Nations Unies E/CN.15/2001/4

Conseil économique et social

Distr.: Générale
30 mars 2001

Français
Original: Anglais

Commission pour la prévention du crime et la justice pénale
Dixième session
Vienne, 8-17 mai 2001
Point 4 de l'ordre du jour provisoire*
Coopération internationale en matière de lutte contre la criminalité transnationale

Conclusions de l'étude sur les mesures efficaces à prendre pour prévenir les délits liés à la technologie et à l'informatique et lutter contre ces délits

Rapport du Secrétaire général

Résumé

Le présent rapport répond en partie à la demande adressée au Secrétaire général par le Conseil économique et social dans sa résolution 1999/23 du 28 juillet 1999, tendant à entreprendre une étude sur les mesures efficaces qui pourraient être prises aux niveaux national et international pour prévenir les délits informatiques et lutter contre eux. Il contient un examen préliminaire de la question et recommande qu'une étude plus détaillée soit, à titre prioritaire, réalisée et présentée à la Commission pour la prévention du crime et la justice pénale à sa onzième session, pour que celle-ci l'examine. Le rapport recommande en outre que la Commission, à sa onzième session, envisage une série d'options concernant des mesures complémentaires, dont l'élaboration éventuelle d'un instrument international contre les délits informatiques, ainsi qu'une stratégie à plus court terme, notamment la mise en place d'un programme mondial des Nations Unies contre les délits liés à la technologie et à l'informatique. Il fournit également des renseignements sur les activités d'autres organisations internationales et intergouvernementales compétentes et tente de répondre à certaines des préoccupations exprimées par différents États Membres.

* E/CN.15/2001/1.

V.01-82400 (F) 230401 230401

Table des matières

I. Introduction

1. Le problème posé par les activités criminelles faisant intervenir les technologies modernes (informatique et télématique) reste un important défi pour les services de justice pénale et de répression des États Membres. Ce défi peut être envisagé sous différents angles, ainsi qu'il est indiqué ci-après:

a) Il s'agit d'un défi de portée mondiale. La plupart des utilisateurs des technologies modernes et, partant, des délinquants et de leurs victimes se trouvaient naguère dans les pays développés. L'élargissement des possibilités d'accès à ces technologies dans les pays en développement est considéré comme prioritaire pour que la société de l'information planétaire devienne un facteur propice au développement plutôt qu'un obstacle supplémentaire[1]. Les pays en développement seront à la merci de la cybercriminalité et de la délinquance informatique et risquent d'être exclus de l'accès aux réseaux informatiques et télématiques du fait des technologies appliquées en matière de prévention du crime ou de sécurité s'ils ne peuvent pas participer à l'élaboration et à la mise en œuvre de politiques de lutte contre la criminalité.

b) Il s'agit d'un défi dynamique. Le développement rapide des technologies nouvelles s'accompagne d'un développement tout aussi rapide des innovations de nature criminelle: du même coup le caractère planétaire de ces technologies entraîne une prolifération de nouvelles formes de délinquance. Il s'avère donc essentiel de contrôler tant le développement légitime de la technologie que les innovations de nature délictueuse en vue d'actualiser les modes d'intervention aux niveaux national et international, notamment dans les pays où les moyens techniques sont limités. Un tel processus, découlant principalement du développement technologique, est de nature évolutive.

c) Le défi à relever est également multi-disciplinaire. Le développement de la technologie des réseaux informatiques et télématiques sous-tend une importante évolution, les activités sociales et économiques qui supposent un effort physique et l'exploitation de produits de base cédant progressivement la place à des activités reposant sur l'information pure ou le savoir. Cela n'est pas sans conséquences dans des domaines tels que la protection des droits de l'homme et le développement social et économique durable. Il importe au plus haut point d'intégrer le contrôle du crime dans ces domaines d'activité, et vice versa. Les technologies de l'information et l'architecture des réseaux informatiques et télématiques sont en grande partie les produits du développement du secteur privé: en mettant au point des mesures de lutte contre les délits liés à la technologie et à l'informatique, il faut donc tenir compte de facteurs tels que la viabilité commerciale et la compétitivité économique des technologies en cause.

