Nations Unies A/CONF.213/9

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

Salvador (Brésil), 12-19 avril 2010

Distr. générale
22 janvier 2010
Français
Original: Anglais

Point 8 de l'ordre du jour provisoire*
Tendances récentes dans l'utilisation de la science et de la technique par les délinquants et par les autorités compétentes pour lutter contre la criminalité, notamment la cybercriminalité

Tendances récentes dans l'utilisation de la science et de la technique par les délinquants et par les autorités compétentes pour lutter contre la criminalité, notamment la cybercriminalité

Document de travail établi par le Secrétariat

I. Introduction

1. Le fait que la cybercriminalité figure en bonne place dans l'ordre du jour du douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale montre bien que son importance ne diminue pas et qu'elle représente un grand défi, en dépit du fait que le sujet soit débattu depuis près d'un demi-siècle.

2. Au cours des 50 dernières années, plusieurs solutions ont été étudiées et élaborées afin de s'attaquer au problème de la cybercriminalité. S'il demeure très difficile à résoudre, c'est en partie dû au fait que la technique ne cesse d'évoluer et que les méthodes utilisées pour commettre des délits informatiques évoluent également.

3. Des années 1960 aux années 1980, les États ont été confrontés à de nouveaux actes, tels que la fraude et la falsification informatiques et l'espionnage de données, qui n'étaient bien souvent pas couverts par la législation pénale en vigueur. À l'époque, le débat se concentrait sur l'élaboration d'une réponse juridique[1].

---

* A/CONF.213/1.

[1] Voir: Susan H. Nycum, *The Criminal Law Aspects of Computer Abuse: Applicability of the State Penal Laws to Computer Abuse* (Menlo Park, Californie, Stanford Research Institute, 1976) et Ulrich Sieber, *Computerkriminalität und Strafrecht* (Cologne, Karl Heymanns Verlag, 1977).

V.10-50383 (F) 170310 180310

4. L'introduction d'une interface graphique dans les années 1990, suivie d'une augmentation rapide du nombre d'utilisateurs de l'Internet, ont fait apparaître de nouveaux défis. Des informations diffusées légalement dans un pays devenaient disponibles à l'échelle de la planète, y compris dans des pays où la publication de telles informations n'était pas légale. Un autre motif de préoccupation lié aux services en ligne était la rapidité de l'échange des données, qui s'est révélée être un problème majeur pour les enquêtes sur des infractions revêtant une dimension internationale[2].

5. La première décennie du XXI[e] siècle est dominée par l'adoption de nouvelles méthodes très élaborées pour commettre des infractions (telles que le "phishing"[3] et les "attaques par des réseaux de robots"[4]) et par l'utilisation de technologies auxquelles les agents des services de détection et de répression ont encore plus de mal à faire face dans les enquêtes (telles que la communication par protocole voix sur IP et le "cloud computing" ou "informatique dans les nuages").

II. Les défis que pose la cybercriminalité

A. Incertitudes quant à l'étendue du problème

6. En dépit d'améliorations technologiques et d'enquêtes approfondies, le degré d'utilisation de la technologie de l'information à des fins illégales reste stable ou pourrait même être en hausse. Selon certains fournisseurs de services de messagerie électronique, sur l'ensemble des courriels envoyés, pas moins de 75 à 90 % sont des spam[5]. Des chiffres similaires, constants ou en hausse, sont également publiés pour d'autres comportements criminels plus répandus. Par exemple, dans son rapport annuel de 2008, la Internet Watch Foundation fait état d'un nombre relativement stable, entre 2006 et 2008, de sites Web commerciaux confirmés de pédopornographie.

7. Si les informations statistiques sont utiles pour appeler l'attention sur l'importance actuelle ou croissante de ce problème, l'un des principaux défis liés à

---

[2] En ce qui concerne les répercussions de la plus grande rapidité des échanges de données sur les enquêtes relatives à des affaires de cybercriminalité, voir Union internationale des télécommunications, *Comprendre la cybercriminalité: Guide pour les pays en développement* (Genève, 2009). Disponible à l'adresse: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

[3] Comme l'a décrit l'Union internationale des télécommunications dans *Comprendre la cybercriminalité: Guide* (voir note de bas de page n° 2), le "phishing" est un acte visant à contraindre la victime à révéler des informations personnelles ou confidentielles. Le terme "phishing" décrivait à l'origine l'utilisation de courriers électroniques pour hameçonner (to phish) des mots de passe et des données financières dans une mer d'internautes. L'emploi du "ph" est liée à des conventions langagières prisées des pirates.

[4] Un "botnet" ou réseau de robots est un groupe d'ordinateurs piratés exécutant un logiciel placé sous contrôle externe. Voir Clay Wilson, "Botnets, cybercrime and cyberterrorism: vulnerabilities and policy issues for Congress", Congressional Research Service Report RL32114, mis à jour le 29 janvier 2008, disponible à l'adresse: www.fas.org/sgp/crs/terror/RL32114.pdf.

[5] Selon le Groupe de travail contre l'utilisation abusive des messageries, entre 85 et 90 % de l'ensemble des courriels étaient des spam. (http://www.maawg.org/sites/maawg/files/news/2009_MAAWG-Consumer_Survey-Part1.pdf).

la cybercriminalité est l'absence d'informations fiables sur l'étendue du phénomène ainsi que sur le nombre d'arrestations, de poursuites en justice et de condamnations. Les infractions ne font pas l'objet d'une catégorie distincte dans les statistiques sur la criminalité et les rares statistiques qui existent sur les effets de la cybercriminalité sont, en règle générale, insuffisamment détaillées pour fournir aux responsables politiques des informations fiables sur l'ampleur ou l'étendue des infractions[6]. En l'absence de ces données, il est difficile de quantifier les répercussions de la cybercriminalité sur la société et d'élaborer des stratégies pour s'attaquer au problème[7].

8. L'une des raisons pour lesquelles il n'existe pas suffisamment de données statistiques tient au fait qu'il est difficile d'estimer l'ampleur des pertes financières et le nombre d'infractions commises par les cyberdélinquants. Selon certaines sources, les pertes causées aux entreprises et aux institutions aux États-Unis[8] en raison de la cybercriminalité s'élèveraient à pas moins de 67 milliards de dollars des États-Unis par an; il n'est cependant pas certain que cette extrapolation fondée sur les résultats d'une enquête par sondage soit justifiable[9]. Cette critique de la méthodologie s'applique non seulement aux pertes, mais aussi au nombre d'infractions reconnues[10]. De même, on ne sait pas vraiment dans quelle mesure les victimes signalent la cybercriminalité. Bien que les autorités responsables de la lutte contre la cybercriminalité les encouragent à signaler les infractions, il est à craindre que, en particulier dans le secteur financier (par exemple les banques), elles ne le fassent pas toujours, de crainte que cette publicité négative ne porte atteinte à leur réputation[11]. Si une entreprise fait savoir que des pirates ont eu accès à son serveur, cela peut entraîner une perte de confiance des clients et l'ensemble des coûts et des conséquences risque même de dépasser le montant des pertes occasionnées par l'attaque lancée par les pirates. En outre, les entreprises ciblées peuvent penser que les services de détection et de répression ne parviendront pas à identifier les délinquants. Or, si ces derniers ne sont pas signalés et poursuivis, ils risquent de continuer à commettre des infractions.

