Nations Unies A/CONF.203/14

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

Distr.: Générale
14 mars 2005
Français
Original: Anglais

Bangkok, 18-25 avril 2005

Point 3 de l'ordre du jour provisoire*
Mesures efficaces contre la criminalité transnationale organisée

Atelier 6: Mesures de lutte contre la criminalité liée à l'informatique**

Document de travail***

Résumé

La prolifération, partout dans le monde, des nouvelles technologies de l'information et de la communication (TIC) a suscité une multiplication de nouveaux types de délits liés à l'information, qui constituent une menace non seulement pour la confidentialité, l'intégrité et la disponibilité des systèmes informatiques mais aussi pour la sécurité d'infrastructures critiques. De plus, comme l'innovation technologique n'est pas partout adoptée de la même façon, l'on se trouve en présence de schémas différents d'innovation dans l'activité criminelle, de sorte que les différentes menaces imposées par la criminalité liée à l'informatique reflètent les différences qui existent aux extrémités de ce qu'il est convenu d'appeler le "fossé numérique". Pour combattre ce type de délinquance, les enquêteurs et les procureurs comme les juges se heurtent à un certain nombre de problèmes découlant en fait de ce que les preuves numériques sont à la fois intangibles et éphémères. De plus, pour pouvoir efficacement faire enquête sur la criminalité liée à l'informatique et entamer des poursuites, il faut souvent retracer l'activité criminelle et ses effets à travers toute une série de prestataires de services Internet ou d'entreprises parfois situées dans des pays différents, ce qui peut susciter d'épineuses questions de compétence et de souveraineté.

La complexité des défis engendrés par la criminalité liée à l'informatique

---

* A/CONF.203/1.

** Le Secrétaire général tient à remercier l'Institut coréen de criminologie de Séoul et le Ministère de la justice du Gouvernement canadien d'avoir aidé à organiser l'atelier 6.

*** La publication du présent document a été retardée par les recherches et consultations supplémentaires qui se sont avérées nécessaires.

V.05-82260 (F) 040405 050405

exige inévitablement une coopération internationale, ce qui signifie qu'en définitive, les pays doivent se doter des outils nécessaires en matière de législation, de procédure et de réglementation. Pour élaborer des méthodes propres à resserrer la coopération internationale dans la lutte contre la criminalité liée à l'informatique, divers efforts ont été entrepris ces dernières années aux échelons régional et interrégional, qui ont débouché sur d'importantes réalisations. Si l'on veut que ces efforts soient couronnés de succès, il faudra appuyer une large gamme de recherches sur les divers aspects qui interviennent dans la lutte contre la criminalité liée à l'informatique ainsi qu'encourager un partenariat dynamique entre les pouvoirs publics et le secteur privé.

Le présent document de travail met en relief les problèmes que soulève la criminalité liée à l'informatique pour aider les participants à l'atelier 6 à examiner les recommandations formulées par les réunions préparatoires régionales du onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale et à tracer la marche à suivre pour permettre une intervention mondiale efficace

Table des matières

I. Introduction

1. Les technologies de l'information et de la communication transforment les sociétés partout dans le monde. L'innovation crée de nouveaux marchés de biens et de services. Ces technologies révolutionnent les méthodes de travail, accroissent la productivité dans les industries classiques et donnent une configuration très nouvelle à la nature et à la rapidité des courants de capitaux. Néanmoins, ces transformations économiques ne sont qu'un aspect du phénomène. Les sociétés traversent en effet elles aussi de profonds bouleversements culturels encouragés par les médias et l'expansion incessante de l'Internet. La multiplication des nouvelles technologies de l'information et de la communication partout dans le monde fait planer une ombre dans la mesure où elle a rendu possible une nouvelle forme d'exploitation, de nouvelles possibilités d'activités criminelles et en fait de nouvelles formes de criminalité.

2. Les quatre réunions préparatoires régionales du onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale ont formulé à l'intention de ce dernier un certain nombre de recommandations tendant notamment: a) à examiner la situation actuelle, les cadres juridiques nationaux existants et les arrangements de coopération entre États ainsi qu'entre États et prestataires de services Internet; b) à examiner les moyens les mieux appropriés de promouvoir la coopération et l'échange de compétences, de savoirs et de connaissances techniques entre les gouvernements et le secteur privé en vue de mettre en place des mécanismes de nature à prévenir et à maîtriser la criminalité liée à l'informatique et à garantir la sécurité des réseaux informatiques des systèmes d'information ainsi que l'existence de mécanismes d'intervention appropriés; c) à étudier les moyens de mettre les gouvernements mieux à même d'élaborer et d'appliquer des méthodes d'enquête spéciales adéquates et de renforcer les capacités de leurs services de répression, notamment en élaborant et organisant de larges programmes de formation à l'intention des agents des systèmes de justice pénale; d) à s'attaquer à l'utilisation des technologies informatiques pour l'exploitation des femmes et des enfants, spécialement dans le contexte de la pornographie et de la pédophilie; e) à examiner les possibilités de mettre en place sur Internet une équipe spéciale mondiale chargée de promouvoir la coopération internationale dans la lutte contre la criminalité liée à l'informatique; et f) à étudier l'opportunité de proposer la négociation de nouvelles conventions contre la cyberdélinquance en vue de poser les bases d'une intervention collective efficace contre cette forme d'activité criminelle.[1]

La conceptualisation de la "criminalité liée à l'informatique" ou d'expressions semblables comme "cyberdélinquance" est une question qui est débattue depuis 30 ans. Le prototype remonte à un rapport de l'Institut de recherche de l'Université de Stanford[1] qui est réapparu sous une forme légèrement modifiée en 1979[2] et en 1989[3] et son architecture a été largement utilisée dans les articles ultérieurs sur la cyberdélinquance: l'ordinateur comme sujet d'un crime; l'ordinateur comme objet d'un crime; ou l'ordinateur comme instrument d'un crime (le quatrième rôle proposé en 1973, l'ordinateur comme symbole, paraît avoir disparu pendant les années 80). Une reformulation utile de ce modèle conceptuel consiste à considérer la criminalité liée à la délinquance comme tout comportement interdit par la législation et/ou par la jurisprudence qui: a) est

La conceptualisation de la "criminalité liée à l'informatique" ou d'expressions semblables comme "cyberdélinquance" est une question qui est débattue depuis 30 ans. Le prototype remonte à un rapport de l'Institut de recherche de l'Université de Stanford[1] qui est réapparu sous une forme légèrement modifiée en 1979[2] et en 1989[3] et son architecture a été largement utilisée dans les articles ultérieurs sur la cyberdélinquance: l'ordinateur comme sujet d'un crime; l'ordinateur comme objet d'un crime; ou l'ordinateur comme instrument d'un crime (le quatrième rôle proposé en 1973, l'ordinateur comme symbole, paraît avoir disparu pendant les années 80). Une reformulation utile de ce modèle conceptuel consiste à considérer la criminalité liée à la délinquance comme tout comportement interdit par la législation et/ou par la jurisprudence qui: a) est dirigé contre les technologies de calcul électronique et de communication elles-mêmes; b) fait intervenir l'utilisation de technologies numériques pour la commission de l'infraction; et c) suppose l'utilisation incidente d'ordinateurs pour la commission d'autres infractions, l'ordinateur étant alors une source de preuves numériques.[4] La législation et les traités, y compris la Convention sur la cyberdélinquance du Conseil de l'Europe,[5] ont défini divers types de crimes liés à l'informatique, comme les crimes contre la confidentialité, l'intégrité ou la disponibilité des systèmes informatiques; les infractions liées au contenu des messages Internet; et les infractions liées à la propriété intellectuelle.

II. La criminalité liée à l'informatique

3. Il existe divers types de crimes dirigés contre les technologies de l'information et de la communication elles-mêmes, qui sont parfois rangés dans la catégorie des crimes contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques. Il s'agit notamment du vol, sous différentes formes, de services de télécommunications ou de services informatiques au moyen de différentes techniques de piratage (selon la méthode utilisée, il peut s'agir d'un accès non autorisé aux services informatiques, du déchiffrage de codes et de mots de passe, d'un clonage numérique, d'utilisation illégale de cartes de crédit, etc.). Les serveurs et les sites web peuvent faire l'objet d'attaques tendant à paralyser leurs services. Dans certains cas, des douzaines ou des centaines d'ordinateurs infectés sont utilisés comme "zombies" pour bombarder la cible de demandes qui deviennent si nombreuses qu'il ne peut être donné suite à aucune d'entre elles. Dans d'autres cas, la paralysie des services provient de "tempêtes de paquets" créées par la reproduction latente de virus ultra rapides (par exemple des programmes informatiques qui se reproduisent automatiquement) qui, en quelques minutes, se reproduisent en milliards d'exemplaires qui, par leur volume même, étouffent les systèmes à fibres optiques les plus rapides et paralysent même les ordinateurs les plus puissants. Des épidémies mondiales de virus informatiques perturbent les réseaux utilisés par les entreprises et les consommateurs depuis 20 ans déjà, ces épidémies étant périodiquement ponctuées de nouveaux types de vers et de virus particulièrement virulents et destructeurs. Deux exemples récents illustrent les deux extrêmes de la spécialisation: l'on trouve à un extrême les vers qui attaquent des dizaines de millions de systèmes informatiques utilisant les systèmes d'exploitation et les applications les plus populaires, et, à l'autre, les vers conçus de manière à n'attaquer que des applications hautement sécurisées qui ne sont utilisées que sur quelques milliers de plateformes.

Deux Australiens de Melbourne ont envoyé entre 6 à 7 millions de courriels à des adresses électroniques d'Australie et des États-Unis et ont affiché d'innombrables messages sur les panneaux des principaux prestataires de services Internet. Ces communications avaient pour objet d'encourager l'achat d'actions dans une société américaine cotée au marché NASDAQ. Ces messages, envoyés sous de faux noms et transmis par l'entremise de serveurs tiers, laissaient entrevoir une hausse de 900% du cours des actions de la société. Peu après, le volume des actions échangées en Bourse et leur cours ont doublé avant que les opérations sur ces actions soient suspendues lorsque la société a refusé de confirmer les affirmations faites dans ces différentes communications.

Les deux auteurs de ce stratagème avaient organisé une opération classique appelée "gonfler et vendre": l'un des complices, actionnaire de la société, diffusait des informations erronées et, après la hausse du cours des actions de la société, les vendait en faisant un bénéfice.

Ces deux personnes avaient agi en contravention de la législation aussi bien de l'Australie que des États-Unis. Outre qu'ils avaient manipulé le cours, le volume du trafic généré pour les courriels qu'ils avaient envoyés était suffisant pour constituer une ingérence dans le fonctionnement licite des ordinateurs. La Commission australienne des opérations boursières (ASIC) est alors intervenue à la suite des plaintes du public australien, notamment sur la base des informations fournies par les autorités américaines. Les auteurs de ce stratagème ont été retrouvés en retraçant les courriels distribués par l'entremise de réseaux innocents et des opérations financières correspondant au paiement des services Internet.