II. Généralités

A. Travaux d'autres organisations intergouvernementales ou internationales

2. La préoccupation croissante des États devant la nature et la portée du problème considéré, tout comme la nécessité de prendre des mesures efficaces de portée mondiale pour y remédier, sont attestées par le nombre d'instances dans le cadre desquelles cette question a été examinée.

1. Conseil de l'Europe

3. Le Conseil de l'Europe est en passe d'achever l'élaboration du texte d'une convention sur la cybercriminalité[2] qui portera sur les infractions suivantes: atteinte à l'intégrité des systèmes, accès non autorisé, fraude et falsification électroniques, infractions se rapportant au contenu et infractions liées aux atteintes à la propriété intellectuelle. Ce projet de texte traite des pouvoirs d'investigation, tels que la localisation des communications ainsi que la recherche, la saisie et la préservation d'éléments de preuve sous forme électronique. Il définit également des termes de base et établit des normes pour l'entraide judiciaire et d'autres formes de coopération internationale. Une fois qu'il aura été effectivement mis au point, ce projet de convention représentera la première initiative visant à mettre en place un instrument international global contre la délinquance informatique. Dans sa dernière version, le texte a été diversement accueilli. Les pouvoirs publics, les experts et les services de répression le considèrent dans l'ensemble comme une initiative positive, même si nombreux sont ceux qui

pensent que certains des enjeux les plus complexes n'ont pas été abordés. Bon nombre de groupes d'intérêts sont d'avis que les réseaux internationaux ne devraient pas être réglementés et reprochent à ce texte de tenter d'étendre les pouvoirs de répression au niveau intérieur aux dépens de la vie privée individuelle et d'autres intérêts.

4. Les négociations sur le texte de l'instrument ont été menées par un Comité d'experts sur la criminalité dans le cyberespace, créé en février 1997, à la suite de plusieurs études sur cette question[3]. En sus des membres du Comité, des experts du Canada, des États-Unis d'Amérique et du Japon ont été invités à participer à ses travaux et d'autres États se sont joints au processus durant les négociations. Le Comité a produit 25 projets de texte successifs au cours de son mandat, qui a pris fin en décembre 2000. Le texte final a été soumis à l'Assemblée parlementaire du Conseil de l'Europe. Il sera ensuite présenté au Comité européen pour les problèmes criminels pour être examiné en juin 2001 et, s'il est approuvé, sera alors transmis au Comité des ministres du Conseil de l'Europe pour adoption.

2. Le G-8

5. Après avoir examiné les problèmes découlant de la criminalité transnationale à leur réunion au sommet tenue à Halifax (Canada) en juin 1995, les sept pays les plus industrialisés et la Fédération de Russie ont créé un groupe d'experts de haut niveau sur la criminalité transnationale organisée (dit Groupe de Lyon), qui comprenait un sous-groupe d'experts de la criminalité informatique. Ce sous-groupe, qui s'est réuni périodiquement depuis 1997, est à l'origine de diverses initiatives. Parmi les sujets de préoccupation examinés, il convient de mentionner les problèmes posés par les perquisitions transfrontières sous forme électronique, la localisation des communications et la nécessité d'une coopération entre les pouvoirs publics et les intérêts pertinents du secteur privé.

6. En décembre 1997, le G-8 a adopté un plan d'action en 10 points sur la cybercriminalité, prévoyant notamment les éléments ci-après: étude de la législation, mesures permettant de disposer de responsables de l'application des lois dûment formés et équipés, prise en considération des aspects liés à la cybercriminalité dans la négociation d'accords d'entraide judiciaire, examen de méthodes permettant de préserver les éléments de preuve électroniques et de les communiquer en cas de poursuites pénales engagées à l'étranger, amélioration de la coopération avec les milieux professionnels, normes de la police scientifique et autres normes techniques en matière de sécurité informatique et utilisation de moyens de preuve électroniques dans les procédures juridiques[4].