9. Une autre difficulté liée aux données statistiques est le fait que, très souvent, des données non fiables ou non vérifiables sont citées à de multiples reprises. Prenons, à titre d'exemple, les statistiques relatives aux aspects commerciaux de la pédopornographie sur Internet. Dans plusieurs analyses, il a été indiqué que, selon une source citée, la pédopornographie sur Internet génère 2,5 milliards de dollars

---

[6] États-Unis d'Amérique, Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, rapport GAO GAO-07-705 (Washington, D.C., juin 2007), p. 22; et Ian Walden, *Computer Crimes and Digital Investigations* (Oxford, Oxford University Press, 2007).

[7] Walden, *Computer Crimes and Digital Investigations*.

[8] États-Unis, Federal Bureau of Investigation, *2005 FBI Computer Crime Survey*, p. 10.

[9] *Comprendre la cybercriminalité: Guide* (voir note de bas de page 2).

[10] Ibid.

[11] Neil Mitchison et Robin Urry, "Crime and abuse in e-business", *IPTS Report*, vol. 57, septembre 2001.

par an dans le monde[12]. Or, la source de ce chiffre (www.toptenreviews.com) ne précise pas comment cette étude a été réalisée. Compte tenu du fait qu'elle indique, sur son site Web, ce qui suit: "toptenreviews vous fournit les informations dont vous avez besoin pour faire un achat malin. Nous vous recommandons le meilleur produit dans chaque catégorie. À l'aide de nos tableaux comparateurs de produits, de nos lettres d'information, de nos articles et de nos vidéos, nous simplifions le processus d'achat pour nos clients", on peut se poser de réelles questions quant à la fiabilité des données. Dans un autre exemple, en 2006, un journaliste du *Wall Street Journal*[13] qui enquêtait sur l'assertion selon laquelle la pédopornographie est une activité générant un chiffre d'affaires de 20 milliards de dollars par an, a découvert que les deux principaux documents contenant des informations sur des recettes allant de 3 à 20 milliards de dollars (publications du National Center for Missing and Exploited Children, aux États-Unis, et du Conseil de l'Europe) se référaient à des institutions n'ayant pas confirmé ces chiffres.

B. Une dimension transnationale

10. La cybercriminalité est dans une large mesure de nature transnationale. L'Internet avait été conçu à l'origine comme un réseau militaire reposant sur une architecture de réseau décentralisée. Du fait de cette architecture sous-jacente et de la disponibilité mondiale des services, la cybercriminalité revêt souvent une dimension internationale. Il est facile d'envoyer des courriers électroniques comportant des contenus illicites à des destinataires situés dans plusieurs pays, y compris lorsque le premier expéditeur et le destinataire final sont situés dans le même pays ou lorsque l'expéditeur ou le destinataire utilise un service de messagerie électronique géré par un fournisseur situé en dehors du pays. Certains fournisseurs de services de messagerie électronique gratuits parmi les plus connus comptent des milliers d'utilisateurs de par le monde, ce qui fait davantage ressortir la dimension transnationale de la cybercriminalité.

11. Les défis que représente cet élément transnational pour les enquêtes sur les infractions ayant pour cadre le cyberespace sont similaires à ceux rencontrés dans les enquêtes portant sur d'autres formes d'infractions transnationales. Du fait du principe fondamental de la souveraineté nationale, en vertu duquel les enquêtes en territoires étrangers ne peuvent être menées sans l'autorisation des autorités locales, une coopération étroite entre les États concernés est indispensable pour les enquêtes sur la cybercriminalité. Un autre défi majeur est celui de la rapidité avec laquelle doivent être menées ces enquêtes. Contrairement aux drogues illicites qui, selon les moyens de transport utilisés, peuvent avoir besoin de plusieurs semaines pour atteindre leur destination, les courriers électroniques peuvent être acheminés en quelques secondes et, pour ceux qui disposent d'un accès avec une largeur de bande suffisante, des dossiers volumineux peuvent être téléchargés en quelques minutes.

---

[12] Kim-Kwang Choo, Russel G. Smith et Rob McCusker, "Future directions in technology-enabled crime: 2007-09", Research and Public Policy Series, No. 78 (Canberra, Institut australien de criminologie, 2007), p. 62; ECPAT International, *La violence contre les enfants dans le cyberespace* (Bangkok, 2005), p. 54; Conseil de l'Europe, *Rapport de situation 2005 sur la criminalité organisée. La menace de la criminalité économique* (Strasbourg, décembre 2005), p. 41.

[13] Carl Bialik, "Measuring the child-porn trade", *Wall Street Journal*, 18 avril 2006.

12. Une coopération efficace et en temps utile entre les autorités de différents pays est également indispensable car, dans le cas de la cybercriminalité, les éléments de preuve sont souvent supprimés automatiquement et dans des délais très courts. Des procédures formelles très longues peuvent donc entraver sérieusement les enquêtes.

13. Nombre des accords d'entraide judiciaire existants reposent encore sur des procédures formelles, complexes et qui prennent souvent un temps considérable. Il est par conséquent essentiel de mettre en place des procédures permettant de réagir rapidement aux incidents et aux demandes de coopération internationale.

14. Le chapitre III de la Convention sur la cybercriminalité du Conseil de l'Europe[14] contient un ensemble de principes pour élaborer un cadre juridique pour la coopération internationale en matière d'enquêtes sur la cybercriminalité. Ce chapitre traite de l'importance croissante de la coopération internationale (articles 23 à 35) et encourage l'utilisation de moyens rapides de communication, notamment la télécopie et le courrier électronique (art. 25, para. 3). En outre, les parties à la Convention sont invitées à désigner un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, pour répondre aux demandes d'assistance formulées par les États (art. 35). On peut trouver d'autres approches dans le projet de convention internationale pour renforcer la protection contre la cybercriminalité et le terrorisme et dans le projet de boîte d'outils de l'Union internationale des télécommunications (UIT) pour une législation en matière de cybercriminalité.

C. Des différences entre les approches juridiques nationales

15. Une conséquence pratique de l'architecture en réseau de l'Internet est que les cyberdélinquants n'ont pas besoin d'être présents sur la scène du crime. Par conséquent, les empêcher de trouver des refuges est devenu un aspect-clef de la prévention de la cybercriminalité[15]. Les délinquants utiliseront en effet des refuges pour gêner les enquêtes. Un exemple bien connu est le ver informatique "I love you" qui a été créé aux Philippines en 2000[16] et aurait infecté des millions d'ordinateurs dans le monde[17]. Les enquêtes locales ont été gênées par le fait que le développement et la diffusion malveillants du logiciel à l'origine des dommages n'étaient pas, à l'époque, incriminés de façon adéquate aux Philippines.

