spécifiques de mesures juridiques ont été identifiés:

a) Approches communes en matière de législation (thème 4);

b) Incrimination (thème 5);

c) Règles de procédure (thème 6);

d) Coopération internationale (thème 7);

e) Garanties et conditions, notamment protection des droits fondamentaux de la personne humaine et des données personnelles;

f) Respect du principe d'égalité souveraine des États et de non-ingérence dans les affaires d'autres États;

g) Preuves électroniques (thème 8);

h) Rôles et responsabilités des prestataires de services et du secteur privé (thème 9).

Prévention du crime, moyens existants en matière de justice pénale et autres réponses à la cybercriminalité (thème 10)

7. La Déclaration de Salvador fait référence à l'étude non seulement des mesures juridiques prises pour lutter contre la cybercriminalité, mais aussi d'autres types de mesures plus générales visant cette même fin.

Organisations internationales (thème 11)

8. Dans la Déclaration de Salvador, les États Membres appellent de leurs vœux une analyse des mesures prises par les États Membres, la communauté internationale et le secteur privé. Si les questions relatives aux mesures juridiques prises par la communauté internationale sont abordées à la rubrique traitant des mesures juridiques, une rubrique distincte consacrée aux mesures prises par la communauté internationale facilitera l'analyse de points plus généraux comme le rapport entre les approches régionales et internationales.

Assistance technique (thème 12)

9. Compte tenu des incidences de la cybercriminalité sur les pays en développement et de la nécessité d'une approche uniforme et coordonnée pour lutter contre ce phénomène, l'assistance technique est l'un des domaines spécifiques devant être couvert par l'étude approfondie.

II. Présentation détaillée des thèmes

Thème 1. Le phénomène de la cybercriminalité

Contexte

10. Les termes "criminalité informatique" et, plus précisément, "cybercriminalité" désignent une catégorie d'actes délictuels. Ce type d'actes pose des défis liés tant à la grande diversité des infractions concernées qu'à l'apparition rapide de nouvelles méthodes de commission des infractions.

L'essor de la criminalité informatique et de la cybercriminalité

11. Dans les années 1960, lorsque les systèmes informatiques à transistors ont été créés et que les ordinateurs ont commencé à se répandre[1], les actes incriminés étaient essentiellement les dommages matériels causés aux systèmes informatiques et aux données stockées[2]. Au cours des années 1970, les infractions traditionnelles contre les systèmes informatiques[3] ont laissé la place à de nouvelles formes d'infractions[4] comme l'usage illégal de systèmes informatiques[5] et la manipulation[6] de données électroniques[7]. Le passage d'opérations manuelles à des opérations effectuées par ordinateur a fait apparaître une nouvelle forme de criminalité: la fraude informatique[8]. Dans les années 1980, les ordinateurs individuels sont devenus de plus en plus courants et de nombreuses infrastructures essentielles ont

---

[1] S'agissant des problèmes connexes, voir R. T. Slivka et J. W. Darrow, "Methods and problems in computer security", *Rutgers Journal of Computers and the Law*, vol. 5, n° 2 (1976), p. 217 à 269.

[2] McLaughlin, "Computer crime: the Ribicoff Amendment to United States Code, Title 18", *Criminal Justice Journal*, vol. 2, 1978, p. 217 et suiv.

[3] Gemignani, "Computer crime: the law in '80", *Indiana Law Review*, vol. 13, 1980, p. 681.

[4] McLaughlin, "Computer crime: the Ribicoff Amendment".

[5] Freed, *Materials and Cases on Computer and Law* (s.l., 1971), p. 65.

[6] Bequai, "The electronic criminals: how and why computer crime pays", *Barrister*, vol. 4, 1977, p. 8 et suiv.

[7] *Criminological Aspects of Economic Crime: Proceedings of the 12th European Conference of Directors of Criminological Research Institutes (November 1976)*, vol. XV, Collected Studies in Criminological Research (Strasbourg, Conseil de l'Europe, 1977), p. 225 et suiv.; États-Unis d'Amérique, *Staff Study of Computer Security in Federal Programs, Committee on Government Operations – United States Senate* (Washington D. C., United States Government Printing Office, 1977).

[8] McLaughlin, "Computer crime: the Ribicoff Amendment" (voir note de bas de page n° 2); Bequai, "Computer crime: a growing and serious problem", *Police Law Quarterly*, vol. 6, 1977, p. 22.

commencé à dépendre de l'informatique[9]. L'un des effets secondaires de la diffusion des systèmes informatiques a été l'intérêt accru suscité par les logiciels, en conséquence de quoi les premières formes de piratage de logiciels et d'infractions liées aux brevets sont apparues[10]. En outre, le début de l'interconnexion des systèmes informatiques a permis à des délinquants de s'introduire dans des systèmes sans être présents sur les lieux de l'infraction[11]. L'avènement, dans les années 1990, de l'interface graphique (World Wide Web), qui a été suivi d'une augmentation rapide du nombre d'utilisateurs d'Internet, a fait apparaître de nouveaux comportements délictuels. La diffusion d'images d'enfants maltraités, par exemple, est passée de l'échange physique de livres et de cassettes à la diffusion en ligne par le biais de sites Web et de services Internet[12]. La criminalité informatique, jusque-là commise à l'échelle locale, est devenue transnationale avec Internet. La première décennie du XXI^{e} siècle a été dominée par l'adoption de nouvelles méthodes très élaborées pour commettre des infractions telles que le "hameçonnage"[13] et les attaques par réseaux d'"ordinateurs zombies"[14], et par de nouvelles applications des technologies telles que la communication vocale par le protocole Internet (VoIP)[15] et l'"informatique en nuage"[16], qui présentent des difficultés pour les services de détection et de répression.

---

[9] E. A. Glynn, "Computer abuse: the emerging crime and the need for legislation", *Fordham Urban Law Journal*, vol. 12, n° 1 (1983-1984), p. 73.

[10] BloomBecker, "The trial of computer crime", *Jurimetrics Journal*, vol. 21, 1981, p. 428; W. Schmidt, "Legal proprietary interests in computer programs: the American experience", *Jurimetrics Journal*, vol. 21, 1981, p. 345 et suiv.; M. Dunning, "Some aspects of theft of computer software", *Auckland University Law Review*, vol. 4, n° 3 (1982), p. 273 et suiv.; Weiss, "Pirates and prizes: the difficulties of protecting computer software", *Western State University Law Review*, vol. 11, 1983, p. 1 et suiv.; R. P. Bigelow, "The challenge of computer law", *Western England Law Review*, vol. 7, n° 3 (1985), p. 401; G. Thackeray, "Computer-related crimes: an outline", *Jurimetrics Journal*, vol. 25, n° 3 (1985), p. 300 et suiv.

[11] Yee, "Juvenile computer crime: hacking — criminal and civil liability*", Comm/Ent Law Journal*, vol. 7, 1984, p. 336 et suiv.; "Who is calling your computer next? Hacker!", *Criminal Justice Journal*, vol. 8, 1985, p. 89 et suiv.; A. M. Wagner, "The challenge of computer-crime legislation: how should New York respond?", *Buffalo Law Review*, vol. 33, n° 3 (1984), p. 777 et suiv.

