20 décembre 2010
Français
Original: anglais

Groupe d'experts sur la cybercriminalité
Vienne, 17-21 janvier 2011

Projets 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.

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

V.10-58678 (F)

privé) et l'objectif recherché (examiner les options envisageables pour renforcer les mesures prises et pour en proposer de nouvelles).

4. Afin d'élaborer un projet de structure pour cette étude, ces trois dimensions (questions de fond, perspective et objectif) ont été déclinées en 13 thèmes en adéquation avec le mandat fixé dans la Déclaration. Ces 13 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) Infractions relevant de la cybercriminalité (thème 1);

b) 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, cinq groupes spécifiques de mesures juridiques ont été identifiés:

a) Harmonisation de la législation (thème 4);

b) Droit pénal matériel (thème 5);

c) Instruments d'enquête (thème 6).

d) Coopération internationale (thème 7);

e) Preuves électroniques (thème 8);

f) Responsabilité (thème 9).

Mesures non juridiques prises pour lutter contre 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.

Mesures prises par la communauté internationale (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.

Mesures prises par le secteur privé (thème 13)

10. Comme indiqué précédemment, les États Membres recommandent également, dans la Déclaration de Salvador, que l'étude approfondie présente une analyse des mesures prises par le secteur privé.

II. Présentation détaillée des thèmes

Thème 1. Le phénomène de la cybercriminalité

Contexte

11. Les termes "criminalité informatique" et, plus précisément, "cybercriminalité" désignent une catégorie d'actes délictuels qui vont du contenu illégal à certaines formes de criminalité économique. 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

12. 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

---

[1] S'agissant des problèmes connexes, voir Slivka/Darrow, "Methods and Problems in Computer Security", *Journal of Computers and Law*, 1975, p. 217 et suiv.

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

[5] Freed, *Materials and cases on computer and law*, 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 Crimes, douzième Conférence des directeurs d'instituts de recherches criminologiques, Conseil de l'Europe, Strasbourg, 1976, p. 225 et suiv.; Staff Study of Computer Security in Federal Programs, Committee on Governmental Operations, 95e congrès, première session, Sénat des États-Unis, février 1977.

fraude informatique[8]. Dans les années 1980, les ordinateurs individuels sont devenus de plus en plus courants et de nombreuses infrastructures essentielles ont 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 de la pornographie mettant en scène des enfants, 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.

---

[8] McLaughlin, "Computer Crime: The Ribicoff Amendment to United States Code, Title 18", *Criminal Justice Journal*, 1978, vol. 2, p. 217 et suiv.; Bequai, "Computer Crime: A Growing and Serious Problem", *Police Law Quarterly*, vol. 6, 1977, p. 22.

[9] "Computer Abuse: The Emerging Crime and the Need for Legislation", *Fordham Urban Law Journal*, 1983, p. 73.

[10] BloomBecker, "The Trial of Computer Crime", *Jurimetrics Journal*, vol. 21, 1981, p. 428; Schmidt, "Legal Proprietary Interests in Computer Programs: The American Experience", *Jurimetrics Journal*, vol. 21, 1981, p. 345 et suiv. Denning, "Some Aspects of Theft of Computer Software", *Auckland University Law Review*, vol. 4, 1980, 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.; Bigelow, "The Challenge of Computer Law", *Western England Law Review*, vol. 7, 1985, p. 401; Thackeray, "Computer-Related Crimes", *Jurimetrics Journal*, 1984, 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.; "The Challenge of Computer-Crime Legislation: How Should New York Respond?", *Buffalo Law Review*, vol. 33, 1984, p. 777 et suiv.

[12] Child pornography, Congrès mondial de Yokohama contre l'exploitation sexuelle des enfants à des fins commerciales, 2001, p. 17; "Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce", Chambre des représentants des États-Unis, 109^{e} congrès, 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 "Understanding Cybercrime: A Guide for Developing Countries", Union internationale des télécommunications, 2009, chapitre 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 Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", 2007, p. 4.

[15] Simon/Slay, *Voice over IP: Forensic Computing Implications*, 2006.