---

[14] Conseil de l'Europe, *Série des Traités européens*, n° 185. Voir également le "rapport explicatif" à la Convention.

[15] Aussi bien l'Assemblée générale, dans sa résolution 55/63, que le Groupe des Huit, dans les principes et le plan d'action pour combattre le crime de haute technologie dont sont convenus les ministres de la justice et de l'intérieur du Groupe des Huit lors de la réunion tenue à Washington, D.C., le 10 décembre 1997 (disponible à l'adresse: www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf), ont souligné la nécessité d'éliminer les refuges pour ceux qui exploitent les technologies de l'information à des fins criminelles.

[16] États-Unis, General Accountability Office, *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*, audition devant la sous-commission des institutions financières de la Commission des affaires bancaires, du logement et des affaires urbaines, Sénat des États-Unis, rapport GAO GAO/T-AIMD-00-181 (Washington, D.C., mai 2000).

[17] "Police close in on Love Bug culprit" *BBC News*, 6 mai 2000. Disponible à l'adresse: http://news.bbc.co.uk/2/hi/science/nature/738537.stm.

16. La question de la convergence des législations est extrêmement importante, étant donné qu'un grand nombre de pays font reposer leur régime d'entraide judiciaire sur le principe de la double incrimination, selon lequel l'acte incriminé doit être considérée comme une infraction à la fois dans l'État requérant une assistance et dans l'État requis[18]. Les enquêtes menées sur le plan mondial sont généralement limitées aux actes incriminés dans tous les pays concernés. Bien qu'un certain nombre d'infractions puissent faire l'objet de poursuites partout dans le monde, les différences régionales jouent un rôle important. Par exemple, différents types de contenus sont incriminés selon les pays[19], ce qui signifie qu'un matériel pouvant être diffusé légalement sur un serveur dans un pays donné peut être considéré comme illicite dans un autre[20].

17. La technologie informatique et des réseaux actuellement utilisée est pratiquement la même partout dans le monde. Mis à part les questions de langue et les adaptateurs électriques, il y a très peu de différences entre les systèmes informatiques et les téléphones portables vendus en Asie et ceux vendus en Europe. Il en va à peu près de même pour l'Internet. Du fait de la standardisation, les protocoles utilisés dans des pays d'Afrique sont les mêmes que ceux utilisés aux États-Unis. La standardisation permet à des utilisateurs du monde entier d'accéder aux mêmes services par le biais d'Internet[21].

18. Deux approches différentes pour faire face à la dimension transnationale de la cybercriminalité et à la différence entre les normes juridiques sont examinées dans les paragraphes ci-après.

1. Compatibilité des législations

19. Une approche pour s'attaquer à la dimension transnationale de la cybercriminalité et resserrer la coopération internationale consiste à développer et harmoniser les législations pertinentes. Plusieurs approches régionales ont été suivies ces dernières années.

20. En 2002, le Commonwealth a élaboré une loi type sur la criminalité informatique et liée à l'informatique dans le but d'améliorer la législation contre la cybercriminalité dans ses États membres et de resserrer la coopération

---

[18] En ce qui concerne le principe de la double incrimination dans les enquêtes relatives à des affaires de cybercriminalité, voir le Manuel de l'Organisation des Nations Unies sur la prévention et la répression de la criminalité liée à l'informatique (*Revue internationale de politique criminelle*, n° 43 et 44: Publication des Nations Unies, numéro de vente E.94.IV.5), p. 269, et le document de travail de Stein Schjølberg et Amanda Hubbard intitulé "Harmonizing national legal approaches on cybercrime", p. 5, qui a été présenté à la réunion thématique de l'UIT sur la cybersécurité, tenue à Genève du 28 juin au 1er juillet 2005.

[19] Les différentes approches juridiques en ce qui concerne la réglementation des contenus est l'une des raisons pour lesquelles certains aspects des contenus illicites ne sont pas inclus dans la Convention sur la cybercriminalité, mais traités dans un protocole additionnel. Voir également *Comprendre la cybercriminalité: Guide*, chap. 2.5 (voir note de bas de page 2).

[20] En ce qui concerne les différentes approches relatives à l'incrimination de la pédopornographie, voir, par exemple, Ulrich Sieber, *Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet: eine strafrechtsvergleichende Untersuchung* (Bonn, Forum Verlag Godesberg, 1999).

[21] En ce qui concerne l'importance d'adopter des normes techniques uniques ou des normes juridiques uniques, voir Marco Gercke, "National, regional and international approaches in the fight against cybercrime", *Computer Law Review International*, 2008, p. 7.

internationale. Sans de telles améliorations, il ne faudrait pas moins de 1 272 traités bilatéraux entre les États du Commonwealth pour régir la coopération internationale sur la question[22]. La loi type contient des dispositions en matière de droit pénal matériel, de droit procédural et de coopération internationale. Comme elle est de portée régionale, ses effets sur l'harmonisation sont limités aux États membres du Commonwealth.

21. L'Union européenne a également fait des efforts pour harmoniser les législations sur la cybercriminalité au sein de ses 27 États membres, par exemple par la directive 2000/31/CE du Parlement européen et du Conseil de l'Union européenne relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur; la décision-cadre du Conseil de l'Union européenne 2000/413/JAI concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces; la décision-cadre du Conseil de l'Union européenne 2004/68/JAI relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie; la décision-cadre du Conseil de l'Union européenne 2005/222/JAI sur les attaques dirigées contre les systèmes d'information[23]; la directive 2006/24/CE du Parlement européen et du Conseil de l'Union européenne relative à la conservation des données générées ou traitées dans le contexte de la prestation de services de communications électroniques d'accès public ou de réseaux publics de communication et portant modification de la directive 2002/58/CE et la décision-cadre du Conseil de l'Union européenne 2008/919/JAI modifiant la décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme. Contrairement à ce qui se passe dans la plupart des autres approches régionales, la mise en œuvre des instruments adoptés par l'Union européenne est contraignante pour tous les États. Ces instruments sont certes efficaces, mais le principal obstacle à une harmonisation au sein de l'Union européenne était, tout au moins jusqu'au début de 2010, les pouvoirs législatifs limités dans le domaine du droit pénal[24]. La diversité des approches vient du fait que la capacité de l'Union européenne à harmoniser les systèmes internes de droit pénal était limitée à des domaines particuliers[25]. Le Traité de Lisbonne modifiant le Traité sur l'Union européenne et le Traité instituant la Communauté européenne a changé les choses et donne désormais à l'Union européenne davantage d'attributions pour harmoniser à l'avenir les législations sur la criminalité liée à l'informatique – mais cela reste limité aux 27 États membres.