7. En 1999, le G-8 a adopté des principes préliminaires de base à l'intention des services de répression désireux d'accéder aux données électroniques stockées dans des États étrangers[5]. Il a été décidé, de manière générale, que les données pouvaient être consultées librement si elles étaient dans le domaine public, comme c'est le cas, par exemple, d'un site Web ouvert à tous ou si une personne dûment autorisée à accéder aux données et à les divulguer a donné son consentement. Dans le cas de données qui ne sont pas dans le domaine public, les responsables de la perquisition sont confrontés à un dilemme. S'ils ne copient pas les données rapidement, les délinquants vont généralement effacer celles-ci. S'ils les copient sans demander auparavant l'autorisation de l'État dans lequel se trouvent ces données, de graves problèmes se posent alors touchant la souveraineté de l'État en question et la protection des droits des personnes dont les intérêts sont mis en cause par les données saisies. Les principes convenus par le G-8 prévoient la présentation d'une demande d'entraide judiciaire accélérée. L'État dans lequel se trouvent les données serait invité à prendre immédiatement des dispositions pour préserver celles-ci en attendant l'octroi d'une aide de caractère plus officiel en vue d'en assurer la saisie et la divulgation à l'État requérant. Les données seraient ensuite transférées à l'État requérant en faisant appel aux procédures et clauses de sauvegarde classiques en matière d'entraide judiciaire.

8. Des principes fondamentaux applicables à la localisation des communications sur les réseaux informatiques sont également envisagés. La plupart des fournisseurs de services conservent des enregistrements électroniques de la source et de la destination de communications telles que les messages électroniques, mais seulement pendant un certain temps. Dans un grand nombre de pays, seules les opérations de recherche et de saisie approuvées par l'appareil judiciaire permettent d'accéder aux fichiers susceptibles d'être utilisés pour repérer des communications et identifier les utilisateurs de systèmes en cause. Cela ne représente pas un obstacle

majeur s'agissant de la plupart des communications intérieures, mais dans les affaires transnationales, les délais sont plus longs en raison de la nécessité de présenter des demandes suivant les circuits de l'entraide judiciaire. Ce problème est connu des cyberdélinquants les plus ingénieux, qui l'exploitent à leur avantage en faisant passer leurs communications par différents pays entre le lieu d'origine et le lieu de destination, ou en les acheminant via des pays dépourvus des lois ou des infrastructures nécessaires pour localiser de telles communications, ce qui permet d'en dissimuler l'origine ou la destination véritable.

9. Pour faciliter et accélérer la coopération entre les services de répression dans les affaires transnationales, le Groupe de Lyon a recommandé la mise en place d'un réseau de points de contact installés dans chaque État, susceptibles d'être appelés 24 heures sur 24 et 7 jours sur 7, pour fournir une aide compétente aux fins d'enquête. Ce réseau, qui se composait initialement des États membres du G-8, a été élargi et comprend désormais 19 pays: la responsabilité des opérations a été confiée à l'Organisation internationale de police criminelle (Interpol).

10. Pour rapprocher les intérêts des pouvoirs publics et ceux du secteur privé, le G-8 a organisé plusieurs conférences sur la coopération avec la profession[6]. En général, les représentants des milieux professionnels comprennent des entreprises qui mettent au point du matériel, du logiciel et d'autres éléments d'infrastructure dans les secteurs de l'informatique et des télécommunications, et des sociétés de services s'adressant à différents utilisateurs. Les échanges de vues ont porté sur différentes questions, qu'il s'agisse de la volonté et de la capacité des entreprises de coopérer avec les services de répression ou de la nécessité de prévenir la criminalité en sensibilisant les clients et en incorporant des éléments de sécurité dans les nouvelles technologies en cours d'élaboration.

3. Autres organisations internationales ou intergouvernementales

11. La question des délits liés à la technologie et à l'informatique a également été traitée par d'autres organisations intergouvernementales et internationales, à la fois en tant que thème distinct et en vue d'autres objectifs liés à la délinquance, tels que la lutte contre le blanchiment d'argent et la criminalité transnationale organisée. Le Commonwealth a commencé à examiner ces problèmes en 1998, en inscrivant la question à l'ordre du jour d'une réunion des ministres de la justice du Commonwealth en mai 1999. À cette réunion, il a été décidé de créer un groupe de travail composé d'experts des délits liés à l'informatique pour élaborer une loi type à l'intention des pays du Commonwealth, mais ce projet a été mis en veilleuse en attendant la conclusion de la Convention du Conseil de l'Europe sur la cybercriminalité. Les travaux ont repris en juillet 2000 et un projet de loi type est en cours d'élaboration. Le Commonwealth a également entrepris de diffuser auprès de ses États membres des documents sur les faits nouveaux survenus au niveau international et d'examiner les dispositifs disponibles dans les pays du Commonwealth concernant les délinquants en fuite et l'entraide judiciaire, l'objectif étant de veiller à ce que ces dispositifs prévoient les formes de coopération nécessaires dans le nouveau domaine de la délinquance liée à la technologie.