Comme cela est actuellement le cas en présence d'infractions de ce type, la Commission des opérations boursières des États-Unis a demandé aux tribunaux de prononcer une ordonnance interdisant aux deux complices, avec caractère immédiat et définitif, de poursuivre leurs activités. Ces derniers ont été tenus de restituer tous leurs bénéfices illicites et de s'engager à ne plus jamais agir de la sorte. Les autorités américaines s'en sont remises aux autorités australiennes pour entreprendre les poursuites pénales appropriées dans ce pays. L'ASIC a déposé 19 plaintes pénales contre les deux inculpés. L'un et l'autre ont plaidé coupable et ont reconnu avoir diffusé des informations fausses ou trompeuses afin d'encourager l'achat de valeurs mobilières et avoir fait obstruction à l'utilisation des sites d'un ordinateur. L'un et l'autre ont été condamnés à des peines de prison de deux ans avec sursis (dans le cas du délinquant principal, après trois mois de détention provisoire).

4. Dans le secteur des entreprises, la privation d'accès aux données va de situations dans lesquelles les données peuvent être récupérées (par exemple lorsqu'un employé mécontent crypte des dossiers sans autorisation) à une destruction irrémédiable des données (le fait de ne pas simplement éliminer les dossiers mais de retirer et/ou de détruire les disques durs ou autres supports de stockage des dossiers). Les réseaux locaux sans fil, de plus en plus largement utilisés par les entreprises ces dernières années, peuvent être exposés à des attaques visant à paralyser les services, par exemple au moyen d'un brouillage, même lorsqu'ils ont été sécurisés pour empêcher tout accès non autorisé.[6]

5. Il est essentiel aussi de bien comprendre comment les ordinateurs sont utilisés comme instruments ou moyens pour commettre d'autres délits. Il y a d'innombrables variantes de délits liés à la modification de données, dont certains sont simplement du vandalisme électronique (comme la modification malveillante de sites web), mais d'autres constituent des faux ou des opérations de contrefaçon qui sont le fait de professionnels. Il existe des sites web où l'on peut obtenir des cartes de crédit falsifiées qui offrent notamment de la fausse monnaie et des faux passeports de haute qualité. Le vol de données[7] englobe une large gamme de délits allant du piratage de l'information et de l'espionnage industriel à la violation des droits d'auteur (vol de la propriété intellectuelle sous forme de logiciels piratés, de dossiers musicaux sur MP3, de vidéos numériques, etc.).[8] Le vol de données peut constituer non seulement un délit économique mais aussi une violation du droit à l'intimité et des droits connexes de l'individu dans le contexte des nouveaux délits liés au vol d'identité.

6. Il existe beaucoup de délits liés à l'informatique qui constituent un vol pur et simple, comme l'introduction clandestine dans le système des banques ou des systèmes financiers ou les virements électroniques frauduleux de fonds. Des préoccupations ont été exprimées aussi quant à la possibilité d'utiliser des moyens électroniques pour le blanchiment d'argent ou l'évasion fiscale.

7. Les ordinateurs sont utilisés aussi pour faciliter une large gamme d'opérations frauduleuses visant à tromper le consommateur pour l'amener à acheter des produits ou à investir. Les enchères frauduleuses sont apparemment la fraude la plus communément dénoncée par les consommateurs: en 2003, selon un rapport détaillé publié aux États-Unis au sujet de la fraude informatique, ces plaintes représentaient 61% du total.[9] D'autres formes de fraudes à la consommation relèvent de la catégorie plus générique du "défaut de livraison des marchandises ou de paiement" à la suite d'une transaction sur Internet. La fraude sur valeurs mobilières, c'est-à-dire la manipulation en Bourse d'investissements de faible valeur, demeure relativement rare au niveau des consommateurs.

> Un adolescent canadien d'une quinzaine d'années, après avoir pris le contrôle d'un certain nombre d'ordinateurs, les a utilisés pour monter des attaques visant à paralyser le service de Yahoo, d'Amazon.com et d'autres importants sites de commerce électronique en février 2000. En ralentissant ou limitant l'accès à ces sites web, il a causé à leurs propriétaires des millions de dollars de manque à gagner, a fait baisser leurs actions et leur a coûté fort cher lorsqu'ils ont dû renforcer la sécurité de leurs systèmes. Après s'être vanté de ces attaques sur Internet, l'adolescent a été identifié par le Federal Bureau of Investigation des États-Unis, qui a saisi de l'affaire la Gendarmerie royale canadienne. Rares sont les pays, si tant est qu'il y en ait, qui sont disposés à extrader des délinquants juvéniles et, en l'occurrence, la législation canadienne interdisait l'extradition de l'intéressé. En septembre 2001, il a été condamné à huit mois de détention dans une maison de correction.

8. Le "phishing" (ou "pêche au spam") consiste à envoyer des courriels provenant de pages web conçues de manière à apparaître comme des sites commerciaux légitimes. Comme le spam, des millions de ces courriels frauduleux sont distribués mais, plutôt que d'offrir simplement de vendre des produits ou des services, ces courriels se présentent comme provenant de banques, de sociétés de vente aux enchères en ligne ou d'autres sites légitimes et cherchent à amener les usagers à répondre et à communiquer des informations personnelles ou commerciales et des mots de passe. Les informations ainsi rassemblées

sont ensuite utilisées pour des achats frauduleux (parfois après que ces informations ont été vendues à une tierce partie).

9. L'on trouve également sur Internet des infractions classiques comme le chantage (menaces de divulguer des informations brevetées ou des informations personnelles ou de compromettre des données ou des systèmes) et le harcèlement. Il y a également eu des cas de diffamation et de calomnie qui ont été portés devant la justice, avec succès.

10. Par ailleurs, il existe toute une série de délits liés à l'informatique qui proviennent du contenu des messages, et tel est particulièrement le cas de diffusion de messages illégaux ou préjudiciables. La pornographie mettant en scène des enfants est un de ces crimes qui préoccupent particulièrement la communauté internationale. Bien que ce type de pornographie existe depuis de nombreuses décennies (sous forme de photographies, de revues, de films et de bandes vidéo), l'on constate depuis la fin des années 80 une tendance croissante à la diffusion de ce type de pornographie par différents réseaux informatiques et toute une série de services Internet, dont sites web, newsgroups de l'Usenet, serveurs IRC (Internet Relay Chat) et réseaux poste-à-poste (P2P).[10] Ces réseaux ont été utilisés pour faciliter les échanges d'informations concernant le commerce d'images ou bandes vidéo pornographiques mettant en scène des enfants, ainsi que des informations sur des transactions monétaires et des informations concernant le tourisme sexuel exploitant des enfants. Une certaine proportion de la pornographie mettant en scène des enfants qui est distribuée sur Internet l'est à des fins commerciales (plutôt que de constituer des trocs non monétaires entre pédophiles), et ce phénomène est associé à la criminalité transnationale organisée. Il existe aussi une "zone grise" moins clairement définie, dans laquelle l'illégalité passe dans un domaine généralement toléré, l'Internet étant utilisé depuis plus de 25 ans pour distribuer de la pornographie, souvent légitimement, dans de nombreux pays, et à des fins commerciales, ces activités étant souvent appelées l'"industrie du divertissement pour adultes".[11] Il y a d'autres cas encore qui sont plus clairement définis; certaines représentations de caractère pornographique (que ce soit sous forme d'images numériques ou de bandes vidéo) sont considérées comme obscènes par la loi dans de nombreux pays, et la diffusion de telles images obscènes constitue une infraction. L'Internet a également été utilisé pour d'autres délits comme la diffusion de propagande incitant à la haine et de slogans xénophobes.[12]

L'un des cas les plus connus des années 90 a été l'attaque lancée contre Citibank par un jeune homme qui, en Fédération de Russie, avait réussi à accéder sans autorisation au serveur de la banque aux États-Unis. Avec l'aide d'un certain nombre de complices, il avait ouvert des comptes dans différentes banques du monde entier puis donné aux ordinateurs de Citibank l'ordre de virer des fonds à ces divers comptes. Lorsque ce stratagème a été découvert et que son auteur a été identifié, un tribunal fédéral aux États-Unis a délivré un mandat d'arrestation. À l'époque, il n'existait pas de traité d'extradition entre la Fédération de Russie et les États-Unis, mais l'inculpé a commis l'erreur de se rendre au Royaume-Uni pour assister à une foire informatique. Conformément aux dispositions en vigueur en matière d'extradition entre le Royaume-Uni et les États-Unis, les autorités britanniques pouvaient fournir une assistance aussi longtemps que l'infraction dont l'intéressé était accusé avait un équivalent en droit britannique. L'accusé a présenté une requête en *habeas corpus* pour contester l'extradition, faisant valoir, entre autres, que l'infraction s'était produite en Fédération de Russie, où se trouvait le clavier de son ordinateur, qui n'était pas aux États-Unis. La Cour a considéré que le fait que l'accusé se trouve physiquement présent à St. Pétersbourg avait moins d'importance que le fait qu'il opérait sur un disque

L'un des cas les plus connus des années 90 a été l'attaque lancée contre Citibank par un jeune homme qui, en Fédération de Russie, avait réussi à accéder sans autorisation au serveur de la banque aux États-Unis. Avec l'aide d'un certain nombre de complices, il avait ouvert des comptes dans différentes banques du monde entier puis donné aux ordinateurs de Citibank l'ordre de virer des fonds à ces divers comptes. Lorsque ce stratagème a été découvert et que son auteur a été identifié, un tribunal fédéral aux États-Unis a délivré un mandat d'arrestation. À l'époque, il n'existait pas de traité d'extradition entre la Fédération de Russie et les États-Unis, mais l'inculpé a commis l'erreur de se rendre au Royaume-Uni pour assister à une foire informatique. Conformément aux dispositions en vigueur en matière d'extradition entre le Royaume-Uni et les États-Unis, les autorités britanniques pouvaient fournir une assistance aussi longtemps que l'infraction dont l'intéressé était accusé avait un équivalent en droit britannique. L'accusé a présenté une requête en *habeas corpus* pour contester l'extradition, faisant valoir, entre autres, que l'infraction s'était produite en Fédération de Russie, où se trouvait le clavier de son ordinateur, qui n'était pas aux États-Unis. La Cour a considéré que le fait que l'accusé se trouve physiquement présent à St. Pétersbourg avait moins d'importance que le fait qu'il opérait sur un disque magnétique qui était situé aux États-Unis. De plus, les actes dont l'intéressé avait été accusé avaient manifestement des équivalents sanctionnés par la loi britannique de 1990 relative à la répression des délits liés à l'informatique; si l'intéressé avait opéré à partir des États-Unis plutôt que de la Fédération de Russie, les tribunaux britanniques auraient été compétents. L'inculpé a été extradé aux États-Unis, où il a été condamné et emprisonné.