[12] "Child pornography", étude thématique établie pour le deuxième Congrès mondial contre l'exploitation sexuelle des enfants à des fins commerciales, Yokohama (Japon), 12-20 décembre 2001, p. 17; "Sexual exploitation of children over the Internet", rapport établi à l'attention de la Commission sur l'énergie et le commerce, Chambre des représentants des États Unis, 109^{e} congrès, janvier 2007, p. 9.

[13] Le terme "hameçonnage" désigne un acte visant à amener la victime à révéler des informations personnelles ou confidentielles. Il décrivait à l'origine l'utilisation de courriers électroniques pour récupérer ("hameçonner") des mots de passe et des données financières auprès des internautes. Pour plus d'informations, voir Union internationale des télécommunications, *Comprendre la cybercriminalité: guide pour les pays en développement* (Genève, 2009), chap. 2.8.4.

[14] Un réseau d'"ordinateurs zombies" est un groupe d'ordinateurs piratés exécutant un logiciel contrôlé de l'extérieur. Pour plus d'informations, voir Clay Wilson, "Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress", Congressional Research Service Report RL32114, 2007, p. 4.

[15] M. Simon et J. Slay, "Voice over IP: forensic computing implications", document établi pour la quatrième Conférence australienne de criminalistique informatique, Perth, 4 décembre 2006.

[16] Cristos Velasco San Martin, "Jurisdictional aspects of cloud computing", document présenté lors de la Conférence Octopus Interface: Coopération contre la cybercriminalité du Conseil de

Portée de l'étude

12. Pour ce qui est de ce thème, l'étude portera sur le phénomène même de la cybercriminalité et non sur les mesures prises pour y faire face:

a) Analyse du phénomène de la cybercriminalité en fonction des actes visés par les législations en vigueur;

b) Inventaire des actes qui sont érigés en infraction;

c) Inventaire des actes qui ne sont pas encore érigés en infraction;

d) Aperçu des infractions de double nature (telles que le "hameçonnage") et des évolutions prévisibles;

e) Inventaire de cas pertinents;

f) Examen de l'importance d'une définition de la cybercriminalité.

Thème 2. Informations statistiques

Contexte

13. Les statistiques sur la criminalité offrent une base pour la discussion et la prise de décisions par les dirigeants et les universitaires[17]. En outre, la disponibilité d'informations précises sur l'étendue réelle de la cybercriminalité peut permettre aux services de détection et de répression d'améliorer les stratégies de lutte contre la cybercriminalité, elle peut permettre de prévenir d'éventuelles attaques et favoriser la promulgation d'une législation plus appropriée et plus efficace.

État actuel des statistiques sur la cybercriminalité

14. Les informations sur l'étendue de la criminalité sont généralement tirées de statistiques et d'études en la matière[18]. Ces deux sources présentent des inconvénients lorsqu'elles sont utilisées pour élaborer des recommandations de politique générale. Premièrement, les statistiques sur la criminalité sont généralement établies au niveau national et ne reflètent pas l'étendue du phénomène au niveau international. Alors qu'il serait théoriquement possible de combiner les données provenant de différents États, cette approche ne produirait pas d'informations fiables en raison des différences entre les législations et les pratiques de comptage[19]. Combiner et comparer des statistiques nationales requiert un certain

---

l'Europe, Strasbourg, 10 et 11 mars 2009; M. Gercke, "Die Auswirkungen von Cloud Storage auf die Tätigkeit der Strafverfolgungsbehörden", dans *Inside the Cloud: Neue Herausforderungen für das Informationsrecht*, J. Taeger et A. Wiebe (sous la direction de), Oldenburger Tagungsbände (Edewecht, Allemagne, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2009), p. 499 et suiv.

[17] P. A. Collier et B. J. Spaul, "Problems in policing computer crime", *Policing and Society*, vol. 2, n° 4 (1992), p. 308.

[18] Concernant l'importance nouvelle des statistiques sur la criminalité, voir D. A. Osborne et S. C. Wernicke, *Introduction to Crime Analysis: Basic Resources for Criminal Justice Practice* (Binghamton, New York, Haworth Press, 2003), p. 1 et suiv.

[19] Dans ce contexte, voir *Overcoming Barriers to Trust in Crimes Statistics: England and Wales*, Monitoring Report n° 5, rapport provisoire (Londres, United Kingdom Statistics Authority, décembre 2009), p. 9, disponible sur le site www.statisticsauthority.gov.uk.

degré de compatibilité[20] qui fait défaut en matière de cybercriminalité. Même si les infractions relevant de la cybercriminalité sont comptabilisées, ce n'est pas forcément séparément[21].

15. Deuxièmement, les statistiques ne peuvent rendre compte que des infractions qui ont été constatées et signalées[22]. S'agissant de la cybercriminalité en particulier, le nombre de cas non signalés pourrait être élevé[23]. Les entreprises craignent parfois qu'une publicité négative ne porte atteinte à leur réputation[24]. Si une entreprise fait savoir que des pirates ont eu accès à ses serveurs, cela peut entraîner une perte de confiance des clients et, partant, des coûts qui risquent de dépasser le montant des pertes occasionnées par l'attaque subie. Cependant, si les infractions ne sont pas signalées ni poursuivies, les délinquants risquent de récidiver. Les victimes pensent parfois que les services de détection et de répression ne parviendront pas à identifier les auteurs des infractions[25] et qu'il y a donc peu d'intérêt à les signaler[26]. L'automatisation des attaques cybercriminelles, qui permet aux cyberdélinquants d'engranger d'importants profits au moyen de nombreuses attaques rapportant

---

[20] A. Alvazzi del Frate, "Crime and criminal justice statistics challenges", dans *International Statistics on Crime and Justice*, S. Harrendorf, M. Heiskanen et S. Malby (sous la direction de), HEUNI Publication Series, n° 64 (Helsinki, Institut européen pour la prévention du crime et la lutte contre la délinquance, affilié à l'Organisation des Nations Unies, 2010), p. 168., disponible (en anglais) à l'adresse www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

[21] "Computer crime", Parliamentary Office of Science and Technology, *Postnote*, n° 271, octobre 2006, p. 3.

[22] Concernant les problèmes connexes, voir M. E. Kabay, "Understanding studies and surveys of computer crime", juin 2009, disponible à l'adresse www.mekabay.com/methodology/crime_stats_methods.pdf.

[23] "Le Federal Bureau of Investigation (FBI) des États-Unis a prié les entreprises de ne pas passer sous silence les attaques de "hameçonnage" et celles commises contre leurs systèmes de technologie de l'information, mais d'en informer les autorités pour qu'elles se fassent une meilleure idée des activités délictuelles menées sur Internet. "Le fait que certaines entreprises craignent visiblement davantage la mauvaise publicité que les conséquences d'une attaque lancée par des pirates nous pose des problèmes", a expliqué Mark Mershon, chef par intérim du bureau du FBI de New York. Voir "FBI wants to know more about hacker attacks", *Heise News*, 27 octobre 2006, disponible à l'adresse www.h-online.com/security/news/item/FBI-wants-to-know-more-about-hacker-attacks-731717.html. Voir également "Comments on computer crime: Senate Bill S. 240", *Memphis State University Law Review*, 1980, p. 660.