12. Interpol a également entrepris des activités, en créant divers groupes de travail régionaux sur la délinquance informatique. Les recherches réalisées et les documents produits par cette organisation répondent généralement aux besoins et aux préoccupations des services de répression. Parmi les documents destinés à la formation des enquêteurs, il convient de mentionner un guide s'adressant aux novices et un manuel plus élaboré sur la cybercriminalité qui présente aux enquêteurs plus chevronnés des pratiques et des techniques optimales. Interpol a également conscience de la nécessité de recourir aux médias les plus modernes pour diffuser des informations auprès des services de répression et met actuellement en place un site Web à cet effet. L'organisation a assumé la responsabilité de la mise à jour d'un annuaire du réseau de points de contact initialement mis en place par le Groupe de Lyon. Interpol prévoit d'autres activités, notamment dans le domaine de la formation des responsables de l'application des lois, et entend suivre les activités d'autres organisations internationales ou y participer pour partager des informations et éviter les chevauchements d'activités.

B. Activités de l'Organisation des Nations Unies

13. La question des délits liés à l'informatique et aux technologies des télécommunications a été examinée

dans le cadre des activités de l'Organisation des Nations Unies et continue d'être suivie activement. Outre la présente étude, menée conformément à la résolution 1999/23 du Conseil économique et social en date du 28 juillet 1999[7], les mesures suivantes ont été prises:

a) Dans la résolution 45/109 de l'Assemblée générale en date du 14 décembre 1990 et dans la résolution 1996/11 du Conseil économique et social en date du 23 juillet 1996, les États Membres ont été instamment priés d'utiliser des techniques informatiques modernes pour gérer de manière plus efficace le fonctionnement de la justice pénale et les systèmes d'information sur la justice pénale. Le huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, qui s'est tenu à La Havane du 27 août au 7 septembre 1990, a recommandé la mise au point d'un instrument international concernant l'informatisation des systèmes de justice pénale[8]. Un atelier de deux jours s'est penché sur cette question durant le neuvième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, qui s'est tenu au Caire du 29 avril au 8 mai 1995. L'atelier a noté que l'information était nécessaire pour suivre le rythme des formes nouvelles de criminalité en soulignant toutefois que des préoccupations avaient été exprimées au sujet de la protection de la vie privée, du respect des droits de l'homme et de la compatibilité opérationnelle des systèmes, dans les pays et parmi eux. Il a également fait observer qu'il fallait assurer une assistance technique sous forme de ressources financières et de compétences spécialisées[9]. De manière générale, l'accent a été mis sur l'utilisation des ordinateurs dans l'administration de la justice pénale et dans la collecte des données statistiques plutôt que sur le recours aux réseaux informatiques en tant qu'instruments d'enquête ou outils opérationnels. Plus récemment, des dispositions visant à accroître l'utilisation des technologies modernes dans la lutte contre la criminalité ont été incorporées dans la Convention des Nations Unies contre la criminalité transnationale organisée[10], et la distribution électronique des documents a joué un rôle important dans le processus de négociation;

b) Le huitième Congrès a en outre examiné le problème de la criminalité informatique en tant que telle[11], et a recommandé une série de mesures visant à:

i) Actualiser les dispositions nationales concernant les infractions, l'instruction, les règles de preuve, la confiscation, la restitution, l'entraide judiciaire et l'extradition, afin de pouvoir les appliquer aux délits informatiques;

ii) Améliorer la sécurité des ordinateurs et adopter d'autres mesures pour prévenir la criminalité;

iii) Sensibiliser le public et former les agents chargés de l'instruction, des poursuites et du jugement dans le cadre des délits informatiques;

iv) Élaborer et diffuser des principes déontologiques concernant l'utilisation des systèmes informatiques;

v) Définir des politiques en faveur des victimes de délits informatiques, notamment des mesures visant à encourager les victimes à porter plainte;