11. Ces dernières années, la corrélation entre le terrorisme et l'Internet a de plus en plus retenu l'attention bien que, dans ce domaine également, les activités en cause soient extrêmement diverses. Certaines indications portent à penser que l'Internet est utilisé pour faciliter le financement du terrorisme et comme un outil logistique pour planifier et exécuter des actes terroristes. En outre, l'attention se porte de plus en plus sur l'utilisation qui est faite d'Internet pour diffuser de la propagande terroriste et pour recruter des terroristes. Ces activités se distinguent du "cyberterrorisme", qui est défini par le Centre national de protection de l'infrastructure des États-Unis comme étant "un acte criminel perpétré au moyen d'ordinateurs qui entraîne violence, mort et/ou destruction et sème la terreur dans le but d'obliger un gouvernement à changer de politique".[13] Il y a à cet égard deux aspects distincts: les attaques dirigées contre des données névralgiques et les attaques dirigées contre les éléments névralgiques d'infrastructure.

12. L'importance des éléments névralgiques de l'infrastructure de l'information est de plus largement admise, dans la mesure où il s'agit de réseaux qui non seulement rendent les communications possibles mais en outre sont utilisés pour gérer et administrer des infrastructures majeures comme l'énergie, les transports, l'alimentation et la santé publique. Dans beaucoup de pays du monde, il arrive que les éléments névralgiques d'infrastructure appartiennent à des entreprises privées et soient particulièrement vulnérables car beaucoup des progiciels de supervision (DCS) et des systèmes d'acquisition et de contrôle des données (SCADA) sont reliés à l'Internet, et peuvent ainsi être paralysés par son intermédiaire. Étant donné l'interdépendance croissante qui caractérise les sociétés modernes, des attaques contre de tels éléments d'infrastructure peuvent immédiatement avoir de graves répercussions sur les systèmes économiques et politiques nationaux et aussi avoir de larges effets transfrontières. Il est essentiel de pouvoir réagir à de telles attaques (qu'elles soient motivées par le terrorisme ou d'autres activités criminelles) pour

réduire au minimum le risque grave d'effets en cascade sur d'autres éléments critiques d'infrastructure essentiels au bon fonctionnement de la société.

13. Les problèmes causés par l'existence et la large disponibilité de puissants systèmes de cryptage, qui retiennent l'attention de la communauté internationale depuis cinq ans, n'ont pas été réglés, et la nouvelle génération de cryptographie quantique se profile aujourd'hui à l'horizon.[14] Bien que la cryptographie soit essentielle dans les affaires et le commerce électronique, elle a également été utilisée par les criminels. Le dilemme créé par les "technologies à double usage" va au-delà de la stéganographie pour s'étendre à divers types de progiciels de communication poste-à-poste aisément disponibles assortis de systèmes de cryptage extrêmement résistants à la censure (comme le logiciel Freenet). Cette technologie encourage la liberté d'expression et peut contribuer à la propagation des libertés démocratiques, mais peut aussi être employée par des criminels pour dissimuler leurs communications ou diffuser des messages illégaux.

III. Le fossé numérique et la criminalité liée à l'informatique

14. Les technologies de l'information et de la communication se propagent certes partout dans le monde, mais leur diffusion n'est pas uniforme. Dans certaines régions, il se peut qu'il soit installé un vaste système de câbles à fibres optiques mais, ailleurs, ce sont les réseaux de téléphonie mobile et de communication sans fil qui se développent le plus rapidement. Comme les technologies ne sont pas adoptées de la même façon, les régions sont exposées à des risques divers, et il apparaît des types spécifiques de criminalité liée à l'informatique qui exploitent les différentes circonstances.

15. Les transformations ont été spectaculaires: par suite de l'explosion du volume des appareils qui font appel aux technologies de l'information et du calcul électronique partout dans le monde, il existe aujourd'hui plus de 2 milliards d'ordinateurs et d'autres types de matériel commandés par des microprocesseurs; la connectivité a augmenté dans des proportions exponentielles; et on assiste à une révolution de l'informatique qui se manifeste dans des domaines comme la miniaturisation, la rapidité et la mémoire; des systèmes intelligents et la robotique ont fait leur apparition; et l'interaction entre l'homme et l'ordinateur devient de plus en plus facile. Or, cette révolution technologique non seulement affecte tous les aspects de l'environnement en reliant l'homme, les objets et l'information d'une manière qui ne s'était jamais vue, mais aussi laisse entrevoir une nouvelle génération de menaces et de vulnérabilité numériques et appelle une refonte totale des idées touchant la nature de la criminalité au XXI^{e} siècle.

16. Consciente de cette réalité, l'Assemblée générale a, en 2002, encouragé la communauté internationale à redoubler d'efforts pour aider les États Membres à combattre la criminalité liée à l'informatique. Dans sa résolution 56/261 du 31 janvier 2002, intitulée "Plans d'action concernant la mise en oeuvre de la Déclaration de Vienne sur la criminalité et la justice: relever les défis du XXI^{e} siècle", l'Assemblée générale a inclus une section spécialement consacrée à la lutte contre la criminalité liée à la haute technologie et à l'informatique contenant des recommandations concernant les interventions et politiques à mettre en oeuvre pour prévenir et réprimer de telles formes de criminalité. Dans sa résolution 57/170 du 18 décembre 2002, l'Assemblée a invité la Commission pour la prévention du crime et la justice pénale à formuler des recommandations tendant à ce que le onzième Congrès, lorsqu'il formulerait des recommandations conformément à la résolution 56/119 de l'Assemblée générale en date du 17 décembre 2001, tienne compte

des progrès accomplis dans la mise en oeuvre de la Déclaration de Vienne et des plans d'action.

17. Le constat de l'existence du fossé numérique a, dès le début du XXIe siècle, été l'un des piliers des activités réalisées par l'Organisation des Nations Unies dans ce domaine. Le contexte général est la Déclaration du Millénaire de l'Organisation des Nations Unies, que l'Assemblée générale a adoptée dans sa résolution 55/2 du 8 septembre 2000. Sous la rubrique de l'Objectif 8 des Objectifs du Millénaire pour le développement, qui figurent en annexe du Rapport du Secrétaire général intitulé "Plan de campagne pour la mise en oeuvre de la Déclaration du Millénaire"(A/56/326), la Cible 18 a été définie comme étant: "En coopération avec le secteur privé, faire en sorte que les avantages des nouvelles technologies, en particulier des technologies de l'information et de la communication, soient accordés à tous". Dans la Déclaration de principes adoptée par le Sommet mondial sur la société de l'information, tenu à Genève du 10 au 12 décembre 2003, les participants ont exprimé comme suit leur vision commune de la société de l'information (A/C.3/59/3, chapitre I, section A): "Nous sommes également pleinement conscients du fait que les avantages de la révolution des technologies de l'information sont aujourd'hui inégalement répartis entre les pays développés et les pays en développement ainsi qu'à l'intérieur des sociétés. Nous sommes fermement résolus à transformer ce fossé numérique en une possibilité numérique pour tous, surtout ceux qui risquent d'être marginalisés et d'être laissés de côté".[15]

À la fin de 2004, 94 millions de personnes avaient accès à Internet en Chine, soit environ 7,2% de la population du pays, dont 45,5% d'usagers de systèmes à bande large. L'on estimait qu'il y avait 41,6 millions de sites, 60 millions d'adresses IPv4, 432 077 noms de domaines et 668 900 sites web.[16] Si la croissance se poursuit à son taux annuel de 18% environ, il y aura plus d'usagers d'Internet en Chine qu'en Amérique du Nord en 2008, et leur nombre dépasse déjà ceux du Japon et de la République de Corée ensemble. En 1999, il n'y avait que 8,9 millions d'usagers, mais ce chiffre est passé à 33,7 millions en 2001, tandis que le nombre de sites est passé de 3,5 millions en 1999 à 33,7 millions en 2001.

18. À la fin de 1985, le nombre de serveurs Internet dépassait 2 000; en 1989, il avait atteint 100 000 et, en 1990, il a dépassé 300 000 avant d'atteindre la barre du million à la mi-1992, 12 millions à la fin de 1995 ou au début de 1996 et 100 millions à la fin de 2000; en juillet 2002, il dépassait 162 millions.[17] En 2002, le monde en développement n'avait que 4,1 usagers d'Internet et 3,3 ordinateurs personnels pour 100 habitants, tandis que ces chiffres étaient de 33,3 et de 36,2 respectivement dans le monde développé (E/2004/62 et Corr. 1). Le cinquième de la population mondiale vivant dans les pays riches représentait 81,9% du nombre total d'ordinateurs personnels dans le monde, 76,2% du nombre total d'usagers d'Internet et 97,5% de serveurs.[18]

19. Dans la plupart des pays en développement, il n'existe pas de réseaux de télécommunications sur lesquels puissent fonctionner des systèmes d'information et de communication aussi dynamiques, modernes et efficaces. En 2000, selon les chiffres de l'Organisation des Nations Unies, 4,5% seulement de la population mondiale avaient accès à un réseau, contre 44% de la population en Amérique du Nord et 10% en Europe, tandis que le pourcentage correspondant en Afrique, en Asie et en Amérique du Sud variait entre 0,3 et 1,6%.[19] À l'heure actuelle, plus de 98% de la bande de fréquence utilisée par le protocole Internet est connectée, dans un sens ou dans l'autre, à l'Amérique du Nord; 55 pays représentaient 99% des dépenses mondiales consacrées aux technologies de

l'information (E/2000/52, par. 50 et 51). L'on constate une claire tendance de l'apparition d'économies fondées sur le savoir mais des éléments autres que le développement, comme la structure des services de télécommunication et le coût d'utilisation de ces services, affectent les possibilités d'accès et d'utilisation.

20. Quoi qu'il en soit, à mesure que les avantages découlant des technologies de l'information et de la communication commencent à se propager plus largement, il faudra aussi susciter une prise de conscience accrue des menaces et des risques que cela peut entraîner par suite de la criminalité liée à l'informatique. Le fossé numérique non seulement définit les différences économiques entre pays développés, pays en développement et pays en transition,[20] mais aussi reflète des schémas distincts pour ce qui est des menaces et risques provenant de la cybercriminalité. Les technologies de l'information et de la communication sont adoptées à un rythme différent dans les diverses régions non seulement en raison des disparités entre riches et pauvres mais aussi par suite de facteurs comme la géographie régionale. Par exemple, dans certains pays montagneux, les coûts de la pose de câbles souterrains de télécommunication peuvent être prohibitifs, de sorte que la construction de pylônes et d'antennes de relais à micro-ondes permet d'adopter des systèmes de téléphonie sans fil. Aussi les utilisations qui sont faites des technologies de l'information et des communications dans un pays ou une région peuvent être très différentes de ce qu'elles sont dans la région ou le pays voisin. Comme l'innovation technologique n'est pas adoptée de la même façon, l'innovation criminelle évolue de façon différente aussi, d'où l'existence de menaces différentes sur le plan de la criminalité liée à l'informatique.