---

[22] Richard Bourne, "2002 Commonwealth Law Ministers' Meeting: policy brief", préparé pour la Réunion des ministres de la justice du Commonwealth, tenue à Kingstown, Saint-Vincent-et-les-Grenadines, du 18 au 21 novembre 2002 (Londres, Institute of Commonwealth Studies, 2002), p. 9.

[23] Pour plus d'informations, voir Marco Gercke, "The EU framework decision on attacks against information systems", *Computer und Recht*, 2005, p. 468 et suivantes; et *Comprendre la cybercriminalité: Guide* (voir note de bas de page 2), p. 99.

[24] Helmut Satzger, *Internationales und Europäisches Strafrecht* (Baden-Baden, Nomos, 2005), p. 84; et P.J.G. Kapteyn et Pieter Verloren van Themaat, *Introduction to the Law of the European Communities: After the Coming into Force of the Single European Act* (Boston, Kluwer Law International, 1989).

[25] En ce qui concerne la législation sur la cybercriminalité dans les pays de l'Union européenne: Lorenzo Valeri et autres, *Handbook of Legal Procedures of Computer Network Misuse in EU Countries* (Santa Monica, Californie, Rand Corporation, 2006).

22. Le Conseil de l'Europe a élaboré trois instruments majeurs afin d'harmoniser les législations sur la cybercriminalité. Le plus connu est la Convention sur la cybercriminalité, qui a été élaborée entre 1997 et 2001. Cette Convention contient des dispositions sur le droit pénal matériel, les règles de procédure et la coopération internationale. En décembre 2009, elle avait été signée par 46 États et ratifiée par 26. Dans la mesure où, pendant la négociation, aucun accord sur l'incrimination du racisme et de la diffusion de matériel xénophobe n'avait pu être trouvé, un protocole additionnel à la Convention, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, a été introduit en 2003[26]. En décembre 2009, 34 États[27] avaient signé le Protocole additionnel et 15 d'entre eux[28] l'avaient ratifié. En 2007, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels[29] a été ouverte à la signature. Elle contient des dispositions spécifiques érigeant en infraction pénale l'échange de pornographie enfantine, ainsi que le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie enfantine (art. 20, par. 1 f)). En décembre 2009, elle avait été signée par 38 États[30], parmi lesquels trois[31] l'avaient ratifiée.

23. On notera également le projet de convention internationale visant à renforcer la protection contre la cybercriminalité et le terrorisme, qui a été élaboré à titre de suivi d'une conférence accueillie par l'université de Stanford, États-Unis, en 1999 et le projet de boîte d'outils de l'UIT pour une législation en matière de cybercriminalité, qui a été élaboré par des représentants de l'American Bar Association et d'autres experts.

2. Territorialisation

24. Théoriquement, les développements découlant de la standardisation technique vont bien au-delà de la mondialisation de la technologie et des services et pourraient conduire à l'harmonisation des législations nationales. Cependant, comme le montrent l'état des ratifications de la Convention sur la cybercriminalité et la négociation du Protocole additionnel, les principes du droit interne évoluent beaucoup plus lentement que la technologie. Cela conduit à un second développement, à savoir des approches pour territorialiser l'Internet.

---

[26] Conseil de l'Europe, *Série des Traités européens*, n° 189. Voir également le "rapport explicatif" au Protocole additionnel.

[27] Afrique du Sud, Albanie, Allemagne, Arménie, Autriche, Belgique, Bosnie-Herzégovine, Canada, Chypre, Croatie, Danemark, Estonie, ex-République yougoslave de Macédoine, Finlande, France, Grèce, Islande, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, République de Moldova, Roumanie, Serbie, Slovénie, Suède, Suisse et Ukraine.

[28] Albanie, Arménie, Bosnie-Herzégovine, Croatie, Chypre, Danemark, ex-République yougoslave de Macédoine, France, Lettonie, Lituanie, Norvège, Roumanie, Serbie, Slovénie et Ukraine.

[29] Conseil de l'Europe, *Série des Traités*, n° 201.

[30] Albanie, Allemagne, Autriche, Azerbaïdjan, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, ex-République yougoslave de Macédoine, Finlande, France, Géorgie, Grèce, Irlande, Islande, Italie, Liechtenstein, Lituanie, Luxembourg, Monaco, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, République de Moldova, Roumanie, Royaume-Uni, Saint-Marin, Serbie, Slovaquie, Slovénie, Suède, Turquie et Ukraine.

[31] Albanie, Danemark et Grèce.

25. Bien que l'Internet puisse faire abstraction des contrôles aux frontières, il existe des moyens de restreindre l'accès à certaines informations[32]. Partant, la possibilité d'obliger les fournisseurs de services Internet à bloquer l'accès aux sites Web contenant de la pornographie enfantine est parvenue à l'attention des gouvernements nationaux et des organisations internationales[33]. D'un point de vue technique, les fournisseurs d'accès sont en règle générale capables de vérifier si le site Web auquel l'utilisateur veut accéder est inscrit sur une liste noire et d'en bloquer l'accès. Les solutions techniques vont d'une manipulation du système de noms de domaine et de l'utilisation de serveurs proxy à des solutions hybrides associant plusieurs approches[34]. Selon l'OpenNet Initiative, ce type de contrôle des contenus est pratiqué par deux douzaines de pays[35]. Plusieurs pays européens, notamment l'Italie, la Norvège, la Suède, la Suisse et le Royaume-Uni ainsi que des pays comme la Chine, l'Iran (République islamique d') et la Thaïlande ont adopté une telle approche. L'Union européenne étudie également l'imposition de telles obligations[36]. Les principaux motifs de préoccupation à ce sujet sont que toutes les solutions techniques disponibles à l'heure actuelle peuvent être mises en échec et que l'accès aux informations sur l'Internet[37] pourrait se trouver bloqué par des excès de zèle. Le Conseil de l'Europe, dans la recommandation de son Comité des Ministres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet, a souligné qu'il était important de protéger les droits fondamentaux.

---

[32] Jonathan Zittrain, "A history of online gatekeeping", *Harvard Journal of Law and Technology*, vol. 19, n° 2 (2006), p. 253.

[33] En ce qui concerne les obligations et les approches en matière de filtres, voir: Ilaria Lonardo, "Italy: Service Provider's Duty to Block Content", *Computer Law Review International*, 2007, p. 89 et suiv.; Ulrich Sieber et Malaika Nolde, *Sperrverfügungen im Internet: Nationale Rechtdurchsetzung im globalen Cyberspace?* (Berlin, Duncker and Humblot, 2008); W. Ph. Stol et autres, *Filteren van kinderporno op internet: Een verkenning van technieken en reguleringen in binnen- en buitenland* (La Haye, Boom Juridische Uitgevers, WODC, 2008); Tom Edwards et Gareth Griffith, "Internet censorship and mandatory filtering", *NSW Parliamentary Library Research Service*, E-Brief 5/08, novembre 2008; Jonathan Zittrain et Benjamin Edelman, "Documentation of Internet filtering worldwide", octobre 2003, projet disponible à l'adresse: http://cyber.law.harvard.edu/filtering.