c) Comme l'a recommandé le huitième Congrès dans sa neuvième résolution, le *Manuel des Nations Unies pour la prévention et la répression de la criminalité informatique* a été publié en 1994[12] à l'intention des enquêteurs et des décideurs et il a été largement diffusé sur Internet;

d) La question des délits informatique a été également inscrite à l'ordre du jour du dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, qui s'est tenu à Vienne du 10 au 17 avril 2000. Durant le Congrès, un atelier d'un jour a été organisé à ce sujet par l'Institut pour la prévention du crime et le traitement des délinquants en Asie en Extrême-Orient[13]. L'atelier a tenu quatre tables rondes portant sur les thèmes suivants: criminologie des délits informatiques; problèmes associés à la perquisition et à la saisie de données dans des réseaux informatiques; problèmes liés à la localisation des communications sur les réseaux informatiques; et relation entre la répression d'une part et l'industrie des ordinateurs et Internet d'autre part. D'éminents spécialistes ont donné des informations aux participants sur les questions en cours et sur l'évolution des débats au sein du Conseil de l'Europe, du Groupe des huit et d'autres instances. Outre les représentants des États participants, plusieurs représentants du secteur industriel ont participé à l'atelier. Ce dernier a fait des recommandations,

notamment pour que s'exerce une plus grande collaboration entre les gouvernements et le secteur industriel, pour que la coopération internationale dans la localisation des délinquants soit améliorée et pour que l'Organisation des Nations Unies intensifie son action en matière de coopération et d'assistance techniques[14];

e) La Déclaration de Vienne sur la criminalité et la justice: relever les défis du XXI[e] siècle, adoptée par le dixième Congrès[15] et approuvée par l'Assemblée générale dans sa résolution 55/59 du 4 décembre 2000, a également abordé les délits technologiques et informatiques. Au paragraphe 18 de la Déclaration de Vienne, les États Membres ont décidé d'élaborer des recommandations concrètes sur la prévention et la répression des délits informatiques et se sont engagés à œuvrer au renforcement des moyens dont ils disposent pour prévenir ces délits, enquêter à leur sujet et en poursuivre les auteurs. Ils ont invité la Commission pour la prévention du crime et la justice pénale à entreprendre l'élaboration de ces recommandations en tenant compte des travaux en cours dans d'autres instances. Dans sa résolution 55/60 du 4 décembre 2000, l'Assemblée générale a ensuite demandé à la Commission de continuer à examiner les conclusions et recommandations figurant dans la Déclaration de Vienne et le rapport du dixième Congrès et a demandé au Secrétaire général de préparer, en consultation avec les États Membres, des projets de plans d'action afin que la Commission les examine lors de sa dixième session;

f) Outre sa contribution aux préparatifs de l'atelier sur les délits liés aux réseaux informatiques tenu durant le dixième Congrès, l'Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient a organisé une série de réunions et d'ateliers destinés à recenser les problèmes et à fixer un calendrier pour les activités à entreprendre. L'Institut a mené une enquête sur les questions liées aux délits informatiques dans les États Membres, dont les résultats doivent paraître prochainement. Il s'emploie actuellement à compiler et publier la documentation utilisée par l'Organisation des Nations Unies et par les participants à l'atelier organisé durant le dixième Congrès. Il se propose d'élaborer et de diffuser des données pratiques pour les enquêtes et les poursuites relatives aux délits informatiques;

g) À sa dixième session, la Commission sera saisie d'un rapport du Secrétaire général sur les projets de plans d'action destinés à la mise en œuvre de la Déclaration de Vienne sur la criminalité et la justice: relever les défis du XXI[e] siècle (E/CN.15/2001/5). Le rapport du Secrétaire général aborde également les délits technologiques et informatiques et comprend une série de recommandations concrètes et de mesures spécifiques qui pourraient être appliquées en vue de renforcer les moyens disponibles aux plans local et international pour prévenir ces délits, enquêter à leur sujet et en poursuivre les auteurs. Ces recommandations et mesures sont fondées sur les données contenues dans le présent rapport;