21. Un pays en développement doté d'une infrastructure de télécommunication rudimentaire peut néanmoins être utilisé comme tremplin pour des attaques ou comme plaque tournante pour des attaques, particulièrement s'il n'existe pas de sanctions visant à décourager la criminalité liée à l'informatique ou à les réprimer. Dans le cas de pays en développement, les types de technologies initialement déployées peuvent déboucher sur des menaces nouvelles pour la région. Certains diraient que des structures informatiques nouvelles et encore fragiles risquent d'être particulièrement vulnérables jusqu'à ce que les systèmes deviennent plus robustes et les normes de sécurité soient renforcées.[21]

22. Le type et l'envergure des ordinateurs et des réseaux informatiques, dans le monde des affaires et dans le secteur public, peuvent beaucoup varier par rapport à ce qu'ils sont dans le secteur des usagers particuliers. Comme la propagation des technologies de l'information et de la communication est plus rapide parmi le public, il apparaît de nouveaux groupes cibles qui sont exposés à des types spécifiques de délits liés à l'informatique, qu'il s'agisse d'infections par un virus et de pénétration des ordinateurs ou de divers types de fraude à la consommation. À mesure que les technologies de l'information et de la communication se propagent dans les pays, divers secteurs de la société sont exposés à différents types de délits informatiques.

IV. Au-delà des frontières: la criminalité transfrontière et la police informatique

23. Pour enquêter sur la criminalité liée à l'informatique, les services de la répression se heurtent à différents problèmes. Il faut notamment reconstruire un délit dans le cas duquel, pour une large part, les éléments de preuve sont intangibles et éphémères. Plutôt que des preuves matérielles, les enquêteurs recherchent des traces numériques souvent changeantes

et aisément détruites. L'une des raisons en est que certains types d'informations concernant les adresses électroniques et les itinéraires empruntés par l'information, c'est-à-dire les "données concernant le trafic", ne sont pas durablement conservées. Ces informations peuvent ne subsister que brièvement dans la mémoire d'un ordinateur puis être couvertes par des informations plus récentes.

24. Les technologies nouvelles créent non seulement des problèmes nouveaux mais aussi des possibilités nouvelles pour les enquêteurs en permettant de reconstruire une trace numérique. Il y a bien des cas dans lesquels les données concernant le trafic et d'autres types d'informations concernant la gestion des réseaux peuvent être conservées en mémoire plutôt que d'être simplement remplacées par des informations plus récentes. Sur Internet ainsi que sur d'autres réseaux informatiques, il est habituellement utilisé différents systèmes de gestion de l'information pour que celle-ci puisse être utilisée par la suite pour faciliter la comptabilité du réseau, vérifier la fiabilité des services ou du matériel, retracer les failles, identifier les tendances des performances et prévenir les capacités. Ces derniers peuvent également être utilisés à des fins de commercialisation et d'études des consommateurs (par exemple, les consultations des sites web de détaillants peuvent aider à déterminer quels sont les produits les plus demandés, les habitudes d'achat ou les caractéristiques des consommateurs).

25. Il intervient néanmoins un certain nombre de considérations qui déterminent si les données concernant le trafic et les informations de ce type seront effectivement conservées. L'une d'elles, par exemple, tient au type de service. Un service d'accès au réseau, par exemple au moyen du protocole Remote Authentication Dial-In User Service (RADIUS) peut conserver certaines informations sur les abonnés et de données sur le trafic avant de leur permettre d'avoir accès à Internet. Tel est notamment le cas pour les services facturés au temps, qui doivent enregistrer l'heure à laquelle l'abonné se connecte et la durée de la connexion. Les services tendant à préserver l'anonymat ou l'intimité des abonnés, en revanche, ne conserveraient que très peu d'informations de ce type.[22]

26. Le courrier électronique, qui remonte aux premiers jours de l'Internet (il existait déjà sur ARPANET en 1971), contient habituellement dans la demande d'accès des informations sur les adresses et d'autres données concernant le trafic.[23] Ces informations sont générées en partie par le programme de l'utilisateur final et en partie par le serveur de courriel (au moyen du protocole simple de transfert de courrier – SMTP).

27. Le service Internet le plus connu est sans doute le World Wide Web, qui utilise essentiellement le système de noms de domaines (DNS) pour établir la corrélation entre les noms des domaines (le nom de l'emplacement des sites web) et les adresses du protocole Internet (IP), c'est-à-dire les adresses numériques à destination et en provenance desquelles se déplacent les paquets de données. Les serveurs web peuvent conserver un volume important de données concernant le trafic, par exemple les pages qui ont été consultées et par qui, c'est-à-dire par quelle adresse IP. Cette pratique est plus commune dans le cas des serveurs commerciaux, du fait que les données concernant les connexions peuvent rapidement représenter plusieurs gigaoctets, de sorte que leur conservation est coûteuse.

28. Les services de transfert des dossiers peuvent aussi, mais tel n'est pas toujours le cas, selon le système, rassembler des informations sur les abonnés. Par le passé, les dossiers étaient transférés par le protocole de transfert des dossiers (FTP) mais, de plus en plus, ces transferts sont sécurisés au moyen d'un cryptage par le protocole Secure Shell (SSH). Récemment, le modèle P2P a commencé à se substituer aux serveurs centraux de dossiers. Le P2P permet un échange de dossiers entre un grand nombre d'usagers (ressources

décentralisées distribuées par des réseaux d'entités transitoires; l'on peut en citer comme exemple, Napster, KaZaA, Morpheus, Gnutella et Freenet). Dans le cas de certaines formes de réseaux P2P, les données concernant le trafic sont aisément accessibles, mais d'autres sont conçus de manière à empêcher toute analyse du trafic.

29. Il y a également d'autres services, dont les quelque 100 000 newsgroups de l'Usenet, qui traitent de presque tous les sujets imaginables. L'on peut y avoir accès au moyen d'un réseau mondial de serveurs de transmission utilisant le protocole de transfert de news de Usenet (NNTP). En pareil cas, une partie des données concernant le trafic peuvent être retrouvées sur le serveur et d'autres sur l'ordinateur personnel local. Il y a aussi d'innombrables formes de salles de discussion en temps réel allant des réseaux IRC aux messages instantanés.

30. Les différents services Internet sont généralement assurés par divers types de matériels comme routeurs ou serveurs. Selon la configuration du site du prestataire de services, il arrive que des données différentes soient conservées sur d'innombrables appareils pouvant être contrôlés par des sociétés différentes et parfois être situés dans des pays différents.

31. Étant donné l'étendue de la gamme de services potentiels, les différents créneaux qui existent sur le marché et toute une série de facteurs, dont le coût de la conservation des données,[24] l'on peut dire que les milieux d'affaires n'ont pas adopté de position unique en ce qui concerne la collecte et la conservation de données concernant le trafic et les abonnés. Il est évident que la conservation de certaines données de ce type peut faciliter le dépistage par les services de répression des criminels qui opèrent sur Internet; certains pays ont récemment adopté des lois qui rendent obligatoire la conservation de ces données. Même en l'absence de lois de cette nature, il est indispensable pour les services de répression de comprendre l'étendue de la gamme de pratiques comptables et de pratiques de gestion des réseaux utilisés par les prestataires de services Internet afin de déterminer dans quelle mesure les habitudes des prestataires de services Internet leur permettent de mener leur tâche à bien.[25] La coopération des prestataires de services Internet, à cet égard, peut être inappréciable dans les enquêtes et poursuites visant des délits liés à l'informatique.

32. Si l'on veut que les enquêtes et les poursuites soient efficaces, il faut souvent retracer l'activité des délinquants par le biais de divers prestataires de services Internet ou sociétés dont les ordinateurs sont connectés à Internet. Les enquêteurs doivent, s'ils veulent aboutir, reconstruire la trace des communications entre l'ordinateur d'origine et l'ordinateur attaqué, en travaillant avec des prestataires de services intermédiaires de divers pays. Pour remonter à la source du délit, les services de répression doivent souvent avoir recours aux registres qui indiquent quand, d'où et par qui les différentes connexions ont été effectuées. Dans d'autres cas, il se peut également que les services de répression doivent remonter à l'origine d'une connexion en cours. Lorsque les prestataires de services se trouvent à l'étranger, ce qui arrive souvent, les services de répression doivent solliciter le concours de leurs homologues d'autres pays. D'une façon générale, les régimes d'entraide judiciaire de type classique, même lorsqu'ils prévoient des procédures accélérées, sont généralement conçus de manière à pouvoir obtenir des données passées ou des données en temps réel en rapport avec des affaires n'impliquant que deux pays (par exemple celui de la victime et celui du délinquant). Lorsqu'un criminel achemine ses communications par l'entremise de trois, quatre ou cinq pays, il faut autant de demandes d'entraide judiciaire avant que les services de répression puissent obtenir des informations de chaque prestataire de services, ce qui

accroît le risque que les données aient disparu et que le délinquant ne puisse pas être découvert et rester ainsi libre de poursuivre ses agissements. [26]

33. Pour faciliter les enquêtes sur la criminalité liée à l'informatique, le Sous-Groupe du G-8 sur la criminalité liée à la haute technologie et à l'informatique a lancé en 1997 le réseau "24-Hour Contacts for International High-Tech", réseau de brigades spécialisées dans la lutte contre la criminalité liée à l'informatique auquel peuvent s'adresser les services de répression 24 heures par jour, 7 jours par semaine, c'est-à-dire sur une base "24/7". Ce réseau de points de contact rassemble actuellement 40 pays et est un aspect qui fait partie intégrante de la mise en oeuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, qui met à la disposition des services de répression une série de méthodes d'enquête pour combattre tout délit commis contre un système informatique au moyen d'un tel système.