[16] Velasco San Martin, *Jurisdictional Aspects of Cloud Computing*, 2009; Gercke, "Impact of Cloud Computing on Cybercrime Investigation", in Taeger/Wiebe, *Inside the Cloud*, 2009,

Portée de l'étude

13. 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 ne sont pas encore érigés en infraction;

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

d) Inventaire de cas pertinents;

e) Définition et typologie de la cybercriminalité;

f) Mécanismes de prévention de la criminalité (technique);

g) Examen de l'importance d'une définition de la cybercriminalité;

h) Réflexion sur la possibilité de recourir à la dépénalisation comme solution à certaines formes de cybercriminalité.

Thème 2. Informations statistiques

Contexte

14. Les statistiques sur la criminalité offrent une base pour la discussion et la prise de décisions par les décideurs 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

15. 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

---

p. 499 et suiv.

[17] Collier/Spaul, "Problems in Policing Computer Crime", *Policing and Soc*iety, 1992, vol. 2, p. 308, disponible à l'adresse http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[18] Concernant l'importance nouvelle des statistiques sur la criminalité, voir Osborne/Wernicke, "Introduction to Crime Analysis", 2003, p. 1 et suiv., disponible à l'adresse www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

de comptage[19]. Combiner et comparer des statistiques nationales requiert un certain 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].

16. 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

---

[19] Dans ce contexte, voir "Overcoming barriers to trust in crimes statistics", United Kingdom Statistics Authority, 2009, p. 9, disponible à l'adresse www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

[20] Alvazzi del Frate, "Crime and criminal justice statistics challenges", in Harrendorf, Heiskanen, Malby, *International Statistics on Crime and Justice*, 2010, p. 168, disponible 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, oct. 2006, p. 3.

[22] Concernant les problèmes connexes, voir Kabay, *Understanding Studies and Surveys of Computer Crime*, 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 *Heise News*, 27.10.2007, disponible à l'adresse www.heise-security.co.uk/news/80152. Voir également "Comments on Computer Crime -- Senate Bill S. 240", *Memphis State University Law Review*, 1980, p. 660.

[24] Voir Mitchison/Urry, "Crime and Abuse in e-Business", rapport de l'IPTS, disponible à l'adresse www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Collier/Spaul, "Problems in Policing Computer Crime", *Policing and Society*, 1992, vol. 2, p. 310, disponible à l'adresse http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[25] Voir Collier/Spaul, "Problems in Policing Computer Crime", *Policing and Society*, 1992, vol. 2, p. 310, disponible à l'adresse http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, p. 2, disponible à l'adresse www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

[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*, 09.10.2007, 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 d'INTERPOL, à l'adresse www.interpol.int/Public/THB/vico/Default.asp.

d'engranger d'importants profits au moyen de nombreuses attaques rapportant chacune un petit montant (cas de fraude aux avances de frais, 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

17. 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. Les défis que pose la cybercriminalité

Contexte

18. 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 recherches, et, deuxièmement, les enquêtes sur les infractions liées aux réseaux se heurtent à des difficultés bien particulières qui sont inconnues des enquêtes traditionnelles.

Les défis que pose la lutte contre la cybercriminalité

19. La liste des défis techniques et juridiques 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 techniques approfondies, tels

---

[27] Voir SOCA, "International crackdown on mass marketing fraud revealed, 2007", disponible à l'adresse www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[28] Selon le rapport du NW3C relatif à la criminalité sur Internet pour 2006, 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.

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

20. 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. Harmonisation de la législation

Contexte

21. 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

22. 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 courrier électronique non sollicité (pourriel)[33], phénomène qui pose davantage problème dans les pays en développement que dans les pays développés en raison

---

[29] "Websense Security Trends Report 2004", p. 11; "Information Security – Computer Controls over Key Treasury Internet Payment System", GAO 2003, p. 3; Sieber, rapport 2004 du Conseil de l'Europe sur la criminalité organisée, p. 143 de la version anglaise.

[30] Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", p. 9.

[31] Pour un bref historique d'Internet, y compris ses origines militaires, voir Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff, "A Brief History of the Internet", disponible à l'adresse www.isoc.org/internet/history/brief.shtml.

[32] Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

[33] Comprendre la cybercriminalité: guide pour les pays en développement, Union internationale des télécommunications, 2009, chapitre 2.6.7.

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 ailleurs qu'elle ressortit à la liberté d'expression[35, 36].

23. 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 certain degré de compréhension et d'harmonisation des législations afin qu'il ne soit pas créé de refuges[39].

Portée de l'étude

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

a) Analyse des efforts concluants et des limites rencontrées en matière d'harmonisation des législations relatives à la cybercriminalité;

b) 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;

---

[34] Voir "Spam Issue in Developing Countries", p. 4, disponible à l'adresse www.oecd.org/dataoecd/5/47/34935342.pdf.