h) Dans sa résolution 55/63 du 4 décembre 2000, l'Assemblée générale a pris note de l'utilité des efforts déployés pour lutter contre l'exploitation des technologies de l'information à des fins criminelles: notamment élimination des paradis fiscaux; coopération des services de répression dans le cadre d'affaires d'ampleur internationale; échange d'informations; formation et équipement du personnel; protection de la confidentialité; préservation des données relatives aux enquêtes pénales et accès rapide à ces informations; application de régimes appropriés d'entraide judiciaire; sensibilisation du public; création de systèmes d'information pour prévenir les délits et faciliter les enquêtes; et prise en compte de la nécessité de protéger les libertés individuelles et la vie privée tout en préservant la capacité des pouvoirs publics de lutter contre l'exploitation des technologies de l'information à des fins criminelles. L'Assemblée générale a également décidé de garder la question de l'exploitation des technologies de l'information à des fins criminelles à l'ordre du jour de sa cinquante-sixième session;

i) Par sa résolution 55/25 du 15 novembre 2000, l'Assemblée générale a adopté la Convention des Nations Unies contre la criminalité transnationale organisée et deux protocoles s'y rapportant (résolution 55/25, annexes I à III). La Convention ne s'applique pas lorsqu'il ne s'agit pas d'infractions graves, lorsqu'il n'est pas question de groupe criminel organisé ou lorsqu'il n'y a aucun élément de nature transnationale dans l'infraction en question[16], ce qui tend à exclure certains délits informatiques. La Convention devrait s'appliquer en revanche lorsque des réseaux informatiques ou de télécommunication

sont utilisés par des délinquants à l'appui de formes plus traditionnelles de criminalité transnationale organisée. Le paragraphe 1 h) de l'article 29 préconise l'élaboration de mesures nationales et la fourniture d'une assistance technique pour combattre la criminalité transnationale organisée perpétrée au moyen d'ordinateurs et de réseaux de télécommunication ou d'autres techniques modernes;

j) Suite à l'adoption de la Convention, un nouvel atelier intitulé "Le défi de la cybercriminalité sans frontières" a été organisé en marge du Colloque sur l'état de droit dans le village planétaire: souveraineté et universalité, qui s'est inscrit dans le cadre de la Conférence de signature par des personnalités politiques de haut rang, de la Convention des Nations Unies contre la criminalité transnationale organisée et des protocoles qui s'y rapportent, tenue à Palerme, en Italie, du 12 au 15 décembre 2000. Parmi les questions abordées figuraient les délits informatiques et d'autres formes de criminalité transnationale dont la répression fondée exclusivement sur le droit interne était jugée insuffisante. On a noté que ces délits se propageaient parallèlement à l'expansion des technologies sur lesquelles ils s'appuyaient, tirant parti du fait qu'il était désormais plus facile de commettre des infractions transfrontières. On a estimé que la législation nationale et un instrument international global étaient des éléments importants de la solution à apporter au problème, mais des préoccupations ont par ailleurs été exprimées face au danger que présentait l'élaboration prématurée de règlements. On a fait valoir que le problème pourrait aussi trouver une solution partielle moyennant l'application, à titre de prévention, de mesures telles que la sécurité technique, l'éducation et l'élaboration de normes déontologiques aux fins de l'utilisation des nouvelles technologies. L'atelier a en outre proposé de classer les cyberdélits en quelques grandes catégories, à savoir: accès non autorisé aux ordinateurs ou aux systèmes informatiques; suppression ou altération de données; entrave à l'utilisation légale d'ordinateurs ou de systèmes informatiques; vol de biens incorporels et recours à des manœuvres frauduleuses pour obtenir un avantage.

C. Nature des délits technologiques et informatiques: typologie préliminaire

14. Le phénomène des délits technologiques et informatiques nécessite de définir des infractions totalement nouvelles et de modifier la définition d'infractions établies de façon à ce qu'elle englobe les utilisations impropres des nouvelles technologies. De nouveaux types de comportements préjudiciables ont dû être étudiés afin de déterminer s'il était approprié, pour s'y attaquer, d'appliquer la législation pénale et s'il fallait même les ériger en infractions. Un consensus se dégage au niveau international sur un ensemble de comportements jugés les plus graves et les plus préjudiciables, mais certains actes ne sont pas encore considérés comme des infractions par tous les États. Les deux principaux exemples en sont les problèmes liés à la propriété intellectuelle, notamment copie non autorisée de logiciel ou de données, et question du contenu qualifié d'offensant.