34. Du fait de la prévalence d'innombrables virus, vers et pirates qui profitent des points faibles des systèmes, il faut également mettre en place des mécanismes pour rendre possible une intervention immédiate. C'est ainsi que des Computer Emergency Response Teams (CERT) ont été établis dans plusieurs de dizaines de pays du monde. Leurs principaux objectifs sont les suivants:

a) Tenir un répertoire des méthodes employées par les pirates informatiques, des points faibles des systèmes et réseaux informatiques et de l'impact des attaques dirigées contre les données, ainsi que diffuser des informations sur les tendances et les caractéristiques des incidences de la vulnérabilité des systèmes;

b) Offrir une infrastructure composée de spécialistes de la sécurité de plus en plus compétents qui peuvent faire face rapidement aux attaques dirigées contre les systèmes connectés à Internet et mettre les systèmes à l'abri de failles de sécurité;

c) Fournir des méthodes pour évaluer, améliorer et sauvegarder la sécurité et la survie des systèmes en réseau;

d) Travailler avec les fournisseurs pour améliorer la sécurité des produits disponibles dans le commerce.[27]

35. Si l'auteur d'une attaque peut se trouver dans un pays, lancer son attaque à partir d'un ordinateur situé dans un autre pays et causer des dommages dans un pays tiers, il est évident qu'indépendamment des risques de disparition des données, les frontières et les domaines de compétence des États suscitent des problèmes juridiques. La nécessité de faire enquête sur les crimes liés à l'informatique et de les poursuivre met en relief l'importance de l'entraide judiciaire. Or, les questions de souveraineté ne sont qu'une des catégories de problèmes qui surgissent lorsqu'il faut faire enquête ou procéder à des saisies à l'étranger. En l'absence d'entraide judiciaire appropriée, il existe le risque que les services de répression d'un État cherchent sans autorisation à rechercher des informations conservées dans des ordinateurs situés dans un autre État. Avant même d'envisager une entraide judiciaire, toutefois, il faut réfléchir à la législation nationale. Après tout, la coopération internationale suppose, en définitive, que les pays aient déjà mis en place des lois permettant de combattre la cyberdélinquance.

V. La législation nationale: condition préalable indispensable

36. Il arrive que certains types de criminalité liée à la délinquance se propagent comme des épidémies sans égard aux frontières nationales. Cependant, il arrive aussi que les éléments de la criminalité franchissent les frontières conformément à une stratégie soigneuse et préméditée visant à brouiller les cartes. Accroître la densité des technologies de l'information et de la communication pour exploiter les avantages qu'offre la société de l'information augmente simultanément la fréquence des délits liés à l'informatique au plan national. Aussi les pays ont-ils tout intérêt, pour protéger leur économie et la sécurité publique, à promulguer une législation pour combattre la cyberdélinquance.

37. Les législations nationales ont suivi un processus d'évolution qui s'est étendu sur plusieurs siècles, tandis que l'Internet n'existe que depuis quelques décennies. Certes, le droit continue de s'adapter à mesure que la société change. Face au défi représenté par la criminalité liée à l'informatique, il peut s'avérer nécessaire de moderniser les législations nationales. Sieber a recensé six principales vagues de lois adoptées dans ce domaine depuis les années 70:[28] a) des lois relatives à la protection des données et de l'intimité; b) des lois pénales visant à réprimer la délinquance économique liée à l'informatique; c) des lois relatives à la protection de la propriété intellectuelle; d) des lois tendant à éliminer les messages illégaux et préjudiciables; e) des textes de procédure pénale; et f) des réglementations concernant des mesures de sécurité comme le cryptage et les signatures numériques. [29]

38. Plusieurs éléments doivent être réunis pour pouvoir combattre la criminalité liée à l'informatique: il faut a) faire en sorte que les délits aient été dûment qualifiés par la loi; b) mettre en place des méthodes d'enquête appropriées pour combattre la cyberdélinquance; et d) mettre en oeuvre ces méthodes d'une manière qui sauvegarde les droits de l'homme et les libertés fondamentales.

A. Nature des infractions

39. Il a été établi des listes détaillées des atteintes à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques.[30] La catégorie des délits informatiques comprend également un certain nombre d'infractions liées au contenu des messages (par exemple la production et la diffusion de matériel pornographique mettant en scène des enfants ou de propagande xénophobe).

Le Bureau de supervision de la sécurité de l'information du Ministère de la sécurité publique de la Chine a fait savoir qu'en 2001, il avait été enregistré un peu moins de 5 000 délits liés à l'informatique, contre 2 900 en 2000 et 400 environ en 1999. À la mi-2002, le Bureau avait signalé un peu plus de 3 000 affaires, et il s'attendait, entre cette date et la fin de 2002, à quelque 350 cas de pénétration des systèmes et à 800 cas de dommages à des systèmes informatiques.[31] Le nombre d'affaires signalées par le Bureau augmentait très rapidement alors même que beaucoup d'affaires n'étaient certainement pas déclarées. La plupart des délinquants étaient des jeunes (de 18 à 30 ans) et la plupart des attaques étaient lancées à partir de cafés Internet, les délinquants dissimulant leurs identités en se raccordant au réseau par l'entremise d'un serveur http ou Sock ou de fausses adresses IP, ou bien en ayant recours à la cryptographie ou à la stéganographie. En conséquence, les cybercafés chinois sont désormais soumis à des conditions plus rigoureuses d'enregistrement et à une surveillance plus étroite.

40. Toute une série de questions ont surgi lorsque les pays ont essayé d'adapter des dispositions conçues pour protéger des biens matériels et ont voulu les utiliser dans le monde intangible et éphémère du numérique.

41. Il importe, au stade de la rédaction des lois, de faire preuve de prudence pour éviter d'incriminer des actes qui sont en fait légitimes. Il importe aussi, dans les efforts de modernisation du droit pénal, d'établir une distinction soigneuse entre ce qui est spécifique et ce qui est général. Il se peut en effet que des dispositions rédigées en termes spécifiques se trouvent dépassées dès qu'une technologie nouvelle est disponible. Aussi est-il conseillé d'utiliser des termes neutres du point de vue technologique.

B. Règles de procédure

42. Ces dernières années, du fait de la généralisation des archives électroniques, beaucoup de pays ont dû se pencher sur les problèmes que soulève la définition d'un "document". Même des expressions élémentaires comme le concept de "lieu" où perquisitionner peuvent juridiquement poser des problèmes lorsque les données sont diffusées par un réseau informatique (en effet, il se peut que la perquisition porte sur un ordinateur de bureau se trouvant en un lieu déterminé mais que les données soient conservées dans un ordinateur se trouvant ailleurs, même s'il est virtuellement "présent" pour l'usager et pour l'enquêteur).

43. Il est bon, lors de l'élaboration des règles de procédure, d'établir une distinction entre trois types différents d'information: a) le contenu effectif des communications électroniques; b) les données concernant le trafic; et c) les informations touchant les abonnés. S'il y a lieu d'établir une distinction entre ces trois types d'information, c'est parce qu'elles peuvent donner lieu à des atteintes différentes pour ce qui est de la protection des activités ou des données ou bien faire intervenir d'autres droits de l'homme et libertés fondamentales.

44. Juridiquement, l'une des premières difficultés tient à la définition d'expressions comme "données concernant le trafic" et "informations concernant les abonnés". La Convention sur la cybercriminalité du Conseil de l'Europe,[32] par exemple, définit les données concernant le trafic comme étant "toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'éléments de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent" (article premier). En outre, la Convention définit les informations relatives aux abonnés comme étant "toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que les données relatives au trafic ou au contenu, et permettant d'établir:

a) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b) l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné ou tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un engagement de service;

c) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service" (paragraphe 3 de l'article 18).

45. La question des définitions a été abordée dans le Manual on the prevention and control of computer-related crime[33] publié par l'Organisation des Nations Unies ainsi que dans la Décision-cadre du Conseil de l'Union européenne relative aux attaques dirigées contre les systèmes informatiques et dans les législations nationales.[34]

46. Selon le droit interne de beaucoup de pays, certains types de contenu jouissent d'une plus grande protection constitutionnelle du fait de l'existence de concepts comme la confidentialité des communications et la liberté d'expression. Ainsi, il peut s'avérer nécessaire d'établir, sur les plans du fond comme de la procédure, une distinction entre le contenu de certains types de communication sur Internet (celles qui ne sont pas publiques ni privées) et des données concernant le trafic. Il se peut également que certains éléments des données concernant le trafic et les abonnés[35] puissent, dans certains contextes, être liés aux dispositions relatives à la protection des données du fait qu'ils constituent des informations personnelles essentielles protégées par le droit à l'intimité.

47. Il y a lieu de noter que la collecte et la conservation de données risquent d'entrer en conflit avec les intérêts et les valeurs des diverses parties prenantes de sorte qu'il peut être indiqué d'essayer de concilier les différents intérêts légitimes en présence. Dans certains pays, la collecte de données est rigoureusement réglementée par les dispositions relatives à la protection de l'information, lesquelles sont parfois consacrées par la loi, dispositions selon lesquelles des données ne peuvent être collectées et utilisées qu'à des fins déterminées, que lorsque l'intéressé a donné son consentement en pleine connaissance de cause, et sous réserve d'autres mesures de sauvegarde (comme une vérification de l'intégrité de l'information, la fixation de délais pour la destruction des données et l'accès à certaines questions).[36]

48. Les techniques utilisées pour conserver les données dans des archives situées à l'étranger peuvent soulever des problèmes juridiques spécifiques dans les pays ayant des régimes différents en ce qui concerne la surveillance du contenu des messages en temps réel (comme les dispositions relatives aux tables d'écoute), par opposition aux perquisitions. Dans le contexte de la criminalité liée à l'informatique, cela risque de poser un problème dans le cas du courrier électronique, dont il se peut que le contenu ne puisse être surveillé en temps réel que pendant que le courriel est en route qu'avec autorisation, mais seulement après délivrance d'un mandat de perquisition lorsqu'il a cessé de circuler, c'est-à-dire lorsqu'il est conservé sur le serveur ou sur le disque dur du destinataire. Dans la mesure où le message transmis pas courriel est essentiellement le même dans les deux circonstances, le recours à deux mécanismes juridiques différents assortis de règles juridiques potentiellement différentes peut susciter des difficultés.

49. Il a été élaboré un certain nombre de mécanismes juridiques pour faciliter les enquêtes sur la criminalité liée à l'informatique, et il y a lieu de citer notamment les ordonnances de conservation et les ordonnances de production. Une ordonnance de conservation est rendue à la suite d'une procédure accélérée pour obliger un prestataire de services à conserver et sauvegarder des données concernant une transaction ou un client spécifique. Une telle procédure est importante lorsqu'il faut recueillir des preuves électroniques car celles-ci peuvent être éliminées ou détruites plus facilement que des documents sur papier. Essentiellement, une ordonnance de conservation est un ordre de "ne pas supprimer". Une ordonnance de conservation[37] est par sa nature même temporaire et est rendue pour permettre aux services de répression d'obtenir les données requises, par exemple au moyen d'un mandat autorisant la saisie des données et d'une ordonnance de production pour que les données soient communiquées.

50. Lorsqu'il a été prononcé une ordonnance de production, la personne ayant la garde des documents a l'obligation de les livrer aux services de répression dans les délais impartis et de les mettre à leur disposition. Les ordonnances de production sont semblables à des mandats de perquisition bien qu'en l'occurrence, ce soit le gardien des documents qui procède à la recherche plutôt que la police. Ce type d'ordonnance est moins intrusif, la personne ayant la garde des données étant souvent mieux à même de savoir où se trouvent les documents recherchés. Aujourd'hui, dans le monde des affaires, il est fréquent que les entreprises conservent leurs dossiers dans un pays autre que celui où elles opèrent afin d'économiser sur les coûts de la tenue des archives. En pareilles circonstances, un mandat de perquisition classique risque de ne pas être approprié, tandis qu'une ordonnance de production permet au propriétaire des données ou à la personne qui est a la garde de rechercher les documents et les archives demandés.