[35] Concernant le principe de la liberté d'expression, voir Tedford, Herbeck, Haiman, *Freedom of Speech in the United States*, 2005; Barendt, *Freedom of Speech*, 2007; Baker, *Human Liberty and Freedom of Speech*; Emord, *Freedom, Technology and the First Amendment*, 1991; concernant l'importance de ce principe en matière de surveillance électronique, voir Woo, 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.; Vhesterman, *Freedom of Speech in Australian Law; A Delicate Plant*, 2000; 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; Cohen, "Freedom of Speech and Press: Exceptions to the First Amendment", CRS Report for Congress 95-815, 2007, disponible à l'adresse www.fas.org/sgp/crs/misc/95-815.pdf.

[36] Ce sont des considérations liées à la liberté d'expression qui expliquent que certains actes racistes n'aient pas été érigés en infraction par la Convention sur la cybercriminalité, mais leur incrimination a été prévue dans le premier Protocole additionnel. Voir Explanatory Report to the First Additional Protocol, n° 4.

[37] Concernant l'étendue des attaques transnationales dans les cas les plus graves d'attaques informatiques, voir Sofaer, Goodman, "Cyber Crime and Security – The Transnational Dimension", in Sofaer, Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 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 Putnam, Elliott, "International Responses to Cyber Crime", in Sofaer, Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, p. 35 et suiv., disponible à l'adresse http://media.hoover.org/documents/0817999825_35.pdf; Sofaer, Goodman, "Cyber Crime and Security – The Transnational Dimension", in Sofaer, Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, p. 1 et suiv., disponible à l'adresse http://media.hoover.org/documents/0817999825_1.pdf.

[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, p. 269, disponible en anglais à l'adresse www.uncjin.org/Documents/EighthCongress.html; Schjolberg, Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, p. 5, disponible à l'adresse www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

c) Analyse de la mesure dans laquelle les différences de normes juridiques affectent la coopération internationale;

d) Identification des techniques de rédaction législative qui offrent suffisamment de souplesse pour permettre de respecter les traditions juridiques fondamentales dans le cadre du processus d'harmonisation.

Thème 5. Incrimination des actes de cybercriminalité

Contexte

25. 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

26. 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 textes vont toutefois plus loin et incriminent des actes comme la production et la distribution d'outils (logiciels ou matériels, par exemple) pouvant être utilisés pour commettre des infractions relevant de la cybercriminalité, les actes se rapportant à la pornographie mettant en scène des enfants, 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.

Portée de l'étude

27. Pour ce qui est de ce thème, l'étude s'appuiera sur les conclusions qui auront été formulées concernant le thème 1, relatif au phénomène de la cybercriminalité, et portera sur ce qui suit:

a) Inventaire des approches adoptées aux niveaux national et régional pour incriminer les actes de cybercriminalité;

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

c) Analyse des différentes approches adoptées dans les pays de *common law* et les pays de droit romain pour incriminer les actes de cybercriminalité.

Thème 6. Procédures d'enquête

Contexte

28. 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

29. 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.

30. Certains États ont adopté des mesures qui vont au-delà de ces dispositions afin de répondre à des problèmes particuliers, tels que l'interception des communications VoIP[42]. Même si la plupart des États ont prévu des mesures d'enquête, comme les écoutes téléphoniques, qui leur permettent d'intercepter des communications passées à l'aide de téléphones portables et fixes[43], celles-ci ne leur permettent généralement pas d'intercepter les communications VoIP. Les appels téléphoniques traditionnels sont habituellement interceptés par l'intermédiaire des prestataires de

---

[40] Concernant les approches de lutte contre la cybercriminalité axées sur les utilisateurs, voir Görling, "The Myth Of User Education", 2006, à l'adresse www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. Voir également la déclaration faite par Jean-Pierre Chevènement, alors Ministre français de l'intérieur, à la Conférence du Groupe des Huit 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, Union internationale des télécommunications, 2009, chapitre 3.2.7.

[42] Le terme "voix sur IP" (VoIP) désigne la technologie de transmission de communications vocales utilisant les réseaux de communication par paquets et les protocoles connexes. Pour de plus amples informations, voir Swale, *Voice Over IP: Systems and Solutions*, 2001; Black, *Voice Over IP*, 2001.