[24] Voir N. Mitchinson et R. Urry, "Crime and abuse in e-business", dans *IPTS Report*, n° 57, 2001, p. 18 à 22; Collier et Spaul, "Problems in policing computer crime" (voir note de bas de page n° 17), p. 310.

[25] Voir Collier et Spaul, "Problems in policing computer crime" (voir note de bas de page n° 17), p. 310; R. G. Smith, "Investigating cybercrime: barriers and solutions", document établi pour l'ACFE (Association of Certified Fraud Examiners), Pacific Rim Fraud Conference, Sydney, 11 septembre 2003, p. 2, disponible à l'adresse www.aic.gov.au/about_aic/research_programs/staff/smith_russell.aspx.

[26] Les journaux et chaînes de télévision limitent leur couverture des enquêtes résolues à des cas spectaculaires, comme lorsqu'un pédophile est identifié grâce au décryptage de photos manipulées. Pour plus d'informations sur ce type de cas et la couverture médiatique qu'il reçoit, voir "Interpol in appeal to find paedophile suspect", *New York Times*, 9 octobre 2007, disponible à l'adresse www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin, ainsi que les informations fournies sur le site Web de l'Organisation internationale de police criminelle (INTERPOL), à l'adresse www.interpol.int/Public/THB/vico/Default.asp.

chacune un petit montant (cas de fraude par demande d'avance d'argent, notamment)[27], pourrait avoir des incidences importantes en matière d'infractions non signalées. En effet, lorsque les montants perdus sont peu élevés, les victimes préfèrent parfois s'épargner les longues procédures de signalement à la police. En pratique, les cas signalés concernent souvent des montants extrêmement élevés[28].

Portée de l'étude

16. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Collecte des statistiques, études et analyses les plus récentes sur la prévalence et l'ampleur de la cybercriminalité;

b) Appréciation de la valeur des statistiques pour formuler des recommandations de politique générale;

c) Identification d'éventuels obstacles à la collecte de statistiques exactes;

d) Identification des pays qui rassemblent des statistiques spécifiques sur la cybercriminalité;

e) Évaluation de la nécessité de recueillir des données statistiques sur la cybercriminalité et de l'intérêt que ces données présentent;

f) Examen des techniques pouvant être utilisées pour recueillir ces informations;

g) Discussion sur l'éventuelle élaboration d'un modèle d'autorité centrale chargée de rassembler des données statistiques.

Thème 3. Défis que pose la cybercriminalité

Contexte

17. Une grande attention est actuellement accordée à l'élaboration de stratégies visant les défis spécifiquement liés à la cybercriminalité. Il y a deux raisons à cela: premièrement, certains instruments nécessaires aux enquêtes en matière de cybercriminalité sont nouveaux et exigent donc d'importants travaux de recherche, et, deuxièmement, les enquêtes sur les infractions liées aux réseaux se heurtent à des difficultés bien particulières qui sont inconnues des enquêtes traditionnelles.

Défis que pose la lutte contre la cybercriminalité et contre les menaces connexes

18. La liste des défis techniques et juridiques spécifiques que pose la cybercriminalité est longue. Le fait que des délinquants puissent commettre des actes cybercriminels à l'aide d'outils qui ne nécessitent pas de connaissances

---

[27] Voir Royaume-Uni, Agence de lutte contre la grande criminalité organisée, "International crackdown on mass marketing fraud revealed", 2007.

[28] Selon le rapport intitulé *2006 NW3C Internet Crime Report*, publié par le National White Collar Crime Center, seulement 1,7 % des pertes signalées, exprimées en dollars des États-Unis, était lié à la fraude dite de la "lettre nigériane", mais chacun des cas signalés représentait une perte moyenne de 5 100 dollars. Si le nombre d'infractions signalées est très bas, les pertes moyennes sont quant à elles élevées.

techniques approfondies, tels que les logiciels[29] conçus pour localiser les ports ouverts d'un ordinateur ou déjouer un système de protection par mot de passe, n'en est qu'un exemple[30]. Le repérage des délinquants constitue également un défi. Bien que les utilisateurs de services Internet laissent de nombreuses traces, les délinquants savent entraver les enquêtes en dissimulant leur identité. Si, par exemple, ils commettent leurs infractions à l'aide de terminaux Internet publics ou de réseaux sans fil ouverts, il peut s'avérer difficile de les identifier. Les enquêtes sur les affaires de cybercriminalité posent aussi un problème plus général lié au fait que, d'un point de vue technologique, Internet offre peu d'instruments de contrôle aux services de détection et de répression. Internet avait été conçu à l'origine comme un réseau militaire[31] reposant sur une architecture décentralisée dont les principales fonctionnalités devaient rester intactes même en cas d'attaque des éléments du réseau. Cette approche décentralisée n'avait pas pour but de faciliter les enquêtes pénales ou de prévenir les attaques au sein du réseau, et les techniques d'enquête qui nécessitent des moyens de contrôle posent des problèmes particuliers dans ce contexte[32].

Portée de l'étude

19. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Inventaire complet des défis que pose la lutte contre la cybercriminalité;

b) Résumé des pratiques optimales, sur les plans tant technique que juridique, pour relever ces défis.

Thème 4. Approches communes en matière de législation

Contexte

20. Au cours des 20 dernières années, plusieurs pays et organisations régionales ont élaboré une législation et des cadres juridiques pour lutter contre la cybercriminalité. Malgré l'apparition de caractéristiques communes, d'importantes différences subsistent entre les législations nationales.

Différences nationales et régionales.

21. L'une des raisons qui explique les différences entre les législations, que ce soit entre les pays ou entre les régions, est que les incidences de la cybercriminalité ne sont pas les mêmes partout, comme en témoigne la lutte contre l'envoi massif de

---

[29] "Websense", *Security Trends Report 2004*, p. 11; États-Unis d'Amérique, General Accounting Office, *Information Security: Computer Controls over Key Treasury Internet Payment System*, GAO-03-837 (Washington, D. C., 2003), p. 3; U. Sieber, "La menace de la cybercriminalité", dans *Criminalité organisée en Europe: la menace de la cybercriminalité (2004)* (Strasbourg, Éditions du Conseil de l'Europe, 2005).

[30] K. Ealy, "A new evolution in hack attacks: a general overview of types, methods, tools, and prevention", SANS Institute, 2003, p. 9.

[31] Pour un bref historique d'Internet, y compris ses origines militaires, voir B. Leiner *et al.*, "A brief history of the Internet", disponible à l'adresse www.isoc.org/internet/history/brief.shtml.

[32] H. F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Pittsburgh, Carnegie Mellon University, Software Engineering Institute, 2002).

courrier électronique non sollicité (pourriel)[33], phénomène qui pose davantage problème dans les pays en développement que dans les pays développés en raison du manque de ressources et des coûts qu'il représente[34]. Pour ce qui est des contenus illégaux, certains pays et régions peuvent incriminer la diffusion d'informations dont on considérera qu'elle ressortit à la liberté d'expression[35] dans d'autres pays ou régions[36].

22. La cybercriminalité étant une infraction de nature véritablement transnationale[37], la coopération internationale est essentielle pour que les enquêtes et poursuites aboutissent[38]. Une coopération internationale efficace nécessite un

---

[33] *Comprendre la cybercriminalité: guide pour les pays en développement* (voir note de bas de page n° 13), chap. 2.6.7.