VI. La recherche de solutions par le biais de la coopération internationale

51. Dans certains cas, les législations nationales devront être adaptées à la situation nouvelle créée par la cyberdélinquance pour pouvoir répondre efficacement aux demandes d'assistance émanant d'autres États pour obtenir une assistance de ces derniers. L'harmonisation des législations peut être un objectif important en matière de lutte contre la criminalité liée à l'informatique. Pour respecter les droits souverains des États et faciliter la coopération internationale, il faut, en définitive, exploiter les possibilités offertes par des mécanismes internationaux formels comme les conventions. Si l'on veut que l'entraide judiciaire fonctionne comme il convient, la qualification des infractions et les règles de procédure des divers États doivent être compatibles.

52. La communauté internationale commence seulement à faire face aux multiples défis qui continuent de surgir dans ce domaine. Une offensive majeure lancée au moyen de centaines d'ordinateurs infectés de plusieurs pays pour paralyser les sites web d'entreprises dans un autre pays ou les dommages considérables que peut causer un virus ou un ver qui se propage partout dans le monde soulèvent des questions fondamentales concernant, par exemple, le lieu de commission de l'infraction et l'État compétent aux fins des poursuites. Une autre question d'importance capitale est de savoir si, en définitive, l'intervention dépend de l'État qui non seulement est disposé à ouvrir une enquête et à entamer des poursuites mais qui a la capacité de le faire. Il est évident que les groupes de criminels internationaux sont prêts à exploiter les échappatoires créés par les différences de systèmes juridiques et de capacité des systèmes de justice pénale. Certains peuvent y voir une érosion de la souveraineté des États, mais d'autres diront que la souveraineté est un concept en voie de transformation dans le monde depuis l'apparition des sociétés de l'information.

53. De telles situations font immédiatement penser à la question complexe de l'extradition, laquelle peut elle-même susciter différents problèmes. Par exemple, si les qualifications des infractions ne sont pas compatibles, il se peut qu'il soit impossible de satisfaire au critère de double incrimination. Simultanément, il est de plus en plus généralement admis que, lorsqu'une double incrimination est requise, ce sont les éléments constitutifs de l'infraction, ou le comportement sous-jacent, qui doivent correspondre, et pas seulement le libellé de la qualification de l'infraction dans les pays intéressés. Même si la double incrimination ne suscite pas de problèmes dans un cas spécifique, le délit dont il s'agit peut ne pas être considéré comme suffisamment sérieux (par exemple au regard des peines dont il est passible) pour justifier une extradition.

54. En dépit des difficultés, cependant, il y a lieu de citer plusieurs réalisations majeures depuis 2000, lorsque s'est réuni le dixième Congrès pour la prévention du crime et le traitement des délinquants, dont deux nouveaux instruments juridiques, la Convention relative à la cybercriminalité du Conseil de l'Europe et la Convention des Nations Unies contre la criminalité transnationale organisée, qui a une portée universelle mais qui ne traite qu'indirectement de la cyberdélinquance, lorsque celle-ci est le fait de groupes de criminels organisés.

55. Au plan international, des entités comme l'Office des Nations Unies contre la drogue et le crime (ONUDC), l'Organisation internationale de police criminelle (Interpol), l'Organisation de coopération et de développement économiques (OCDE) et le G-8, ainsi que des institutions régionales comme l'Union européenne, le Conseil de l'Europe, l'Organisation des États américains, l'Association des nations de l'Asie du Sud-Est et le Conseil de coopération économique pour l'Asie et le Pacifique (APEC) peuvent offrir des compétences politiques et techniques nécessaires pour resserrer la coopération internationale. L'on peut aujourd'hui, ce qui n'était pas le cas il y a quelques années seulement, parler d'un consensus international sur la lutte contre la cybercriminalité, surtout sous ses formes transnationales. Ainsi, il existe enfin un climat moral propice à une action concertée, que celle-ci revête la forme de mesures civiles, pénales ou administratives, coopération qui reflète ce que les sociologues appellent la "communauté d'un sort partagé".[38]

56. La Convention relative à la cybercriminalité a été ouverte à la signature le 23 novembre 2001 et a été signée par 30 États et ratifié par 8 d'entre eux. Elle peut être signée par des États extérieurs à l'Europe, et 4 États non européens (Afrique du Sud, Canada, États-Unis et Japon) l'ont déjà fait. Aux termes de la Convention, qui est entrée en vigueur le 1er juillet 2004, les États parties sont tenus d'harmoniser leurs législations nationales pour ce qui est de la qualification des infractions. Il s'agit notamment des infractions dirigées contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques, ainsi que d'infractions comme le faux et usage de faux, la fraude informatique, les infractions qui supposent une violation du droit d'auteur et les infractions liées à la pornographie mettant en scène des enfants commises au moyen d'un système informatique. En outre, la Convention contient une importante série de règles de procédure, concernant notamment les injonctions de production et de conservation, visant à faciliter les enquêtes et les poursuites dans le contexte des réseaux informatiques mondiaux. Elle contient également des dispositions tendant à établir un système rapide et efficace de coopération internationale. Enfin, le problème posé par l'incitation à la haine sur Internet a donné lieu à l'élaboration d'un Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques,[39] qui a été ouvert à la signature le 28 janvier 2003. Le Protocole additionnel a été signé par 20 États et ratifié par 2 d'entre eux.

57. En 2002, les Ministres de la justice des pays du Commonwealth ont adopté une loi type relative aux délits liés à l'informatique intitulée Computer and Computer Related Crimes Act.[40.] Cette loi type, inspirée du cadre constitué par la Convention relative à la cybercriminalité du Conseil de l'Europe, met à la disposition des services de répression des moyens efficaces et modernes de lutte contre la cyberdélinquance.

58. Depuis le huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, en 1990, l'Organisation des Nations Unies a entrepris d'étudier activement divers aspects des conséquences de la révolution informatique.[41] En 1994, l'Organisation a publié son Manual on the Prevention and Control of Computer-related

Crime,[42] grâce à une assistance technique et financière considérable du Gouvernement canadien et au concours d'un certain nombre d'experts de gouvernements d'autres pays et d'organisations non gouvernementales.

59. En 2000, lors du dixième Congrès, il s'est tenu un atelier consacré à la criminalité liée aux réseaux informatiques.[43] En 2001, le Secrétaire général a soumis à la Commission pour la prévention du crime et la justice pénale les conclusions d'une étude sur les mesures efficaces à prendre pour prévenir et réprimer les délits liés à la haute technologie et à l'informatique (E/CN.15/2001/4).

60. En 2004, à la suite de la première phase du Sommet mondial sur la société de l'information, tenu à Genève en décembre 2003, le Secrétaire général a créé un groupe de travail chargé d'étudier la gouvernance d'Internet pour examiner les questions liées au spam, à la sécurité et aux systèmes informatiques et aux utilisations faites d'Internet, en prévision de la deuxième phase du Sommet mondial, qui doit avoir lieu à Tunis en novembre 2005.

61. La criminalité liée à l'informatique est un phénomène international qui appelle une solution internationale. Pour y parvenir, la communauté internationale devra étudier attentivement les moyens dont elle dispose déjà pour resserrer la coopération internationale. Elle devra s'efforcer aussi d'approfondir ses connaissances et de mieux comprendre les différentes manifestations du phénomène, les défis que celles-ci représentent et les solutions les mieux appropriées et les plus réalistes qui peuvent être envisagées pour prévenir et combattre ce phénomène.

VII. Coopération dans les domaines de la recherche sur la criminalité liée à l'informatique

62. Réunir les données factuelles nécessaires à l'élaboration des politiques futures ne sera pas tâche facile. La recherche sur la criminalité liée à l'informatique n'en est en effet encore qu'à un stade embryonnaire. En outre, il se peut que les experts ou les institutions bien informées des secteurs aussi bien public que privé répugnent, pour des raisons commerciales ou politiques ou des considérations liées à la sécurité nationale, à partager leur savoir avec les chercheurs. Les informations du domaine public, en outre, sont souvent incomplètes et inexactes. En dépit de ces handicaps, il importe de constituer une base de connaissances si l'on veut que les efforts déployés pour rétrécir le fossé numérique commencent à être couronnés de succès.

63. Il faudra avoir recours à des méthodes de recherche et à des études comparatives très diverses pour rassembler un minimum de données sur la prévalence et la gravité des divers types de cyberdélinquance. Il faudra en outre entreprendre des recherches sur l'efficacité des nouvelles lois, des stratégies de répression et des poursuites en analysant les affaires connues et les résultats des efforts déployés. Outre que ces sources d'information gagneraient souvent à être plus spécifiques et plus uniformes, les recherches ne doivent pas se limiter aux archives de la police ou des tribunaux: elles devront en priorité porter sur le comportement des victimes et des délinquants, tout en suivant l'évolution des législations et des méthodes employées par les services de répression partout dans le monde.[44]

VIII. Coopération entre les secteurs public et privé pour la lutte contre la criminalité liée à l'informatique

64. Les gouvernements et les représentants du secteur privé sont de plus en plus conscients de la nécessité impérieuse de collaborer étroitement dans les efforts qu'ils déploient pour combattre la criminalité liée à l'informatique. Aucun gouvernement ou groupe de gouvernements, aucune entreprise ni aucun secteur industriel, à lui seul, ne peut y parvenir: il faut plutôt qu'il existe entre les secteurs public et privé un étroit partenariat caractérisé par l'ouverture et une solide communication à double sens. Les entités du secteur privé ont joué et continueront de jouer un rôle vital dans la mise au point de technologies pouvant aider à prévenir la cybercriminalité et à faire enquête sur ce type de délit. Toutefois, indépendamment des solutions technologiques, le secteur privé peut aussi beaucoup contribuer à aider les décideurs à identifier les priorités et les solutions possibles dans le domaine législatif. L'expérience a montré qu'un partenariat actif entre les pouvoirs publics et l'industrie peut améliorer l'efficacité de l'action menée par les services de répression pour poursuivre les cyberdélinquants.

65. Il est encourageant de constater que les partenariats entre les secteurs public et privé se multiplient. Les pays membres du G-8 sont conscients depuis longtemps que, pour lutter efficacement contre la cybercriminalité, une coopération sans précédent entre le gouvernement et la justice s'impose et ils ont adopté d'importantes mesures en ce sens, notamment en organisant des conférences entre les pouvoirs publics et l'industrie pour discuter des préoccupations communes et trouver des solutions possibles.[45] L'Organisation des Nations Unies, l'APEC, l'OCDE et d'autres organisations multilatérales ont elles aussi redoublé d'efforts pour associer le secteur privé à ces activités.