15. L'utilisation délictueuse des nouvelles technologies a donné naissance à des formes totalement inédites de criminalité. D'autre part, les auteurs d'infractions plus classiques emploient de nouveaux moyens qui leur permettent d'obtenir plus d'avantages ou de réduire les risques auxquels ils s'exposent. Une troisième grande catégorie d'activités délictueuses renvoie aux délinquants qui recourent plus généralement aux technologies pour organiser leurs activités et les soustraire à la surveillance et pour communiquer. Les principaux autres modes de classification proposés reposent notamment sur les critères suivants: les infractions sont-elles commises en vue de l'obtention d'un gain pécuniaire ou matériel, ou pour d'autres motifs, ou encore ont-elles pour cible des systèmes informatiques ou de communication, ou l'utilisation de ces technologies pour victimiser des tiers.

16. Les principaux types de délits technologiques et informatiques sont décrits ci-dessous.

1. Délits commis à l'encontre des technologies et de leurs utilisateurs

a) Accès non autorisé à des ordinateurs ou des systèmes informatiques

17. Dans la plupart des cas, l'accès non autorisé à des ordinateurs ou des systèmes informatiques est considéré comme une infraction, en ce sens qu'il porte atteinte à la vie privée des utilisateurs légitimes dont les données ont pu être consultées, et parce que, souvent, il accompagne d'autres infractions ou entrave l'utilisation légitime du système.

b) Utilisation non autorisée de systèmes informatiques

18. L'utilisation non autorisée de systèmes informatiques et l'accès non autorisé se recoupent, l'accès non autorisé impliquant qu'il faut utiliser les systèmes. Cela étant, une fois qu'il a accédé au système, le délinquant l'utilise également pour commettre d'autres infractions ou pour dissimuler sa véritable identité. L'utilisation non autorisée est généralement incriminée au motif que l'utilisation de temps machine ou d'équipements représente un bien d'une certaine valeur, qui n'est pas rémunérée par le délinquant tandis qu'elle est parfois refusée à des utilisateurs payants légitimes.

c) Lecture, copie ou appropriation de données sans autorisation

19. Comme dans le cas d'un vol classique, le préjudice causé par la lecture, la copie ou l'appropriation de données sans autorisation réside dans la perte subie par la victime et le gain abusif réalisé par le délinquant. S'agissant de données, toutefois, ces deux aspects sont dissociés puisqu'il est possible de copier des données sans les soustraire. Ce type d'acte peut également être érigé en infraction en tant qu'atteinte à la vie privée.

d) Création ou diffusion de programmes hostiles

20. Les virus, vers et autres programmes informatiques hostiles perturbent le fonctionnement des systèmes en en réduisant la capacité de traitement et de stockage. Qui plus est, dans la plupart des cas, ils se propagent par l'intermédiaire du courrier électronique ou de disquettes contaminées, de telle sorte que leurs auteurs perdent rapidement tout contrôle sur l'ampleur des dégâts causés une fois les programmes en circulation. De nombreux programmes hostiles endommagent en outre les données puisqu'ils effacent ou modifient des fichiers. Le préjudice peut être considérable: impossibilité de faire fonctionner le système, perte de données et coût lié à la suppression des programmes hostiles et à la remise en marche du système.

e) Vandalisme ou sabotage informatique

21. Les délinquants qui ont obtenu, intentionnellement ou non, un accès non autorisé, peuvent endommager directement le système en essayant soit de l'utiliser soit de dissimuler le fait qu'ils s'y sont introduits. Parfois, ces infractions sont aussi le fait de personnes bénéficiant d'un accès autorisé au système. Cette catégorie d'infractions comprend les attaques par déni de service, qui consistent à obtenir un accès non autorisé à un grand nombre d'ordinateurs en réseau et à les utiliser pour bombarder le système cible de données aléatoires afin de le surcharger et de le mettre hors service. Il peut s'agir soit de vandalisme pur et simple, soit d'une diversion visant à dissimuler d'autres infractions en mettant hors d'état de marche les mécanismes techniques de sécurité. Les programmes hostiles tels que les virus peuvent également servir à commettre certains actes de vandalisme et de sabotage, mais ils se distinguent de l'acte commis directement par le délinquant en ce sens que, lorsqu'ils commencent à se propager, ils frappent généralement sans discrimination.