[34] Pour une vue d'ensemble des aspects techniques, voir: Sieber et Nolde, *Sperrverfügungen im Internet*, p. 50 et suiv.; Stol et autres, *Filteren van kinderporno op internet*, pp. 10 et suivantes; Andreas Pfitzmann, Stefan Köpsell et Thomas Kriegelstein, *Sperrverfügungen gegen Access-Provider: Technisches Gutachten*, Université technique de Dresde, disponible à l'adresse: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; Richard Clayton, Steven J. Murdoch et Robert N. M. Watson, "Ignoring the Great Firewall of China", document présenté lors du 6e Atelier sur les technologies de protection de la vie privée, Cambridge, juin 2006; Lori Brown Ayre, *Internet Filtering Options Analysis: An Interim Report*, préparé pour le InfoPeople Project, mai 2001.

[35] Miklós Haraszti, "Preface", in Governing the Internet: Freedom *and Regulation in the OSCE Region*, C. Möller et A. Amouroux, sous la direction de (Vienne, Organisation pour la Sécurité et la Coopération en Europe, 2007), pp. 5 et 6.

[36] Commission des Communautés européennes, "Proposition de décision-cadre du Conseil relative à l'exploitation et aux abus sexuels concernant les enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI", document COM(2009) 135, Bruxelles, 25 mars 2009.

[37] Pour plus de détails sur le blocage d'Internet et la protection des libertés fondamentales, voir Cormac Callanan et autres, *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Dublin, Aconite Internet Solutions, octobre 2009), chapitres 6 et 7.

D. La criminalité organisée

26. Si les infractions liées à l'informatique sont en général commises par des personnes, des groupes criminels organisés sont aussi actifs dans ce domaine. Ce fait nouveau est particulièrement important dans la mesure où il crée la possibilité d'appliquer des instruments conçus pour lutter contre la criminalité organisée, tels que la Convention des Nations Unies contre la criminalité transnationale organisée[38].

27. Pour débattre de la cybercriminalité et de la criminalité organisée, il est nécessaire d'établir une distinction entre deux grandes formes d'implication des groupes criminels organisés: le recours aux technologies de l'information par des groupes criminels organisés traditionnels, et les groupes criminels organisés qui se consacrent essentiellement à la cybercriminalité[39].

28. Les groupes criminels organisés traditionnels qui ne se sont pas spécialisés dans des activités criminelles liées à Internet utilisent les technologies de l'information pour coordonner leurs activités et faciliter la commission d'infractions[40]. Dans pareils cas, les technologies de l'information servent à améliorer l'efficacité du groupe dans son domaine d'activité traditionnel. Les groupes criminels organisés vont notamment passer aux communications électroniques, ce qui leur permet par exemple de recourir au cryptage et de communiquer de façon anonyme. En outre, Internet peut être utilisé pour ouvrir de nouveaux marchés étant donné que, comme l'a constaté le groupe de lutte contre le crime organisé (Organised Crime Task Force) du Royaume-Uni, Internet offre un débouché nouveau et beaucoup plus important que le marché classique à ceux qui s'adonnent à la vente de biens contrefaits et piratés[41].

29. Les rapports font état d'une tendance selon laquelle des groupes criminels organisés traditionnels se livrent à de nouvelles formes d'activités criminelles commises à l'aide de technologies de pointe[42]. Il s'agit notamment du piratage de logiciels et d'autres formes d'atteintes à la propriété intellectuelle[43], mais d'autres domaines de la cybercriminalité, tels que la pédopornographie[44] et la criminalité

---

[38] Nations Unies, *Recueil des Traités*, vol. 2225, n° 39574.

[39] Kim-Kwang Raymond Choo, "Organised crime groups in cyberspace: a typology", *Trends in Organized Crime*, vol. 11, n° 3 (septembre 2008), p. 270 à 295. Dans cet article, Choo avance qu'il existe trois catégories de groupes criminels organisés qui exploitent les technologies de l'information à des fins délictueuses.

[40] Ibid., p. 273; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 2e éd. (Londres, Academic Press, 2004), p. 9.

[41] Royaume-Uni, Organised Crime Task Force, *Annual Report and Threat Assessment 2007: Organised Crime in Northern Ireland* (2007), p. 34. Disponible à: www.octf.gov.uk.

[42] Royaume-Uni, Serious Organised Crime Agency, *The United Kingdom Threat Assessment of Organised Crime: 2009/10*, p. 10. Disponible à l'adresse: www.soca.gov.uk.

[43] Canada, Service canadien du renseignement de sécurité "La criminalité transnationale: contexte mondial", *Perspectives*, 17 août 2000, disponible à l'adresse: www.csis-scrs.gc.ca/pblctns/prspctvs/200007-fra.asp; Choo, "Organised crime groups", p. 273 (voir note de bas de page 40).

[44] Choo, "Organised crime groups", p. 281; Office européen de police (Europol), "Child abuse in relation to trafficking in human beings", Serious Crime Overview, janvier 2008, p. 2; *Rapport de situation 2005 sur la criminalité organisée*, p. 8; John Carr, *Child Abuse, Child Pornography and the Internet* (Londres, NCH, The Children's Charity, 2004), p. 17; Canada, Service canadien

liée à l'identité, sont eux aussi souvent investis par la criminalité organisée. En ce qui concerne l'application de la Convention contre la criminalité organisée, il convient de prendre en considération les caractéristiques et les groupes cybercriminels organisés ci-dessous:

a) Les groupes cybercriminels tendent à avoir une structure plus lâche et plus souple, qui permet d'intégrer des membres pour une période limitée[45];

b) Les groupes cybercriminels sont souvent beaucoup plus petits que les groupes criminels organisés traditionnels[46];

c) Il est fréquent que les membres des groupes communiquent exclusivement sous forme électronique, sans jamais se rencontrer en personne.

III. Réponses à la cybercriminalité

30. Les organisations internationales et régionales, les administrations centrales, les services de détection et de répression et les organisations non gouvernementales luttent contre la cybercriminalité de différentes manières, notamment par des moyens législatifs et répressifs et par le renforcement des capacités.

A. Législation

31. À l'heure actuelle, la législation relative à la cybercriminalité est principalement élaborée aux échelons national et régional. Alors que les normes techniques utilisées pour les transferts de données sont les mêmes partout dans le monde, aucun effort n'a été fait à ce jour au niveau mondial pour harmoniser les législations relatives à la cybercriminalité.