[34] Voir Organisation de coopération et de développement économiques, "Spam issues in developing countries", document DSTI/CP/ICCP/SPAM(2005)6/FINAL, 26 mai 2005, p. 4, disponible à l'adresse www.oecd.org/dataoecd/5/47/34935342.pdf.

[35] Concernant le principe de la liberté d'expression, voir T. L. Tedford et D. A. Herbeck, *Freedom of Speech in the United States*, 5e éd. (State College, Pennsylvania, Strata, 2005); E. Barendt, *Freedom of Speech* (Oxford, Oxford University Press, 2007); C. E. Baker, *Human Liberty and Freedom of Speech* (New York, Oxford University Press, 1989); J. W. Emord, *Freedom, Technology and the First Amendment* (San Francisco, Pacific Research Institute for Public Policy, 1991); concernant l'importance de ce principe en matière de surveillance électronique, voir C. Woo et M. So, "The case for Magic Lantern: September 11 Highlights — the need for increasing surveillance", *Harvard Journal of Law and Technology*, vol. 15, n° 2 (2002), p. 530 et suiv.; M. Chesterman, *Freedom of Speech in Australian Law: A Delicate Plant* (Aldershot, Hampshire, Ashgate, 2000); E. Volokh, "Freedom of speech, religious harassment law, and religious accommodation law", *Loyola University Chicago Law Journal*, vol. 33, 2001, p. 57 et suiv., disponible à l'adresse www.law.ucla.edu/volokh/harass/religion.pdf; H. Cohen, "Freedom of speech and press: exceptions to the First Amendment", Congressional Research Service Report 95-815, 2009, disponible à l'adresse www.fas.org/sgp/crs/misc/95-815.pdf.

[36] Ce sont des considérations liées à la liberté d'expression (par exemple le premier amendement à la Constitution des États-Unis) qui expliquent que certains actes racistes n'aient pas été érigés en infraction par la Convention sur la cybercriminalité (Conseil de l'Europe, *Série des traités européens*, n° 185), mais leur incrimination a été prévue dans le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (Conseil de l'Europe, *Série des traités européens*, n° 189). Voir aussi le Rapport explicatif sur le Protocole additionnel, disponible à l'adresse http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm.

[37] Concernant l'étendue des attaques transnationales dans les cas les plus graves d'attaques informatiques, voir A. D. Sofaer et S. E. Goodman, "Cyber crime and security: the transnational dimension", dans *The Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer et S. E. Goodman (sous la direction de), Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), p. 7, disponible à l'adresse http://media.hoover.org/documents/0817999825_1.pdf.

[38] S'agissant de la nécessité d'une coopération internationale dans la lutte contre la cybercriminalité, voir T. L. Putnam et D. D. Elliott, "International responses to cyber crime", dans *Transnational Dimension of Cyber Crime and Terrorism*, Sofaer et Goodman (sous la direction de), Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), p. 35 et suiv., disponible à l'adresse http://media.hoover.org/documents/0817999825_35.pdf; et Sofaer et Goodman, "Cyber crime and security: the transnational dimension".

certain degré de compréhension mutuelle et l'adoption d'approches communes en matière de législation afin qu'il ne soit pas créé de refuges[39].

23. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Analyse des efforts faits pour adopter des approches communes en matière de législation relative à la cybercriminalité;

b) Autres éléments concernant l'adoption d'approches communes en matière de législation relative à la cybercriminalité, y compris la gravité perçue des actes et l'efficacité des normes relatives aux droits de l'homme;

c) Inventaire des modalités selon lesquelles les pays appliquent les normes juridiques des organisations régionales et analyse visant à déterminer quelles techniques peuvent contribuer à la cohérence de ces approches;

d) Analyse de la mesure dans laquelle les différences de législation relative à la cybercriminalité affectent la coopération internationale.

Thème 5. Incrimination

Contexte

24. Pour mener des enquêtes et des poursuites efficaces, il faut que les actes non encore visés par la législation en vigueur soient érigés en de nouvelles infractions. Non seulement l'existence d'une législation adaptée est pertinente pour mener des enquêtes au niveau national, elle a aussi des incidences en matière de coopération internationale, comme indiqué plus haut.

Droit pénal matériel

25. La plupart des cadres généraux mis en place à l'échelon régional pour lutter contre la cybercriminalité comprennent un ensemble de dispositions de droit pénal matériel destinées à combler les lacunes des législations nationales. Habituellement, ces dispositions visent notamment à incriminer l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système, la falsification informatique et la fraude informatique. Certains dispositifs nationaux pourraient aller plus loin et incriminer des actes comme la production et la distribution d'outils (logiciels ou matériels, par exemple) pouvant être utilisés aux fins de la commission d'infractions relevant de la cybercriminalité ou à des fins terroristes, les actes se rapportant aux images d'enfants maltraités, la prise de contact avec des inconnus sur Internet en vue de la commission d'infractions à caractère sexuel, ou l'incitation à la haine.

---

[39] S'agissant du principe de double incrimination dans les enquêtes internationales, voir le Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique, "United Nations Manual on the Prevention and Control of Computer-Related Crime", *International Review of Criminal Policy*, n° 43 et 44, 1994 (publication des Nations Unies, numéro de vente: E.94.IV.5), par. 269, disponible en anglais à l'adresse www.uncjin.org/Documents/EighthCongress.html; Judge Stein Schjolberg et Amanda M. Hubbard, "Harmonizing national legal approaches on cybercrime", document établi pour l'Union internationale des télécommunications, réunion thématique sur la cybersécurité du Sommet mondial sur la société de l'information, Genève, 28 juin-1er juillet 2005, p. 5.

Portée de l'étude

26. L'étude s'appuiera sur les conclusions qui auront été formulées concernant le thème 1, relatif au phénomène de la cybercriminalité:

a) Inventaire des approches adoptées aux niveaux national et régional pour incriminer les actes de cybercriminalité, y compris en ce qui concerne la participation et la tentative;

b) Évaluation des meilleures pratiques en matière d'incrimination;

c) Analyse des différences entre les approches adoptées dans des traditions et des systèmes juridiques variés pour incriminer les actes de cybercriminalité.

Thème 6. Règles de procédure

Contexte

27. Pour mener des enquêtes efficaces, les services de détection et de répression doivent pouvoir recourir à des procédures d'enquête qui leur permettent de prendre les mesures voulues pour identifier les auteurs d'infractions et recueillir les preuves nécessaires à la procédure pénale[40]. Ces mesures peuvent être les mêmes que celles utilisées dans les enquêtes traditionnelles ne concernant pas la cybercriminalité. Toutefois, du fait que son auteur ne se trouve pas nécessairement sur le lieu de l'infraction ni même à proximité de celui-ci, les enquêtes sur la cybercriminalité devront très probablement être menées d'une manière différente[41].

Mesures d'enquête

28. La plupart des cadres généraux mis en place au niveau régional pour lutter contre la cybercriminalité contiennent non seulement des dispositions sur les actes de cybercriminalité proprement dits, mais aussi un ensemble de dispositions destinées spécifiquement à faciliter les enquêtes sur la cybercriminalité. Habituellement, ces dispositions prévoient notamment des procédures spécifiques de fouille et de saisie, la protection rapide des données informatiques, la divulgation des données stockées, l'interception de données relatives au contenu et la collecte des données relatives au trafic.