[43] Concernant l'importance de l'interception et les solutions techniques, voir Karpagavinayagam, State, Festor, "Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection", ICIMP, 2007. Concernant les problèmes rencontrés lors de l'interception de la communication de données, voir Swale, Chochliouros, Spiliopoulou, Chochliouros, "Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response", in Janczewski, Colarik, *Cyber Warfare and Cyber Terrorism*, 2007, p. 424.

services de télécommunication[44]. De même, les services de détection et de répression collaborent généralement avec les fournisseurs d'accès à Internet et les prestataires de services VoIP pour intercepter les communications VoIP. Toutefois, si les services VoIP reposent sur le poste à poste, il est possible que ces prestataires ne puissent pas intercepter de communications[45].

Portée de l'étude

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

a) 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;

d) Analyse des différences entre les approches adoptées dans les pays de *common law* et les pays de droit romain en ce qui concerne les dispositions relatives aux enquêtes sur la cybercriminalité.

Thème 7. Coopération internationale

Contexte

32. De plus en plus souvent, la cybercriminalité revêt une dimension internationale[46], 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

---

[44] S'agissant des différences entre la communication par le réseau téléphonique public commuté (RTPC) et celle par VoIP, voir Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne, State, Niccolini, *Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks*, 2008, p. 217 et suiv.

[45] Concernant l'interception des communications VoIP par les services de détection et de répression, voir Bellovin et al., "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP"; Simon, Slay, "Voice over IP: Forensic Computing Implications", 2006; Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne, State, Niccolini, *Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks*, 2008, p. 217 et suiv.

[46] Concernant la dimension internationale de la cybercriminalité, voir Keyser, "The Council of Europe Convention on Cybercrime", *Journal of Transnational Law and Policy*, vol. 12, n° 2, p. 289, disponible à l'adresse www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. Sofaer, Goodman, "Cyber Crime and Security – The Transnational Dimension", in Sofaer, Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, p. 1 et suiv., disponible à l'adresse http://media.hoover.org/documents/0817999825_1.pdf.

coopérer à l'échelon international et à aider l'État qui s'est déclaré compétent[47]. 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 coopération internationale conclus entre États[48].

Instruments de coopération internationale

33. 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 quatre sources principales.

34. La première source est constituée des dispositions relatives à la coopération internationale qui peuvent être incluses dans des accords régionaux et internationaux visant à lutter contre une forme de criminalité internationale particulière, comme c'est le cas de la Convention des Nations Unies contre la criminalité transnationale organisée[49, 50] et de la Convention sur la cybercriminalité du Conseil de l'Europe[51]. La deuxième source est constituée des traités régionaux de coopération internationale tels que les conventions sur l'extradition ou sur l'entraide judicaire en matière pénale du Conseil de l'Europe, de l'Organisation des États américains et de la Communauté de développement de l'Afrique australe. La troisième source est constituée des accords bilatéraux d'extradition ou d'entraide judiciaire; ces accords contiennent en général des informations précises sur les types de demandes qui peuvent être formulées, ils établissent les procédures à suivre et les modalités pour entrer en contact avec un interlocuteur, et ils définissent les droits et obligations des États requis et requérants[52]. La quatrième source est la législation nationale, qui peut prévoir une coopération internationale sur la base de la réciprocité ou au cas par cas.

---

47 Voir à ce sujet les Guides législatifs pour l'application de la Convention des Nations Unies contre la criminalité transnationale organisée, 2004, p. 217, disponibles à l'adresse http://www.unodc.org/pdf/crime/legislative_guides/French%20Legislative%20guide_Full%20version.pdf.

48 Gabuardi, "Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America", *Mexican Law Review*, vol. I, n° 2, p. 156, disponible à l'adresse http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

49 Concernant la Convention, voir Smith, "An International Hit Job: Prosecuting Organized Crime Acts as Crimes Against Humanity", *Georgetown Law Journal*, 2009, vol. 97, p. 1118, disponible à l'adresse www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

50 Convention interaméricaine sur l'entraide en matière pénale, 1992, Série sur les traités, Organisation des États américains, n° 75. Le texte de la Convention est disponible à l'adresse http://www.oas.org/JURIDICO/MLA/fr/traites/fr_traites-mla-interam.html et la liste des signatures et des ratifications à l'adresse http://www.oas.org/juridico/english/sigs/a-55.html.