1. Portée limitée des instruments existants

32. Les effets à l'échelle mondiale des approches régionales qui ont été suivies par le Commonwealth, la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), l'Union européenne et le Conseil de l'Europe sont limités étant donné que ces approches ne s'appliquent qu'aux États membres desdites organisations. Actuellement, l'instrument ayant la plus large portée est la Convention sur la cybercriminalité, reconnue comme importante dans la lutte contre la cybercriminalité et soutenue par différentes organisations internationales. En outre, en vertu de son article 37, tout État non membre du Conseil peut adhérer à la Convention. Quatre États non membres (Afrique du Sud, Canada, États-Unis et Japon) ont pris part à l'élaboration de la Convention; trois d'entre eux (Canada, États-Unis et Japon) sont étroitement liés au Conseil de par leur statut

---

du renseignement de sécurité, *Rapport annuel sur le crime organisé au Canada 2007* (Ottawa, 2007), p. 4; "Annual report on organized crime in Greece for the year 2004", *Trends in Organized Crime*, vol. 9, n° 2 (2005), p. 5; Nations Unies, Commission des droits de l'homme, rapport du Rapporteur spécial sur la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants (E/CN.4/2005/78), p. 8.

[45] Choo, "Organised crime groups", p. 273 (voir note de bas de page 40).

[46] Susan W. Brenner, "Organized cybercrime? How cybercrime may affect the structure of criminal relationships", North Carolina Journal of Law and Technology, n° 4 (2002), p. 27.

d'observateur. En décembre 2009, 46 États[47] (parmi lesquels les quatre États non membres ayant pris part à la négociation) avaient signé la Convention; 26 États et 1 État non membre du Conseil l'avaient ratifiée[48].

33. On ne saurait mesurer l'impact de la Convention sur la cybercriminalité uniquement au nombre d'États l'ayant signée ou ratifiée. L'Argentine, le Botswana, l'Égypte, le Nigéria, le Pakistan et les Philippines, par exemple, se sont inspirés de la Convention, sans y adhérer officiellement, pour élaborer certaines parties de leur législation. Reste que, rapportés aux normes mondiales, le nombre et le rythme de signatures et de ratifications de la Convention continue de poser problème. En neuf ans, depuis que les 30 premiers États ont signé la Convention le 23 novembre 2001, seuls 16 nouveaux États sont devenus signataires. Depuis 2001, aucun État non membre du Conseil de l'Europe n'a adhéré à la Convention, bien que cinq États (Chili, Costa Rica, Mexique, Philippines et République dominicaine) aient été invités à le faire. Le rythme des ratifications est tout aussi lent, deux États (Albanie et Croatie) ayant ratifié la Convention en 2002, deux (Estonie et Hongrie) en 2003, quatre (ex-République yougoslave de Macédoine, Lituanie, Roumanie et Slovénie) en 2004, trois (Bulgarie, Chypre et Danemark) en 2005, sept (Arménie, Bosnie-Herzégovine, États-Unis, France, Norvège, Pays-Bas et Ukraine) en 2006, trois (Finlande, Islande et Lettonie) en 2007, deux (Italie et Slovaquie) en 2008 et trois (Allemagne, République de Moldova et Serbie) en 2009. Sachant qu'en plus de devoir être ratifiée, la Convention doit généralement être mise en œuvre, elle n'aura d'effets que si les États l'ayant ratifiée adaptent pleinement leur droit interne en conséquence. En outre, les États doivent apporter la preuve qu'ils ont pleinement adapté leur législation.

2. Débat mondial

34. Un autre aspect du rôle des cadres régionaux en tant qu'instruments d'harmonisation à l'échelon mondial est la possibilité pour les États non membres d'y participer. En dépit de sa dimension transnationale, la cybercriminalité n'a pas les mêmes incidences dans les différentes régions du monde, particulièrement dans les pays en développement[49]. Les approches régionales mentionnées au paragraphe 32 ci-dessus n'offrent pas la possibilité d'une participation étendue des États non membres. Si la Convention sur la cybercriminalité est à l'heure actuelle l'instrument comptant le plus d'États contractants, elle n'en limite pas moins la possibilité de participation des États non membres puisqu'elle dispose en son

---

[47] Afrique du Sud, Albanie, Allemagne, Arménie, Autriche, Azerbaïdjan, Belgique, Bosnie-Herzégovine, Bulgarie, Canada, Chypre, Croatie, Danemark, Espagne, Estonie, États-Unis, ex-République yougoslave de Macédoine, Finlande, France, Géorgie, Grèce, Hongrie, Irlande, Islande, Italie, Japon, Lettonie, Lituanie, Luxembourg, Malte, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, République de Moldova, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Ukraine.

[48] Albanie, Allemagne, Arménie, Bosnie-Herzégovine, Bulgarie, Chypre, Croatie, Danemark, Estonie, États-Unis, ex-République yougoslave de Macédoine, Finlande, France, Hongrie, Islande, Italie, Lettonie, Lituanie, Norvège, Pays-Bas, République de Moldova, Roumanie, Serbie, Slovaquie, Slovénie et Ukraine.

[49] Voir, par exemple, le rapport de l'Organisation de coopération et de développement économiques, *Spam Issues in Developing Countries* (Paris, OCDE, 2005), p. 4. Disponible à l'adresse: http://www.oecd.org/dataoecd/5/47/34935342.pdf); et *Comprendre la cybercriminalité: Guide,* p. 15 (voir note de bas de page 2).

article 37 que, pour adhérer, les États doivent consulter les États contractants à la Convention et obtenir leur assentiment unanime. De plus, la participation au débat sur d'éventuels amendements futurs est limitée aux Parties à la Convention (art. 44).

35. L'expérience a montré que les États étaient en règle générale peu disposés à ratifier des conventions ou à y adhérer lorsqu'ils n'avaient pas participé à leur élaboration et à leur négociation, quel que soit le sujet des conventions.

36. Lors des quatre réunions régionales préparatoires au douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, des appels ont été lancés pour que soit élaborée une convention internationale relative à la cybercriminalité.

37. Un appel similaire a également été lancé lors des réunions des Chefs des services chargés de la répression au plan national pour l'Afrique, le Proche et le Moyen-Orient et l'Europe, à l'occasion desquelles des discussions ont porté sur Internet, le rassemblement de preuves électroniques, la législation, etc. Lors des réunions tenues dans d'autres régions, les participants ont conclu que les services de détection et de répression et les systèmes judiciaires n'étaient pas assez préparés et n'avaient pas de moyens suffisants pour faire face à l'évolution de la situation en matière de cybercriminalité et pour rassembler et exploiter des éléments de preuve issus des cybertechnologies aux fins d'engager des poursuites. Tous se sont accordés pour dire que les législations nationales ne suivaient pas le rythme et qu'il fallait les modifier pour faciliter les enquêtes, les poursuites et la condamnation des délinquants en se fondant sur des éléments de preuve obtenus à l'aide des cybertechnologies. Il existe un besoin urgent de règles communes et de coopération entre États afin que les autorités puissent agir de manière efficace par delà les juridictions et que les délinquants soient traduits en justice. Des appels en faveur d'un instrument international sont également parvenus du monde universitaire[50].