---

[40] Concernant les approches de lutte contre la cybercriminalité axées sur les utilisateurs, voir S. Görling, "The myth of user education", document établi pour la Virus Bulletin Conference, Montréal, 11-13 octobre 2006, disponible à l'adresse www.virusbtn.com/conference/vb2006/abstracts/Gorling.xml. Voir également la déclaration faite par Jean-Pierre Chevènement, alors Ministre français de l'intérieur, à la Conférence du Groupe des Huit sur la sécurité et la confiance dans le cyberespace tenue à Paris en 2000: "Plus largement, nous avons un effort pédagogique à faire. Tous les usagers doivent savoir ce qu'ils peuvent faire et ne pas faire sur Internet et doivent être avertis des dangers potentiels. C'est un travail de prévention qui se fera naturellement au même rythme qu'Internet se généralisera."

[41] Grâce aux protocoles utilisés pour les communications sur Internet et à l'accessibilité mondiale d'Internet, il n'est que très rarement nécessaire d'être physiquement présent sur le lieu où un service est effectivement fourni. Le lieu de l'action étant sans rapport avec le lieu de l'infraction, de nombreuses infractions liées à Internet ont un caractère international. Concernant l'indépendance entre le lieu de l'action et les conséquences de l'infraction, voir *Comprendre la cybercriminalité: Guide pour les pays en développement* (voir note de bas de page n° 13), chap. 3.2.7.

29. Actuellement, les services de détection et de répression se trouvent face à des technologies récemment mises au point qui font que les méthodes d'enquête classiques sont impuissantes. Nombre de ces problèmes n'ont pas encore été abordés.

Portée de l'étude

30. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Inventaire des exemples d'enquêtes qui ont montré que des mesures d'enquête spéciales étaient nécessaires pour les affaires de cybercriminalité;

b) Inventaire des différentes dispositions relatives aux enquêtes prévues dans les cadres juridiques nationaux et régionaux;

c) Aperçu des besoins des services de détection et de répression en matière de dispositions spéciales relatives aux enquêtes en matière de cybercriminalité pour s'attaquer aux problèmes posés par les nouvelles technologies;

d) Analyse des différences entre les approches propres à des traditions et des systèmes juridiques variés en ce qui concerne les dispositions relatives aux enquêtes sur la cybercriminalité.

Thème 7. Coopération internationale

Contexte

31. De plus en plus souvent, la cybercriminalité revêt une dimension internationale[42], en particulier parce que les délinquants qui opèrent sur Internet, réseau transnational par nature, ont rarement besoin d'être là où se trouve la victime. En raison de cette disjonction entre le lieu où se trouve la victime et celui où se trouve l'auteur de l'infraction ainsi que de la mobilité des délinquants, les services de détection et de répression et les autorités judiciaires sont appelés à coopérer à l'échelon international et à aider l'État qui s'est déclaré compétent[43]. Une coopération internationale efficace est l'un des principaux défis à relever pour lutter contre une criminalité de plus en plus internationalisée, en ce qui concerne tant les infractions traditionnelles que la cybercriminalité. Les différences entre les législations et les pratiques nationales peuvent rendre la coopération internationale difficile, tout comme le nombre relativement faible de traités et d'accords de

---

[42] Concernant la dimension internationale de la cybercriminalité, voir Mike Keyser, "The Council of Europe Convention on Cybercrime", *Journal of Transnational Law and Policy*, vol. 12, n° 2 (2003), p. 289, disponible à l'adresse www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; Sofaer et Goodman, "Cyber crime and security: the transnational dimension" (voir note de bas de page n° 37), p. 1 et suiv.

[43] Voir à ce sujet les *Guides législatifs pour l'application de la Convention des Nations Unies contre la criminalité transnationale organisée et protocoles s'y rapportant* (publication des Nations Unies, numéro de vente: F.05.V.2), p. 234, disponible à l'adresse http://www.unodc.org/pdf/crime/legislative_guides/French%20Legislative%20guide_Full%20version.pdf.

coopération internationale conclus entre États[44]. En outre, la question de savoir ce qui devrait être considéré comme revêtant un caractère international dans les affaires de cybercriminalité devrait être examinée et faire l'objet d'un consensus.

Instruments de coopération internationale

32. Le fondement juridique nécessaire à une coopération internationale formelle, qu'il s'agisse d'extradition, d'entraide judiciaire en matière pénale ou de coopération à des fins de confiscation, puise à différentes sources. Des dispositions relatives à la coopération internationale peuvent être incluses dans des accords régionaux et internationaux, comme c'est le cas dans la Convention des Nations Unies contre la criminalité transnationale organisée[45].

Portée de l'étude

33. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Inventaire des approches juridiques nationales adoptées pour déterminer le caractère international d'une affaire en matière de répression pénale des infractions liées à Internet;

b) Examen des options envisageables concernant des bases juridiques efficaces, notamment des bases internationales universelles, et d'autres mesures de lutte contre la cybercriminalité;

c) Difficultés qui font obstacle à une coopération internationale efficace, en particulier à l'extradition et à l'entraide judiciaire dans les affaires de cybercriminalité, notamment l'application du principe de double incrimination et les différences entre les techniques d'enquête;

d) Inventaire des dispositions nationales et internationales relatives à la coopération internationale qui sont pertinentes pour les enquêtes et les poursuites dans les affaires de cybercriminalité;

e) Inventaire d'exemples de meilleures pratiques se fondant sur des traités et arrangements bilatéraux et multilatéraux, et notamment des enseignements tirés du fonctionnement du réseau 24/7 de points de contact;

f) Inventaire des affaires de cybercriminalité impliquant une coopération internationale;

g) Rôle des moyens informels de coopération internationale tels que l'échange de renseignements, et difficultés qui se posent;

h) Aperçu des besoins des autorités compétentes en matière de coopération internationale;

---

[44] Carlos A. Gabuardi, "Institutional framework for international judicial cooperation: opportunities and challenges for North America", *Mexican Law Review*, vol. 1, n° 2 (2009), p. 156, disponible à l'adresse http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[45] Nations Unies, *Recueil des Traités*, vol. 2225, n° 39574; concernant la Convention, voir Jennifer M. Smith, "An international hit job: prosecuting organized crime acts as crimes against humanity", *Georgetown Law Journal*, vol. 97, 2009, p. 1, 118, disponible à l'adresse www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.

i) Identification de projets en cours et d'idées pour de futurs projets dans les domaines de la formation, de l'échange de données d'expérience, du renforcement des capacités et de l'assistance technique pour renforcer les capacités en matière de justice pénale et permettre aux pays de coopérer à l'échelon international.