66. En décembre 2004, les représentants d'un certain nombre de secteurs et d'institutions internationales de répression ont annoncé la création du Digital PhishNet, opération concertée qui a permis de conjuguer les efforts des dirigeants des secteurs de la technologie, de la banque, des secteurs financiers et des maisons de vente aux enchères sur Internet ainsi que des services de répression pour s'attaquer au "phishing", forme de plus en plus répandue de vol d'identité en ligne. Le réseau Digital PhishNet offre un moyen de communication unifié entre l'industrie et les services de répression, de sorte que ces derniers puissent rassembler en temps réel des données indispensables pour combattre ce phénomène. D'autres groupes industriels se sont employés à identifier les sites web utilisés pour le phishing et à diffuser les meilleures pratiques et des informations sur les affaires découvertes, mais le réseau du système PhishNet est le premier groupe en son genre qui ait principalement pour but d'aider les services de répression à appréhender et à poursuivre les personnes ayant ainsi escroqué les consommateurs. Le réseau Digital PhishNet rassemble les dirigeants de neuf des dix plus grands établissements financiers et banques des États-Unis, quatre des cinq premiers prestataires de services Internet et cinq entreprises de commerce électronique et de technologie et collabore avec les services de répression du Gouvernement fédéral des États-Unis ainsi qu'avec les institutions internationales de police.

67. Au cours des quelques dernières années, plusieurs entités du secteur privé se sont associées à l'Université de Hong Kong pour organiser un certain nombre d'importantes conférences sur la cybercriminalité. Ces manifestations ont réuni de hautes personnalités de la magistrature et de la police de tous les pays d'Asie et du Pacifique ainsi que des universitaires réputés et des représentants d'organisations multilatérales comme l'Organisation des Nations Unies, le Conseil de l'Europe, Interpol et l'APEC. La discussion

a porté notamment sur la vulnérabilité des réseaux, les menaces qui pèsent sur le commerce électronique, comme le spam, le phishing et d'autres formes de fraude en ligne, et le piratage informatique.

68. Les services de répression du monde entier ont, ces dernières années, collaboré avec un certain nombre de sociétés de réputation mondiale pour faire enquête et poursuivre les auteurs d'escroqueries en ligne et d'autres cyberdélinquants, dont certains des "spammeurs" les plus connus.

69. En dépit des progrès réalisés, l'on pourrait faire plus pour resserrer encore la collaboration entre les pouvoirs publics et l'industrie et mieux structurer et institutionnaliser le dialogue et le partenariat entre les secteurs public et privé.

IX. Recommandations

70. Les participants voudront peut-être examiner les recommandations ci-après, formulées lors de deux réunions d'experts organisées par l'Institut coréen de criminologie de Séoul, compte tenu également des informations pertinentes des réunions régionales préparatoires du onzième Congrès:

a) Il est indispensable d'adopter une approche large et inclusive pour lutter contre les problèmes liés à la cybercriminalité en allant au-delà du droit pénal, des procédures pénales et de l'action des services de répression. L'accent devra être mis sur les conditions qui doivent être remplies de sorte qu'une cyberéconomie puisse fonctionner en sécurité et optimiser ainsi la confiance des milieux d'affaires et l'intimité des particuliers, ainsi que sur les stratégies tendant à promouvoir et à protéger l'innovation et le potentiel de création de richesse et des possibilités offertes par les technologies de l'information et de la communication, notamment en mettant en place des mécanismes d'alerte rapide et d'intervention en cas d'attaques dirigées contre des réseaux informatiques. Indépendamment de la nécessité de prévenir et de réprimer la criminalité liée à l'informatique, il faut, d'une façon plus générale, créer une culture mondiale de cybersécurité tenant compte des besoins de toutes les sociétés, y compris les pays en développement, dont les structures informatiques sont nouvelles et encore vulnérables;

b) Il faudrait s'attacher à resserrer encore plus la coopération internationale à tous les niveaux. Du fait de son universalité, le système des Nations Unies, doté des mécanismes renforcés de coordination interne demandés par l'Assemblée générale, devrait jouer un rôle de premier plan dans les activités entreprises au plan intergouvernemental pour garantir le bon fonctionnement et la protection du cyberespace de sorte que celui-ci ne fasse pas l'objet d'abus et soit exploité par des criminels ou des terroristes. En particulier, le système des Nations Unies devrait continuer à promouvoir l'application d'approches mondiales de la lutte contre la cybercriminalité et de la coopération internationale en vue d'éviter et d'atténuer l'impact négatif de la criminalité liée à l'informatique sur l'infrastructure critique, le développement durable, la protection de l'intimité, le commerce électronique, les opérations bancaires et le commerce;

c) Tous les États devraient être encouragés à actualiser leurs législations pénales dès que possible afin de pouvoir tenir compte plus efficacement des spécificités de la cybercriminalité. S'agissant des formes classiques de délits commis grâce à l'utilisation de nouvelles technologies, cette nouvelle dimension des lois devra tendre à préciser ou à abolir les dispositions qui ne sont plus totalement adaptées, comme les lois qui ne peuvent

pas réprimer la destruction ou le vol de biens intangibles, ou à créer de nouvelles dispositions pour faire face à de nouvelles formes de criminalité, comme l'accès non autorisé à des ordinateurs ou à des réseaux informatiques. Les États devraient également s'employer à moderniser leurs règles de procédure (par exemple pour remonter la trace des communications) ainsi que les lois, accords ou arrangements relatifs à l'entraide judiciaire (par exemple pour garantir rapidement la préservation des données). Les États devraient être encouragés, lorsqu'ils entreprennent d'élaborer de nouvelles lois, à s'inspirer des dispositions de la Convention relative à cybercriminalité du Conseil de l'Europe;

d) Les gouvernements, le secteur privé et les organisations non gouvernementales devraient collaborer afin de rétrécir le fossé numérique, de susciter une prise de conscience accrue des risques représentés par la cybercriminalité et d'introduire des contre-mesures appropriées et de mettre les professionnels de la justice pénale, y compris le personnel des services de répression, les services du parquet et les magistrats, mieux à même de combattre ce phénomène. À cette fin, les administrations judiciaires nationales et les facultés de droit devraient incorporer à leurs programmes d'enseignement des matières traitant en détail de la criminalité liée à l'informatique;

e) Le onzième Congrès devrait faire porter toute son attention sur la nécessité d'établir des mécanismes visant à promouvoir l'échange d'informations au plan international, l'alerte rapide, l'intervention policière et la limitation des dommages (par le biais d'Interpol, des mécanismes d'alerte 24/7 du G-8, de la Convention relative à la cybercriminalité, de Computer Emergency Response Teams (CERT) et du Forum of Incident Response and Security Teams (FIRST)), qui demeurent limités à certains pays, surtout développés, ainsi que d'améliorer et élargir la gamme de ceux qui existent déjà. Ces mécanismes devraient pouvoir être utilisés par tous les États afin de faciliter le partage des connaissances et de l'information sur les méthodes permettant de détecter, de prévenir, d'éviter et de réprimer les nouveaux types de cyberdélinquance ainsi que d'informer le public des mécanismes d'intervention qui ont été mis en place. En outre, l'on devrait s'attacher particulièrement à mettre ces mécanismes à la disposition des pays en développement en leur offrant une formation dans ce domaine;

f) Les politiques élaborées pour lutter contre la cybercriminalité devraient être fondées sur des informations factuelles et par des évaluations rigoureuses afin d'en maximiser l'efficience et l'efficacité. Des efforts concertés et coordonnés devraient par conséquent être déployés au plan international afin d'établir des mécanismes de financement de manière à faciliter les recherches appliquées et à pouvoir faire face ainsi à d'innombrables types nouveaux de cyberdélinquance. Néanmoins, il importe tout autant de veiller à ce que les recherches soient coordonnées au plan international et à ce que leurs résultats soient largement diffusés;

g) L'ONUDC devrait porter les résultats de l'atelier sur les mesures de lutte contre la criminalité liée à l'informatique qui a eu lieu à l'occasion du onzième Congrès à l'attention de la deuxième phase du Sommet mondial sur la société de l'information qui doit avoir lieu à Tunis en 2005.

Notes

[1] D.B. Parker, S. Nycum et S.S. Oüra, *Computer Abuse* (Menlo Park, Californie, Standford Research Institute, 1973).

[2] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, Ministère de la justice des États-Unis, 1979).

[3] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, Ministère de la justice des États-Unis, 1989).

[4] Russel G. Smith, Peter N. Grabosky et Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

[5] Conseil de l'Europe, *Série des Traités européens*, 1985.

[6] Dans certains pays, où des personnes qui utilisent Internet chez elles ont adopté des réseaux locaux sans fil, des réseaux locaux non sécurisés ont été utilisés pour obtenir un accès à Internet sans autorisation à différentes fins. C'est ce que l'on appelle souvent les "opérations offensives", l'auteur de tels actes se déplaçant dans son automobile avec son ordinateur portable pour identifier des points d'accès et se connecter ainsi à Internet.

[7] Dans certains pays, le concept de "vol" s'applique uniquement aux biens tangibles et est défini comme étant le fait de soustraire de tels liens à une personne. Ce concept n'englobe donc pas le vol d'un bien intangible et ne s'appliquerait pas au fait de copier sans autorisation un dossier numérique. Dans certains pays, de tels actes ne sont pas passibles de sanctions pénales mais relèvent plutôt du droit civil, et notamment des dispositions relatives aux droits d'auteur.

[8] Le progiciel poste-à-poste BitTorrent de Bram Cohen est de plus en plus largement utilisé pour échanger des dossiers numériques volumineux à des fins légitimes (comme la distribution de logiciels libres, de jeux informatiques ou de programmes de télévision) mais aussi pour le piratage de bandes vidéo. Pour un aperçu de cette dernière question, voir Clive Thompson, The BiTorrent Effect". *Wired*, 13 janvier 2005, et Jeff Howe "The Shadow Internet", *Wired*, 13 janvier 2005.

[9] *IC3 2003 Internet Fraud Report*: *January 1, 2003-December 31, 2003* (National White Collar Crime Center et Federal Bureau of Investigation des États-Unis).

[10] Voir Michael D. Mehta, Don Best et Nancy Poon. "Peer-to-peer sharing on the Internet: An Analysis of how Gnutella networks are used to distribute pornographic material". *Canadian Journal of Law and Technology*, Vol. 1, No. 1 (janvier 2002); et États-Unis d'Amérique, General Accounting Office. *File Sharing Programs: Peer-to-peer Networks Provide Ready Access to Child Pornography*. GAO-03-351 (Washington, février 2003).

[11] Dick Thornburgh et Herbert S. Lin (eds.), *Youth, Pornography and the Internet* (Washington, National Academy Press, 2003).

[12] Pour un aperçu des lois adoptées par 24 pays pour combattre les messages de caractère raciste, xénophobe et antisémite, voir le document à ce sujet examiné lors de la Conférence sur ll'antisémitisme tenue à Berlin les 28 et 29 avril 2004 sous l'égide de l'Organisation pour la sécurité et la coopération en Europe (CIO.GAL/25/04/Rev.1),.