3. Réponses aux tendances récentes

38. La cybercriminalité ne cesse de changer. Lorsque les approches régionales telles que la loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique et la Convention sur la cybercriminalité ont été élaborées, les attaques de grande ampleur au moyen de réseaux d'ordinateurs zombies, le "hameçonnage" et l'utilisation d'Internet à des fins terroristes étaient encore inconnus ou ne jouaient pas un rôle aussi important qu'aujourd'hui; ces nouvelles formes de cybercriminalité ne font donc pas l'objet de dispositions spécifiques. Lors des réunions régionales préparatoires au douzième Congrès, on a examiné la demande tendant à ce que l'on s'attaque à ces nouveaux phénomènes, dont l'utilisation d'Internet à des fins terroristes, qui va de la propagande, de la communication et du financement du terrorisme par des services de paiement sur Internet à la collecte de renseignements sur une cible potentielle. Ce phénomène et

---

[50] Joachim Vogel, "Towards a global convention against cybercrime", document présenté à la première Conférence mondiale de droit pénal, Guadalajara (Mexique), 19-23 novembre 2007; Stein Schjølberg et Solange Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and Security in Cyberspace* (Oslo, E-dit, 2009).

les réponses qui pouvaient y être apportées sur le plan juridique ont été examinés à plusieurs occasions par l'Équipe spéciale de lutte contre le terrorisme[51].

39. Si, sur le plan du droit pénal positif, de tels phénomènes peuvent souvent être couverts par les dispositions relatives aux atteintes à l'intégrité des systèmes ou à la falsification informatique, l'application des instruments procéduraux prévus dans les instruments régionaux existants est beaucoup plus difficile, notamment du fait que les technologies et les services offerts par le biais d'Internet (les réseaux sociaux, par exemple) ont considérablement évolué. L'interception de communications utilisant la voix sur IP, la recevabilité des moyens de preuve numériques dans le cadre d'une procédure pénale, les procédures à suivre pour enquêter sur des affaires faisant intervenir le cryptage ou des moyens de communication anonymes: ces questions pourtant urgentes ne sont pas traitées au niveau régional et ne le sont que dans certains cas au niveau national[52].

40. Il est important de s'attaquer à ces problèmes car les instruments d'investigation traditionnels sont souvent inefficaces dans le cadre des enquêtes relatives à des affaires de cybercriminalité. L'interception des communications en est un exemple. Au cours des dernières décennies, les États ont élaboré des instruments d'investigation, tels que les écoutes téléphoniques, qui leur ont permis d'intercepter des communications passées à l'aide de téléphones portables et fixes. Les appels téléphoniques traditionnels sont habituellement interceptés par le biais des prestataires de services de télécommunication. Si l'on voulait appliquer ce même principe aux communications par voix sur IP, il faudrait que les services de détection et de répression collaborent avec les prestataires de services de téléphonie sur IP. Or, si leurs services reposent sur le poste à poste[53], ces prestataires ne peuvent généralement pas intercepter de communications dans la mesure où les données sont transférées directement entre les personnes qui communiquent[54]. Par conséquent, de nouvelles techniques, en plus des instruments juridiques qui y sont associés, pourraient se révéler nécessaires.

41. La capacité de mener des enquêtes très pointues est importante non seulement pour ce qui est des nouvelles infractions, mais aussi pour ce qui est des formes plus traditionnelles de cybercriminalité, telles que la pédopornographie. Depuis le milieu des années 1990, les diffuseurs et les consommateurs de pornographie mettant en scène des enfants ont accès à des services en réseaux qui sont utilisés de manière toujours plus intense[55]. Internet est devenu le principal support d'échange de

---

[51] Voir, par exemple: Équipe spéciale de lutte contre le terrorisme, "Report of the Working Group on Countering the Use of Internet for Terrorist Purposes", février 2009. Disponible à l'adresse: www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf.

[52] Pour une vue d'ensemble des différentes approches nationales sur ces questions, voir *Comprendre la cybercriminalité: Guide*, chap. 6 (voir note de bas de page 2).

[53] Le poste à poste (P2P) permet une connectivité directe entre les participants aux réseaux, qui ne sont pas obligés de passer par les structures traditionnelles de serveurs centralisés.

[54] En ce qui concerne l'interception de communications utilisant la voix sur IP par les services de détection et de répression, voir Steven Bellovin *et al.*, "Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP", 13 juin 2006, disponible sur www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf; Matthew Simon et Jill Slay, "Voice over IP: forensic computing implications", document présenté à la 4e Conférence australienne de criminalistique informatique, Perth (Australie), décembre 2006.

[55] États-Unis, Chambre des représentants, "Sexual exploitation of children over the Internet" (2007), 109e Congrès, p. 9.

pédopornographie. Les problèmes liés à la détection des affaires de pédopornographie et aux enquêtes sur le sujet sont connus depuis les années 1990; ils continuent d'exister dans une large mesure parce que les délinquants peuvent utiliser des technologies de pointe pour gêner les enquêtes. Selon une étude, par exemple, 6 % des personnes prises avec du matériel de pédopornographie avaient eu recours au cryptage, 17 % avaient utilisé un logiciel protégé par un mot de passe, 3 % un logiciel éliminant les preuves et 2 % des systèmes de stockage à distance[56]. De plus, un changement a été observé en ce qui concerne la technologie employée: si au tout début d'Internet, l'échange par des voies traditionnelles comme les forums de discussion interactifs sur Internet dominait, au cours des dernières années, le matériel de pédopornographie s'est échangé par le biais d'autres technologies, comme les réseaux de poste à poste [57].

B. Détection et répression

42. La détection et la répression reposent sur des instruments juridiques, mais elles dépendent aussi dans une large mesure de la disponibilité d'outils d'investigation tels que des logiciels de criminalistique (pour rassembler des éléments de preuve, enregistrer les frappes au clavier, décrypter des fichiers ou récupérer des fichiers effacés) et des logiciels ou des bases de données permettant de gérer les enquêtes (par exemple au moyen d'empreintes numériques d'images connues de pornographie mettant en scène des enfants). Au cours des dernières années, plusieurs outils de ce type ont été mis au point et d'autres continuent de l'être[58]. Par exemple, un projet de recherché intitulé "Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis" est actuellement mené à l'University College Dublin (informations disponibles à l'adresse http://cci.ucd.ie/?q=node/33) et, en décembre 2009, une nouvelle technologie permettant de traquer la pédopornographie – dénommée PhotoDNA – a été introduite aux États-Unis. L'un des principaux problèmes liés à la mise au point de tels outils reste la nécessité pour les développeurs de coordonner leurs efforts afin d'éviter les doubles emplois. De même, les efforts des réseaux de points de contact (tels que ceux du Groupe des Huit et d'INTERPOL, et le réseau lié à la Convention sur la cybercriminalité) doivent aussi être coordonnés.