Thème 8. Preuves électroniques

Contexte

34. Étant donné que de plus en plus d'informations sont conservées sous forme numérique, les éléments de preuve électroniques devraient être pris en compte dans le cadre des enquêtes sur la cybercriminalité mais aussi des enquêtes traditionnelles. L'informatique et les réseaux font désormais partie de la vie quotidienne dans les pays développés et, de plus en plus souvent, dans les pays en développement. Les capacités croissantes des disques durs[46] et le coût relativement faible[47] de la conservation des documents numériques par rapport au stockage des documents physiques ont contribué à l'augmentation du nombre de documents sous forme numérique[48]. À l'heure actuelle, beaucoup de données sont stockées sous forme numérique uniquement[49]. Compte tenu de cette évolution, les documents électroniques, tels que les fichiers de texte et les vidéos et photos numériques[50], jouent un rôle dans les enquêtes sur la cybercriminalité et les procédures judiciaires connexes[51].

---

[46] Voir D. Abramovitch, "A brief history of hard drive control", *IEEE Control Systems Magazine*, vol. 22, n° 3 (2002), p. 28 et suiv.; T. Coughlin, D. Waid et J. Porter, "The disk drive: 50 years of progress and technology innovation — the road to two billion drives", *Computer Technology Review*, avril 2005, disponible à l'adresse www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[47] S. M. Giordano, "Electronic evidence and the law", *Information Systems Frontiers*, vol. 6, n° 2 (2006), p. 161; S. D. Willinger et R. M. Wilson, "Negotiating the minefields of electronic discovery", *Richmond Journal of Law and Technology*, vol. 10, n° 5 (2004).

[48] Lange, Minster, Electronic Evidence and Discovery, p. 6.

[49] Chet Hosmer, "Proving the integrity of digital evidence with time", *International Journal of Digital Evidence*, vol. 1, n° 1 (2002), p. 1, disponible à l'adresse www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[50] Concernant la recevabilité et la fiabilité des éléments de preuve sous forme d'images numériques, voir Jill Witkowski, "Can juries really believe what they see? New foundational requirements for the authentication of digital images", *Washington University Journal of Law and Policy*, vol. 10, 2002, p. 267 et suiv.

[51] Michael Harrington, "A methodology for digital forensics", *Thomas M. Cooley Journal of Practical and Clinical Law*, vol. 7, 2004, p. 71 et suiv.; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science*, *Computers and the Internet*, 2e édition (Londres, Academic Press, 2004), p. 14. Concernant les cadres juridiques dans les différents pays, voir C. A. Rohrmann et J. S. A. Neto, "Digital evidence in Brazil", Digital Evidence and Electronic Signature Law Review, n° 5, 2008; M. Wang, "Electronic evidence in China", *Digital Evidence and Electronic Signature Law Review*, n° 5, 2008; P. Bazin, "An outline of the French Law on digital evidence", *Digital Evidence and Electronic Signature Law Review*, n° 5, 2008; A. B. Makulilo, "Admissibility of computer evidence in Tanzania", *Digital Evidence and Electronic Signature Law Review*, n° 4, 2007; R. Winick, "Search and seizures of computers and computer data", *Harvard Journal of Law and Technology*, vol. 8, n° 1 (1994), p. 76; F. Insa,

Règles relatives aux preuves électroniques

35. Les preuves électroniques posent un certain nombre de problèmes en ce qui concerne aussi bien leur collecte que leur recevabilité en tant que preuves[52]. Durant le processus de collecte, les enquêteurs doivent respecter certaines procédures et règles, notamment pour protéger l'intégrité des données. Les services de détection et de répression doivent pouvoir recourir à des mesures spéciales pour mener efficacement leurs enquêtes. Cela est particulièrement vrai en l'absence d'éléments de preuve traditionnels tels que les empreintes digitales ou les témoignages de personnes. Dans de tels cas, l'efficacité de l'identification d'un auteur d'infractions et des poursuites connexes dépend de la bonne collecte et de la bonne évaluation des preuves numériques[53].

36. La numérisation influe également sur la manière dont les services de détection et de répression et les tribunaux traitent les preuves[54]. Alors que les documents traditionnels sont simplement produits devant le tribunal, les preuves numériques exigent parfois la mise en œuvre de procédures particulières, par exemple l'impression des fichiers[55], qui font que ce ne sont pas des preuves traditionnelles.

Portée de l'étude

37. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Inventaire des dispositions, des garanties et des normes relatives à la collecte, à la préservation, au stockage, à l'analyse et à la recevabilité des preuves électroniques;

b) Analyse des différentes approches adoptées et identification des principes communs en matière de preuves électroniques dans des traditions et des systèmes juridiques variés;

c) Collecte de meilleures pratiques en matière de formation spécialisée, de renforcement des capacités et d'échanges de technologie;

d) Analyse du mécanisme d'échange transnational de preuves numériques.

"Situation report on the admissibility of electronic evidence in Europe", in *Syllabus to the European Certificate on Cybercrime and E-Evidence*, 2008, p. 213.

[52] Casey, *Digital Evidence and Computer Crime* (voir note de bas de page n° 51), p. 9.

[53] Concernant la nécessité de codifier la criminalistique informatique, voir R. Leigland et A. W. Krings, "A formalization of digital forensics", *International Journal of Digital Evidence*, vol. 3, n° 2 (2004).

[54] Concernant les difficultés rencontrées dans le traitement des preuves numériques selon les procédures et principes traditionnels, voir R. Moore, "To view or not to view: examining the plain view doctrine and digital evidence", *American Journal of Criminal Justice*, vol. 29, n° 1 (2004), p. 57 et suiv.

[55] Voir John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 2e édition (Hingham, Massachusetts, Charles River Media, 2005), p. 3. Concernant les débuts du débat au sujet de l'utilisation de tirages sur papier, voir Robinson, "The admissibility of computer printouts under the business records exception in Texas", *South Texas Law Journal*, vol. 12, 1970, p. 291 et suiv.

Thème 9. Rôles et responsabilités des prestataires de services et du secteur privé

Contexte

38. L'efficacité de la prévention de la cybercriminalité et des enquêtes sur les affaires qui en relèvent dépend de divers éléments. Même si l'auteur agit seul, la commission d'un acte de cybercriminalité implique automatiquement un certain nombre de personnes et d'entreprises. Étant donné la structure d'Internet, la transmission d'un simple message électronique exige l'intervention d'un certain nombre de prestataires de services: l'opérateur de services de messagerie électronique, les fournisseurs d'accès et les routeurs qui acheminent le message jusqu'au destinataire. La situation est comparable en ce qui concerne le téléchargement d'images d'enfants maltraités: le processus de téléchargement fait intervenir le fournisseur de contenus qui a mis les images en ligne (par exemple, sur un site Web), l'hébergeur qui a fourni le support de stockage pour le site Web, les routeurs qui ont acheminé les fichiers jusqu'à l'utilisateur et enfin le fournisseur d'accès qui a permis à l'utilisateur de se connecter à Internet.

39. Bien que l'accent soit souvent mis sur l'adoption d'une législation adaptée, le secteur privé continue de jouer un rôle important à la fois dans la prévention de la cybercriminalité et dans les enquêtes qui s'y rapportent. Sa participation aux enquêtes pose toutefois un certain nombre de problèmes.

Questions juridiques

40. Étant donné qu'un acte de cybercriminalité ne peut pas être commis sans impliquer de prestataires de services, mais aussi que ces prestataires sont rarement en mesure d'empêcher la commission de tels actes, la question se pose de savoir si leur responsabilité devrait être limitée. De la réponse qui y sera apportée dépend le développement économique de l'infrastructure des technologies de l'information et de la communication.