[13] Scott Berinato, "The truth about cyberterrorism", *CIO Magazine*, 15 mars2002.

[14] En ce qui concerne les produits disponibles dans le commerce qui utilisent la cryptographie quantique pour le cryptage de données sur les systèmes à fibres optiques ou les réseaux sans fil, voir Gary Stix, "Best-kept secrets", *Scientific American* (janvier 2005).

[15] Pour une analyse des aspects des Objectifs du Millénaire pour le développement concernant les technologies de l'information et de la communication, voir Union internationale des télécommunications, *Rapport sur le développement des télécommunications dans le monde 2003: Indicateurs d'accès pour la société de l'information*, septième édition (2003). Cette étude contient une évaluation intéressante des OMD dans le contexte des technologies de l'information et de la communication; le nouvel Indicateur d'accès numérique (IAN) semble particulièrement prometteur.

[16] China Internet Network Information Center (CNNIC), *quinzième rapport statistique sur le développement d'Internet en Chine (janvier 2005)* (www.cnnic.net.cn) (adresse consultée le 25 janvier 2005).

[17] Internet Systems Consortium (http://www.isc.org).

[18] Tiré de: Union internationale des télécommunications, *Base de données des indicateurs des télécommunications mondiales*, huitième édition (2004).

[19] *Étude sur la situation économique et sociale dans le monde 2000* (publication des Nations Unies, numéro de vente: F.00.II.C.1).

[20] Pour une analyse statistique de la complexité du fossé numérique, voir le cadre conceptuel proposé par Georges Sciadas (eds.), *Monitoring the Digital Divide ... and Beyond* (2003).

[21] Il y a lieu de noter que, paradoxalement, de telles circonstances recréent à un niveau différent un fossé numérique précisément lorsque celui-ci est sur le point d'être comblé et peuvent saper la confiance des milieux d'affaires locaux ou compromettre l'attrait des premiers investissements.

[22] La principale différence entre un système anonyme et un système pseudonyme est que ce dernier préserve une identité (un alias) pendant une certaine période (et qu'il peut par conséquent y avoir un lien plus solide entre l'identité pseudonyme, l'identité de l'abonné et l'identité réelle). Un service anonyme, sous sa forme la plus pure, est essentiellement un service utilisé pour une seule communication ou une seule transaction. Il y a divers types de services anonymes et pseudonymes, dont la plupart offrent des serveurs directs ou différents moyens combinés pour accéder à un ou plusieurs services Internet usuels, comme serveurs utilisés pour faire suivre le courriel, sa navigation sur le web, IRC ou newsgroups de l'Usenet. Il y a également divers degrés d'anonymité et de pseudonymité selon non seulement des facteurs comme le progiciel sous-jacent de cryptage et d'authentification mais aussi la nature et la sécurité du serveur ou du réseau de serveurs qui garantissent l'anonymat, les procédures de création d'un pseudonyme et, dans le cas de services payants, le mécanisme de facturation.

[23] David H. Crosker, rev., *Standard for the Format of ARPA Internet Text Messages*, RFC 822 (13 août 1982).

[24] L'atelier sur la conservation des données qui a eu lieu lors du Dialogue entre les pouvoirs publics et l'industrie concernant la sécurité des systèmes informatiques et la confidentialité dans le cyberespace qui a eu lieu à Berlin dans le contexte du G-8 en octobre 2000, les participants ont identifié les éléments de coûts ci-après: volume des données à conserver; recherche des données existantes; ingénierie et développement; dépenses administratives et opérationnelles et coûts de formation; protection de la sécurité et de l'intimité; responsabilité concernant la gestion des données et leur remise aux services de répression; et dépenses liées au coût d'opportunité et à la confiance des consommateurs.

[25] Les prestataires de services peuvent conserver les données pendant des périodes de durée diverse, selon le modèle opérationnel, les services et les technologies dont il s'agit. Certaines données sont conservées à des fins de facturation et d'autres pour la vérification des performances des systèmes. La durée de conservation varie de quelques secondes à des périodes plus longues, selon ce qu'imposent ou autorisent les législations nationales à des fins autres que l'action policière. Différents types de données sur le trafic sont également conservées pendant des périodes de durée diverse; par exemple, les registres d'accès au réseau (RADIUS ou Terminal Access Controller Access Control System (TACACS+)) sont soumis, en ce qui concerne l'administration et le stockage des données, à des exigences différentes de celles qui s'appliquent aux registres NNTP et de ce fait, peuvent parfois être disponibles plus longtemps. Habituellement, le contenu des messages n'est ni conservé, ni disponible.

[26] *Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations* (http://canada.justice.gc.ca/en/news/g8/doc2.html).

[27] Voir *CERT Coordination Center, 2003 Annual Report* (www.cert.org) et Forum of Incident Response and Security Teams (www.first.org).

[28] Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study* (1er janvier 1998).

[29] Le modèle de Sieber, c'est-à-dire les six vagues de législations nationales, a été appliqué au cas de l'Australie dans: Russel G. Smith, Peter N. Grabosky et Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

[30] Organisation de développement et de coopération économiques, *Criminalité liée à l'informatique: analyse des politiques législatives*, série ICCP No. 10 (1986). Voir également la recommandation No. R (89) 9 adoptée par le Comité des ministres du Conseil de l'Europe le 13 septembre 1989.

[31] Rapport présenté par la Chine à l'occasion de la Conférence sur la cyberdélinquance et la sécurité de l'information en Asie et dans le Pacifique organisée à Séoul du 11 au 13 novembre 2002 par la Commission économique et sociale pour l'Asie et le Pacifique et le Ministère de l'information et de la communication de la République de Corée. Le nombre de délinquants est sans doute important si l'on considère que dans un quartier de Beijing (district de Haidian), il a été arrêté entre 2001 et mai 2004 52 suspects, dont 48,4% d'entre eux pour avoir pénétré les systèmes informatiques.

[32] Conseil de l'Europe, *Série des Traités européens*, No. 185.

[33] *Revue internationale de politique pénale*, No. 43 et 44 (publication des Nations Unies, numéro de vente: F.94.IV.5).

[34] La loi britannique de 2000 portant réglementation des pouvoirs d'enquête contient au paragraphe 9 de son article 2 une définition des données concernant le trafic, bien que celle-ci englobe également les informations relatives aux abonnés. L'on trouve également une approximation conceptuelle des données sur le trafic dans les définitions que les États-Unis ont élaborées des expressions "pen register" et "trap and trace device" (Code des États-Unis, Titre 18, article 3127), qui ont été actualisées par la loi de 2001 relative à la lutte contre le terrorisme (Loi PATRIOT).

[35] En ce qui concerne les informations sur les abonnés, il peut exister déjà dans certains pays une réglementation dans le domaine de la téléphonie (informations sur les clients, et notamment sur leurs noms et leurs adresses).

[36] Entre autres instruments internationaux pertinents, l'on peut notamment citer la Convention pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel conclue sous l'égide du Conseil de l'Europe (Conseil de l'Europe, *Série des Traités*, No. 108) ou les Lignes directrices de l'OCDE régissant la protection de l'intimité et les échanges transfrontières de données à caractère personnel (OCDE, 1980). Ces instruments ont eu pour but d'établir des principes selon lesquels les informations à caractère personnel doivent être obtenues en respectant les garanties établies par la loi; ne doivent être utilisées qu'aux fins initialement spécifiées; doivent être adéquates, pertinentes et ne pas dépasser celles qui sont nécessaires auxdites fins; doivent être exactes et à jour; doivent pouvoir être obtenues par l'intéressé; doivent être tenues confidentielles; et doivent être détruites après que leur utilité a disparu. La nature de cette obligation a été renforcée dans certains pays, par exemple par les Directives du Parlement européen et du Conseil de l'Union européenne relatives à la protection des données (Directive 95/46/CE et Directive 97/66/CE). Après la promulgation de ces directives, beaucoup de pays d'Europe ont promulgué des lois plus rigoureuses en matière de protection des données afin d'honorer les obligations juridiques que leur imposaient les Directives. En dehors de l'Europe, il existe également des instruments comportant des dispositions semblables relatives à la protection de données à caractère personnel, comme la Loi canadienne relative à la protection des informations à caractère personnel et au transfert des documents électroniques.

[37] Il y a lieu de noter que les ordonnances de préservation des données ont pour but de garantir que les informations spécifiées concernant un abonné déterminé ne soient pas supprimées. En revanche, la "conservation des données" est un concept de caractère général visant à obliger tous les prestataires de services Internet à rassembler et à conserver une série de données concernant tous leurs abonnés.

[38] Roderic Broadhurst, "Content crimes: criminality and censorship in Asia", paper presented at Octopus Interface: the Challenge of Cybercrime", Strasbourg, 15-17 septembre 2004.

[39] Conseil de l'Europe, *Série des Traités européens*, No. 189.

[40] La loi type peut être consultée sur le site web de la Division des affaires juridiques et des affaires constitutionnelles du Secrétariat du Commonwealth (http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf).

[41] À l'occasion du huitième Congrès, il a été organisé un atelier sur l'informatisation de l'administration de la justice pénale (A/CONF. 144/14). Dès 1992, l'Organisation a publié un "*Guide for Computerization of Criminal Justice Information Systems*" (publication des Nations Unies, numéro de vente: E. 92.XVII.6). Lors du neuvième Congrès, en 1995, il s'est tenu un atelier sur la coopération et l'assistance internationales en ce qui concerne la gestion des systèmes de justice pénale: informatisation des opérations de la justice pénale et collecte, analyse et utilisation aux fins de la formulation des politiques d'informations sur la justice pénale (A/CONF.169/13) (voir également: Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient, *The Global Challenge of High-Tech Crime: Workshop on Crimes Related to the Computer Networks; dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, 15 avril 2000, Vienne, Autriche* (Tokyo, avril 2001).

[42] *Revue internationale de politique pénale*, No. 43 et 44 (publication des Nations Unies, numéro de vente: F.94.IV.5).

[43] Voir le document de travail établi pour l'atelier sur la criminalité liée aux réseaux informatiques (A/CONF.187/10).

[44] Peter Grabosky et Roderic Broadhurst 2005, "The Future of Cyber-crime in Asia", *Cybercrime: the Challenge in Asia*, Roderic Broadhurst et Peter Grabosky (eds.) (Hong Kong University Press, 2005) p. 347-360.

[45] Voir "G-8 Berlin Meeting: Government/Industry Dialogue on Safety and Confidence in Cyberspace (Summary and Assessment)" (disponible à l'adresse http://194.25.60.123/www/de/aussenpolitik/friedenspolitik/g8/cyberspace/documents/paris-l); et Kuriko Miyake, "G8 concludes Tokyo high-tech crime meeting (disponible à l'adresse http://archives.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg).

———————