---

[56] Janis Wolak, David Finkelhor et Kimberly J. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crime: Findings From the National Juvenile Online Victimization Study* (Alexandria, Virginie, National Center for Missing and Exploited Children, 2005), p. 9.

[57] États-Unis, General Accountability Office, *File-Sharing Programs, Child Pornography is Readily Accessible over Peer-to-Peer Networks*, audition devant la Commission de la réforme du gouvernement, Chambre des représentants, GAO Rapport GAO-03-537T (Washington, mars 2003); Gretchen Ruethling, "27 charged in international online child pornography ring", *New York Times*, 16 mars 2006; Choo, "Organised crime groups", p. 282 (voir note de bas de page 40); Royaume-Uni, Stockport Safeguarding Children Board, *Safeguarding Children in Stockport: Policy and Practice Handbook* (mai 2008), p. 299, disponible à l'adresse: http://www.safeguardingchildreninstockport.org.uk/documents/Section%2000%20-%20Preface%20and%20contents.pdf.

[58] Voir, par exemple, le projet de recherche intitulé "Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis" mené à l'University College Dublin (informations disponibles à l'adresse: htt://cci.ucd.ie/?q=node/33).

C. Renforcement des capacités

43. La cybercriminalité est un problème non seulement pour les pays développés, mais aussi pour les pays en développement. Selon la Development Gateway Foundation, il y avait en 2005 plus d'internautes dans les pays en développement que dans les pays industrialisés[59]. Le fait que la CEDEAO ait adopté récemment une directive sur la cybercriminalité et que la Communauté de l'Afrique de l'Est ait présenté un projet de cadre juridique sur le sujet sont des signes positifs. Un appui complémentaire pourrait aider les services de détection et de répression à se préparer aux infractions qui pourraient être commises lorsqu'un plus grand nombre d'utilisateurs auront accès au large bande dans le monde en développement. L'Assemblée générale a, dans sa résolution 64/179 intitulée "Renforcement du Programme des Nations Unies pour la prévention du crime et la justice pénale, surtout en ce qui concerne ses capacités de coopération technique", appelé l'attention sur les grands problèmes qui commençaient à se faire jour et que le Secrétaire général avait identifiés (A/64/123), à savoir le piratage, la cybercriminalité, l'exploitation sexuelle des enfants et la délinquance urbaine, et invité l'UNODC à rechercher, dans le cadre de son mandat, les moyens de s'attaquer à ces problèmes.

D. Formation

44. Compte tenu du fait que les enquêtes sur la cybercriminalité et la poursuite des auteurs de ce type d'infractions représentent des défis sans équivalent, il est important de dispenser des formations aux agents des services de détection et de répression, aux procureurs et aux juges. Ainsi que cela a été souligné lors de la réunion du groupe d'experts de l'UNODC sur la cybercriminalité, tenue à Vienne les 6 et 7 octobre 2009, la plupart des organisations régionales et internationales s'occupant de cette question ont adopté des mesures afin que des experts soient formés pour enquêter sur la cybercriminalité et que du matériel de formation soit mis au point[60].

---

[59] Informations disponibles à l'adresse: http://topics.developmentgateway.org/special/informationsociety.

[60] Par exemple, l'Association de coopération économique Asie-Pacifique a organisé plusieurs activités de formation sur la cybercriminalité, notamment sur la législation en la matière; le Commonwealth a organisé des sessions de formation juridique et technique; le Conseil de l'Europe a contribué à des activités de formation dans différentes parties du monde et mis au point du matériel de formation spécifique à l'intention des juges; l'Union européenne a appuyé la mise au point de sessions et de matériel de formation pour les services de détection et de répression de ses États membres et organisé plusieurs sessions de formation en Europe et hors d'Europe; INTERPOL a organisé plusieurs sessions de formation à l'intention des services de détection et de répression et mis au point du matériel de formation; l'UIT a mis au point du matériel de formation sur la cybercriminalité dans toutes les langues officielles de l'Organisation, dispensé une formation générale à l'occasion de plusieurs événements régionaux et dispensé des formations spécifiques à l'intention des juges.

IV. Conclusions et recommandations

45. Enquêter sur la cybercriminalité et en poursuivre les auteurs est un défi pour toutes les institutions concernées. Compte tenu de la complexité du problème et des progrès techniques constants, il demeure essentiel de maintenir et de développer encore la formation pour toutes les autorités concernées. Les discussions qui ont eu lieu à la réunion que le groupe d'expert sur la cybercriminalité de l'UNODC a tenue en 2009 ont montré que le renforcement des capacités et la viabilité à long terme étaient deux facteurs clefs pour mesurer la réussite des initiatives à venir.

46. Si l'on veut éliminer les refuges et resserrer la coopération internationale, il conviendrait de s'attacher à réduire les disparités entre les législations actuelles et à promouvoir l'homogénéité, la cohérence et la compatibilité des lois. Compte tenu de l'importance qu'il y a à harmoniser les législations et à s'appuyer sur les résultats des réunions préparatoires au douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, il conviendrait d'examiner attentivement et favorablement la question de l'élaboration d'une convention mondiale contre la cybercriminalité.

47. En attendant, l'UNODC, qui fixe des règles en matière de prévention du crime et de justice pénale, servira de plate-forme multilatérale et concentrera ses efforts sur les pays en développement. L'Office continuera de suivre une approche générale, multidisciplinaire et fondée sur le partenariat, en conjuguant les compétences avérées qui sont les siennes en matière de lutte contre les activités criminelles sur les plans juridique, technique et de la détection et de la répression avec les compétences spécifiques et bien développées de ses partenaires clefs déjà actifs dans la lutte contre la cybercriminalité. L'UNODC s'efforcera de mettre en place des partenariats et de rapprocher les outils et les experts, y compris du secteur privé (en particulier les fournisseurs d'accès à Internet), pour s'attaquer au problème dans un pays donné ou une région donnée. La priorité ira à la fourniture d'une assistance technique aux États Membres qui en ont besoin, dans le but de palier le manque de moyens et de compétences, et de garantir la viabilité à long terme de la lutte contre la criminalité liée à l'informatique.

48. En particulier, l'UNODC se donnera pour tâche: d'aider les États Membres à adopter une législation visant à garantir l'efficacité des enquêtes relatives aux infractions liées à l'informatique et des procédures engagées contre leurs auteurs; de développer les connaissances opérationnelles et techniques des juges, des procureurs et des agents des services de détection et de répression dans le domaine de la cybercriminalité, par la formation, l'adaptation/élaboration de matériel de formation sur les enquêtes et les poursuites relatives à des infractions liées à l'informatique, etc.; de former les services de détection et de répression à la bonne utilisation des mécanismes de coopération internationale pour lutter contre la cybercriminalité; de sensibiliser la société civile et de créer une dynamique parmi les décideurs pour unir les efforts visant à prévenir et combattre la cybercriminalité; et d'identifier et de diffuser des bonnes pratiques et de promouvoir des partenariats public-privé en vue de prévenir et combattre la cybercriminalité.