41. Le succès des efforts déployés par les services de détection et de répression est très souvent fonction de la coopération dont font preuve les fournisseurs d'accès à Internet, ce qui est inquiétant car, si la responsabilité de ces prestataires à l'égard des actes commis par leurs clients était imposée ou limitée, cela pourrait avoir des répercussions sur la coopération et le concours qu'ils apportent dans le cadre des enquêtes ainsi que sur l'action de prévention de la cybercriminalité.

Rôle des entreprises

42. Le rôle des entreprises dans la lutte contre la cybercriminalité est complexe; il peut aller de l'élaboration et la mise en œuvre de solutions destinées à protéger ses propres services contre toute utilisation impropre à la protection des utilisateurs et la fourniture d'un appui dans le cadre des enquêtes. Les mesures d'autoprotection adoptées par une entreprise font souvent partie intégrante de ses stratégies commerciales plus larges et ne nécessitent en général aucune base juridique particulière tant qu'elles ne comprennent pas de mesures de lutte active qui seraient illégales. Les mesures de protection prises au nom des utilisateurs ne posent pas non plus problème si elles sont prises avec l'agrément de ces derniers. La participation des entreprises aux enquêtes criminelles a en revanche posé des problèmes dans

beaucoup de pays et différentes approches ont été adoptées à cet égard. Dans certains pays, les entreprises participent à ces enquêtes sur une base purement volontaire et des lignes directrices ont été élaborées pour faciliter la coopération entre elles et les services de détection et de répression. D'autres pays ont adopté une démarche différente en imposant aux entreprises des obligations juridiques en vertu desquelles elles sont tenues de coopérer avec ces services.

Portée de l'étude

43. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Approches et pratiques relatives à la responsabilité des prestataires de services, notamment en fonction des différents types de prestataires;

b) Inventaire des rôles, natures et fonctions du secteur privé, notamment des prestataires de services;

c) Pratiques adoptées par le secteur privé pour prévenir la cybercriminalité et enquêter dans ce domaine;

d) Pratiques relatives à la coopération entre le secteur privé et les services de détection et de répression pour prévenir la cybercriminalité et enquêter dans ce domaine;

e) Mesure dans laquelle les prestataires de services nationaux et internationaux peuvent aider les services de détection et de répression à prévenir la cybercriminalité et à enquêter dans ce domaine;

f) Prise en charge des coûts de la cybercriminalité;

g) Évaluation des points forts et points faibles des approches existantes.

Thème 10. Prévention du crime, moyens existants en matière de justice pénale et autres réponses à la cybercriminalité

Contexte

44. Le débat sur la lutte contre la cybercriminalité porte le plus souvent sur les seules mesures juridiques, mais les stratégies adoptées dans ce domaine suivent généralement une approche plus complète.

Autres mesures

45. Outre l'adoption de mesures juridiques, la lutte contre la cybercriminalité comprend aussi l'adoption de mesures de prévention du crime, la mise en place de l'infrastructure nécessaire (en matériel et personnel, par exemple) pour enquêter sur les infractions et engager des poursuites, la formation de spécialistes en matière de lutte contre la cybercriminalité, la mise en place de meilleures pratiques, l'information des utilisateurs d'Internet et la mise en œuvre de solutions techniques pour prévenir la cybercriminalité ou enquêter sur les affaires qui en relèvent.

Portée de l'étude

46. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Aperçu des autres approches adoptées pour lutter contre la cybercriminalité;

b) Mesures de prévention de la cybercriminalité;

c) Définition des moyens de mesurer l'efficacité de ces approches;

d) Analyse du lien entre les différentes mesures et des possibilités de combiner ces mesures.

e) Rôle que pourrait jouer le monde universitaire, particulièrement par le biais de programmes d'enseignement adaptés et de travaux de recherche sur le phénomène de la cybercriminalité.

Thème 11. Organisations internationales

Contexte

47. Dans les années 1970 et 1980, la plupart des approches juridiques adoptées pour lutter contre la cybercriminalité ont été élaborées au niveau national. Dans les années 1990, la question de la cybercriminalité a commencé à être examinée au sein des organisations régionales et internationales, dont l'Assemblée générale, qui a adopté au fil des ans plusieurs résolutions sur la question[56], le Commonwealth (Loi type sur la cybercriminalité et extension potentielle aux données électroniques du Système relatif à l'entraide judiciaire en matière pénale), le Conseil de l'Europe (Convention sur la cybercriminalité), l'Union européenne (Décision-cadre relative aux attaques visant les systèmes d'information et Convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne), la Communauté d'États indépendants (CEI) (accord de coopération des pays de la CEI pour lutter contre les infractions commises dans le domaine informatique, 2001), l'Organisation des États américains et l'Organisation de Shanghai pour la coopération. Des organisations internationales, dont l'Union internationale des télécommunications, qui a entrepris des activités dans le cadre du Programme mondial cybersécurité, et l'Office des Nations Unies contre la drogue et le crime ont collecté des données et élaboré des études sur le sujet.

Harmonisation des normes

48. L'unification des normes relatives aux protocoles techniques s'est révélée concluante et soulève la question de savoir comment éviter les conflits entre les différentes approches adoptées à l'échelle internationale[57]. La Convention sur la cybercriminalité du Conseil de l'Europe et la Loi type du Commonwealth sur la cybercriminalité se fondent toutes deux sur l'approche la plus globale qui soit,

---

[56] Voir par exemple les résolutions 45/121, 55/63, 56/121 et 60/177 de l'Assemblée générale.

[57] Pour des informations plus détaillées, voir M. Gercke, "National, regional and international legislative approaches in the fight against cybercrime", *Computer Law Review International*, 2008, p. 7 et suiv.

puisqu'elles prévoient des dispositions de droit pénal matériel, des règles de procédure et des modalités de coopération internationale. Au titre de ce thème, il serait possible d'examiner les cadres existants afin d'identifier leur portée, leurs points forts et leurs points faibles ainsi que d'éventuelles lacunes.

Portée de l'étude

49. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Inventaire des meilleures pratiques des organisations régionales et internationales, y compris du système des Nations Unies;

b) Points forts et points faibles des approches existantes;

c) Analyse des lacunes des approches juridiques adoptées sur le plan international.

Thème 12. Assistance technique

Contexte

50. Contrairement à ce que l'on peut penser, la cybercriminalité n'est pas un problème qui touche essentiellement les pays développés. En 2005, le nombre d'usagers d'Internet dans les pays en développement a pour la première fois dépassé celui des pays industrialisés[58]. L'un des objectifs fondamentaux des stratégies de lutte contre la cybercriminalité étant d'empêcher que les usagers ne soient victimes de ce phénomène, l'importance de cette lutte dans les pays en développement ne devrait pas être sous-estimée. Il est également primordial de tenir compte du fait que la cybercriminalité peut avoir des incidences différentes dans les pays en développement et dans les pays développés. En 2005, l'Organisation de coopération et de développement économiques a publié un rapport sur les incidences du pourriel sur les pays en développement[59] qui montre que ces pays sont nombreux à déclarer que leurs internautes sont davantage touchés par les incidences du pourriel et de l'usage impropre d'Internet que ceux des pays développés.