51 Convention sur la cybercriminalité du Conseil de l'Europe, Série des Traités européens, n° 185.

52 Voir à ce sujet le Traité type d'entraide judiciaire en matière pénale des Nations Unies, 1990, résolution 45/117 de l'Assemblée générale, et les Guides législatifs pour l'application de la Convention des Nations Unies contre la criminalité transnationale organisée, 2004, p. 217, disponibles à l'adresse http://www.unodc.org/pdf/crime/legislative_guides/French%20Legislative%20guide_Full%20version.pdf.

Portée de l'étude

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

a) Défis à relever en matière de coopération internationale dans les affaires de cybercriminalité;

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

c) Inventaire d'exemples de meilleures pratiques se fondant sur des accords bilatéraux;

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

e) Rôle des moyens informels de coopération tels que l'échange de renseignements;

f) Aperçu des besoins des autorités compétentes en matière de coopération internationale.

Thème 8. Preuves électroniques

Contexte

36. 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[53] et le faible coût[54] 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[55]. À l'heure actuelle, beaucoup de données sont stockées sous forme numérique uniquement[56]. Compte tenu de cette évolution, les documents électroniques, tels que

---

[53] Voir Abramovitch, "A brief history of hard drive control", *Control Systems Magazine*, IEEE, 2002, vol. 22, n° 3, p. 28 et suiv.; Coughlin, Waid, Porter, *The Disk Drive, 50 Years of Progress and Technology Innovation*, 2005, disponible à l'adresse: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf

[54] Giordano, "Electronic Evidence and the Law", *Information Systems Frontiers*, vol. 6, n° 2, 2006, p. 161; Willinger, Wilson, "Negotiating the Minefields of Electronic Discovery", *Richmond Journal of Law and Technology*, 2004, vol. X, n° 5.

[55] Lange, Minster, *Electronic Evidence and Discovery*, 2004, p. 6.

[56] Homer, "Proving the Integrity of Digital Evidence with Time", *International Journal of Digital Evidence*, 2002, vol. 1, n° 1, p. 1, disponible à l'adresse www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

les fichiers de texte et les vidéos et photos numériques[57], jouent un rôle dans les enquêtes sur la cybercriminalité et les procédures judiciaires connexes[58].

Règles relatives aux preuves électroniques

37. Les preuves électroniques posent un certain nombre de problèmes en ce qui concerne aussi bien leur collecte que leur recevabilité en tant que preuves[59]. 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[60].

38. La numérisation influe également sur la manière dont les services de détection et de répression et les tribunaux traitent les preuves[61]. 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, qui font que ce ne sont pas des preuves traditionnelles[62].

---

57 Concernant la recevabilité et la fiabilité des éléments de preuve sous forme d'images numériques, voir Kwiatkowski, "Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images", *Journal of Law and Policy*, p. 267 et suiv.

58 Harrington, "A Methodology for Digital Forensics", T. M. Cooley, *Journal of Practical and Clinical Law*, 2004, vol. 7, p. 71 et suiv.; Casey, *Digital Evidence and Computer Crime*, 2004, p. 14. Concernant les cadres juridiques dans les différents pays, voir Rohrmann, Neto, "Digital Evidence in Brazil", *Digital Evidence and Electronic Signature Law Review*, 2008, n° 5; Wang, "Electronic Evidence in China", *Digital Evidence and Electronic Signature Law Review*, 2008, n° 5; Bazin, "Outline of the French Law on Digital Evidence", *Digital Evidence and Electronic Signature Law Review*, 2008, n° 5; Makulilo, "Admissibility of Computer Evidence in Tanzania", *Digital Evidence and Electronic Signature Law Review*, 2008, n° 5. Winick, "Search and Seizures of Computers and Computer Data", *Harvard Journal of Law and Technology*, 1994, vol. 8, n° 1, p. 76; Insa, "Situation Report on the Admissibility of Electronic Evidence in Europe", in *Syllabus to the European Certificate on Cybercrime and E-Evidence*, 2008, p. 213.

59 Casey, *Digital Evidence and Computer Crime*, 2004, p. 9.

60 Concernant la nécessité de codifier la criminalistique informatique, voir Leigland, Krings, "A Formalization of Digital Forensics", *International Journal of Digital Evidence*, 2004, vol. 3, n° 2.

61 Concernant les difficultés rencontrées dans le traitement des preuves numériques selon les procédures et principes traditionnels, voir 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.