Assistance technique

51. Compte tenu de la dimension internationale de la cybercriminalité, tous les pays doivent agir de manière efficace et coordonnée. La prestation d'une assistance technique est dans l'intérêt à la fois des pays développés et des pays en développement. Empêcher la création de refuges pour les cybercriminels est l'un des principaux défis de la lutte contre la cybercriminalité[60]. Renforcer les capacités

---

[58] Voir Development Gateway's Special Report, *Information Society – The Next Steps* (2005).

[59] "Spam issues in developing countries" (voir, ci-dessus, note de bas de page n° 34).

[60] Cette question a été examinée par un certain nombre d'organisations internationales. La résolution 55/63 de l'Assemblée générale pose que "les États devraient faire en sorte que leurs lois et leur pratique ne permettent pas que ceux qui exploitent les technologies de l'information à des fins criminelles puissent compter sur l'impunité". Le texte complet de la résolution est disponible à l'adresse: www.unodc.org/pdf/crime/a_res_55/res5563f.pdf. Dans les principes et le plan d'action pour la lutte contre la criminalité liée à la haute technologie adoptés par les ministres de la justice et des affaires intérieures du Groupe des Huit réunis à Washington le

des pays en développement pour leur permettre de combattre la cybercriminalité est par conséquent devenu une tâche importante de la communauté internationale.

52. L'importance de l'assistance technique est affirmée dans la Déclaration de Salvador adoptée au douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, tenu en 2010; dans ce texte, il était recommandé à l'Office des Nations Unies contre la drogue et le crime de fournir aux États qui en faisaient la demande une assistance technique pour lutter contre la cybercriminalité. Il y était également proposé d'examiner la question de l'élaboration d'un plan d'action en matière de renforcement des capacités au niveau international, avec la participation de toutes les parties prenantes. L'assistance technique devrait être actualisée en fonction de l'évolution de la situation et fournie de manière continue.

Portée de l'étude

53. Pour ce qui est de ce thème, l'étude portera sur ce qui suit:

a) Identification des éléments et principes fondamentaux de l'assistance technique à la lutte contre la cybercriminalité;

b) Inventaire des cours de formation sur la cybercriminalité existants aux niveaux national, régional et international;

c) Identification des meilleures pratiques en matière de fourniture d'une assistance technique à la lutte contre la cybercriminalité.

---

10 décembre 1997, il est précisé qu'il ne doit pas exister de refuges pour ceux qui exploitent les technologies de l'information à des fins criminelles.

Annexe II

Méthodologie de l'étude

1. Dans le cadre de son mandat, le groupe d'experts a élaboré la structure ci-après, destinée à faciliter la conduite de l'étude qui sera réalisée sous ses auspices.

2. Chaque pays aura le droit de présenter ses avis, qui devraient être pris en compte dans l'étude.

3. L'Office des Nations Unies contre la drogue et le crime (UNODC) sera chargé de réaliser l'étude, et notamment d'élaborer un questionnaire, de collecter et d'analyser des données et de rédiger un projet de texte. Pour ce faire, il s'appuiera sur les compétences et capacités internes de ses différents services (Division des traités, Service de l'analyse des politiques et de la recherche). Des ressources extrabudgétaires suffisantes devraient donc être mises à sa disposition pour lui permettre de s'acquitter efficacement de ces fonctions. Pour que les disciplines, les systèmes et les besoins technologiques les plus importants soient représentés de manière satisfaisante, chaque groupe régional communiquera au Secrétariat les noms, les coordonnées et les domaines de compétence d'experts gouvernementaux (pas plus de six) qu'il pourra consulter de manière ponctuelle, le cas échéant.

4. Le Secrétariat informera et consultera régulièrement le Bureau du groupe d'experts au sujet de ses travaux et distribuera aux États Membres les procès-verbaux de ces consultations. La liste d'experts n'est pas dressée dans le but de créer un groupe à composition limitée ni d'autres organes parallèles ou subsidiaires par rapport au groupe d'experts.

5. Pour la collecte d'informations, l'UNODC établira un questionnaire qui sera distribué auprès des États Membres, des organisations intergouvernementales et des entités du secteur privé (voir le calendrier indicatif ci-après), et qui se présentera comme un instrument d'enquête unique élaboré selon les grandes lignes du document de réflexion/de travail de la première réunion du groupe d'experts, tel que modifié, et suivant les recommandations formulées par le groupe d'experts dans le rapport de cette réunion.

6. Éventuellement, en cas de besoin, le Secrétariat pourra, considérant la nécessité d'une représentation équilibrée des différentes régions, consulter des représentants du secteur privé, notamment des représentants de fournisseurs d'accès à Internet, des usagers et d'autres acteurs pertinents; des représentants du monde universitaire issus de pays développés et en développement; et des représentants d'organisations intergouvernementales compétentes.

Calendrier indicatif

Janvier 2011: Orientations générales et directives fournies par le groupe d'experts à sa première réunion. Approbation des thèmes, de la méthodologie et du calendrier de l'étude.

Février-avril 2011: Identification des experts qui aideront l'UNODC dans la conduite de l'étude (voir ci-dessus). Présentation des noms au Bureau du groupe d'experts. Communication des noms des experts gouvernementaux par l'intermédiaire des groupes régionaux.

Avril 2011: Vingtième session de la Commission pour la prévention du crime et la justice pénale. Distribution d'un projet de questionnaire de l'UNODC en vue de la collecte des informations. Sollicitation de réactions/commentaires de la part des États Membres. Consultations en ligne pour le recueil des commentaires des membres du groupe d'experts. La Commission prend note des résultats de la première réunion du groupe d'experts et des travaux futurs proposés à cette occasion.

Mi-juin 2011: Date limite de réception des commentaires concernant le questionnaire.

Mi-juillet 2011: Finalisation du questionnaire et distribution aux États Membres. Le questionnaire sera également envoyé, sous plis séparés, à des organisations intergouvernmentales et à des représentants du secteur privé et d'établissements universitaires, qui seront invités à fournir des informations et à répondre aux questions qui les concernent. Il sera garanti, en particulier pour le secteur privé, que toutes les données recueillies resteront confidentielles et, si elles sont publiées, anonymes.

Mi-juillet-fin décembre 2011: Collecte et classement des données (cinq mois et demi, avec une lettre de rappel à mi-parcours, envoyée par le Secrétariat au début du mois d'octobre 2011).

Début décembre 2011: Deuxième réunion du groupe d'experts, en marge de la reprise de la vingtième session de la Commission. Compte rendu des progrès réalisés. Rapport provisoire d'activité qui sera communiqué pour information à la Commission à sa vingt et unième session (avril 2012).

Avril 2012: Présentation du rapport provisoire d'activité à la Commission à sa vingt et unième session.

Mi-janvier 2012-juillet 2012: Analyse des données et rédaction de l'étude. Finalisation du projet de texte.

Août 2012: Diffusion du projet de texte de l'étude aux membres du groupe d'experts pour qu'ils aient le temps de préparer leur troisième réunion.

Octobre 2012: Troisième réunion du groupe d'experts, qui examine, révise et adopte le projet de texte.

Avril 2013: Présentation de l'étude à la Commission à sa vingt-deuxième session, pour examen.