62 Voir Vacca, *Computer Forensics, Computer Crime Scene Investigation*, 2e édition, 2005, p. 3. Concernant les débuts du débat concernant 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.

Portée de l'étude

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

a) Inventaire des dispositions relatives au traitement et à la recevabilité des preuves électroniques;

b) Analyse des différentes approches adoptées et identification des principes communs en matière de preuves électroniques dans les pays de *common law* et les pays de droit romain.

Thème 9. Responsabilité des fournisseurs d'accès à Internet

Contexte

40. 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[63]. La situation est comparable en ce qui concerne le téléchargement de films pornographiques mettant en scène des enfants: 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.

Rôle du fournisseur d'accès à Internet

41. 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 la responsabilité des fournisseurs d'accès à Internet devrait être limitée[64]. De la réponse qui y sera apportée dépend le développement économique de l'infrastructure des technologies de l'information et de la communication.

42. 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 fournisseurs à l'égard des actes commis par leurs clients était 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.

---

[63] Concernant l'architecture du réseau et ses conséquences pour les fournisseurs de services, voir Black, *Internet Architecture: An Introduction to IP Protocols*, 2000; Zuckerman, McLaughlin, *Introduction to Internet Architecture and Institutions*, 2003, disponible à l'adresse http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[64] Pour une introduction à la discussion, voir Elkin-Koren, "Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic", *Journal of Legislation and Public Policy*, vol. 9, 2005, p. 15 et suiv., disponible à l'adresse www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

Portée de l'étude

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

a) Inventaire des approches adoptées pour réglementer la responsabilité des fournisseurs d'accès à Internet en fonction des différents types de fournisseurs;

b) Question de la limitation de la responsabilité des fournisseurs d'accès à Internet;

c) Capacité des fournisseurs d'accès à Internet d'aider les services de détection et de répression et de prévenir la cybercriminalité.

Thème 10. Mesures non juridiques contre 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.

Mesures non juridiques

45. Les mesures non juridiques prises pour lutter contre la cybercriminalité comportent notamment 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, 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 approches non juridiques adoptées pour lutter contre la cybercriminalité;

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

c) Analyse des liens entre les différentes mesures non juridiques et des possibilités de combiner ces mesures.

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[65], le Commonwealth (Loi type sur la cybercriminalité), le Conseil de l'Europe (Convention sur la

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

cybercriminalité) et l'Union européenne (Décision-cadre relative aux attaques visant les systèmes d'information).

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[66]. 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, 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;

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[67]. 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[68] 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.

---

[66] Pour des informations plus détaillées, voir Gercke, "National, Regional and International Legislative Approaches in the Fight Against Cybercrime", *Computer Law Review International*, 2008, p. 7 et suiv.

[67] Voir "Development Gateway's Special Report, Information Society – Next Steps?", 2005, disponible à l'adresse http://topics.developmentgateway.org/special/informationsociety.

[68] "Spam Issue in Developing Countries", disponible à l'adresse www.oecd.org/dataoecd/5/47/34935342.pdf.

Assistance technique

51. Compte tenu de la dimension internationale de la cybercriminalité, tous les pays doivent agir de manière coordonnée. Empêcher la création de refuges pour les cybercriminels est l'un des principaux défis de la lutte contre la cybercriminalité[69]. Renforcer les capacités des pays en développement pour leur permettre de combattre la cybercriminalité est par conséquent devenu une tâche importante de la communauté internationale. La Déclaration de Salvador adoptée au douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, tenu en 2010, en témoigne, dans laquelle 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.

Portée de l'étude

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

Thème 13. Secteur privé

Contexte

53. L'efficacité de la prévention de la cybercriminalité et des enquêtes sur les affaires qui en relèvent dépend de divers éléments. 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.

Rôle des entreprises

54. 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

---

[69] Cette question a été examinée par un certain nombre d'organisations internationales. Dans sa résolution 55/63, l'Assemblée générale a indiqué 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. Le plan d'action en 10 points adopté par le Groupe des Huit souligne qu'il ne doit pas exister de refuges pour ceux qui exploitent les technologies de l'information à des fins criminelles.

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

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

a) Inventaire des meilleures pratiques adoptées par le secteur privé pour prévenir la cybercriminalité et enquêter dans ce domaine;

b) Analyse des besoins des entreprises et des services de détection et de répression;

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