2. Infractions classiques commises à l'aide de l'informatique ou des technologies de la communication

a) Infractions constituées par des contenus offensants

22. Les infractions constituées par des contenus offensants consistent à utiliser des systèmes informatiques pour produire ou diffuser des images, du texte ou d'autres informations passibles de sanctions pénales. Les types de contenus en cause diffèrent selon les États. Actuellement, la production ou la diffusion d'œuvres pornographiques mettant en scène des enfants

constitue une infraction dans la plupart des États, mais les notions d'obscénité, de pornographie, de blasphème ou d'incitation à la haine ne font pas l'objet du même consensus. Les droits fondamentaux inscrits dans la constitution, notamment la liberté d'expression ou de parole, limitent, pour beaucoup d'États, la mesure dans laquelle ils peuvent incriminer certains types de contenus.

b) Enlèvements organisés grâce à Internet

23. Des délinquants pédophiles ont commencé à utiliser Internet pour se mettre en rapport avec des enfants sans révéler leur véritable identité. Ils entament un dialogue par le biais d'un forum de discussion électronique et, une fois la confiance établie, ils fixent un rendez-vous à leur victime, qu'ils enlèvent. Un certain nombre de délinquants ont été arrêtés par des agents des services de répression se faisant passer pour des enfants sur Internet. Dans certains cas, les délinquants persuadent leurs victimes d'effacer les fichiers contenant leurs conversations afin de dissimuler les preuves de l'enlèvement.

c) Fraude

24. Appartiennent à cette catégorie la plupart des infractions portant sur le transfert électronique frauduleux de fonds et la communication de fausses informations aux utilisateurs des technologies afin de les dépouiller de fonds ou de biens. Ces infractions peuvent être commises par des personnes ayant accès au système (employés, par exemple) ou par d'autres personnes qui obtiennent un accès non autorisé à des systèmes privés ou entrent de fausses informations dans des systèmes publics. Les fraudes et autres délits économiques devraient sensiblement augmenter à mesure que le commerce électronique se développe. Dans ce domaine, le recours aux technologies pour manipuler les marchés financiers pose de plus en plus de problèmes.

d) Espionnage commercial ou industriel

25. Le fait que les entreprises dépendent de plus en plus des systèmes informatiques pour produire et transférer des informations en fait les cibles de l'espionnage industriel. Ce type d'espionnage est possible depuis l'extérieur, en obtenant un accès non autorisé, ou depuis l'intérieur de l'entreprise, en recourant à l'informatique pour réunir des informations précieuses et les envoyer aux concurrents sans être repéré.

e) Délits liés à la propriété intellectuelle

26. La capacité qu'offrent les nouvelles technologies de stocker, de transmettre et de copier des informations fait de la copie et de l'utilisation non autorisées un sujet de préoccupation majeur. Cependant, ces actes ne constituent pas une infraction pénale dans tous les États. Pour certains, il s'agit d'une affaire civile entre les parties directement concernées.

f) Jeu

27. La mise en place de l'infrastructure nécessaire au commerce électronique à petite échelle a également rendu possible le jeu sur Internet. La législation pénale s'applique lorsque des sites se trouvant sur des territoires où le jeu est licite sont utilisés par des joueurs depuis des territoires où il ne l'est pas. Sans entrer dans des considérations morales, le jeu est souvent réglementé de façon à générer des recettes fiscales, à s'assurer que les organisations criminelles en sont exclues et à protéger les joueurs des tricheries. Depuis peu, le jeu sur Internet est également perçu comme un moyen de blanchir de l'argent.

g) Blanchiment de l'argent

28. Le développement progressif du commerce électronique et d'autres activités commerciales faisant appel aux réseaux informatiques devrait offrir de nombreuses possibilités de blanchiment d'argent. En règle générale, les technologies permettent aux délinquants de dissimuler leur véritable identité et le lieu où ils se trouvent, d'exploiter les différences entre législations en utilisant des comptes à l'étranger ou en opérant sur plusieurs territoires, et de dissimuler la véritable nature de leurs transactions grâce à des techniques telles que le chiffrement. Dans certains cas, d'autres infractions comme le jeu ou la fraude peuvent y être associées[17].

3. Utilisation de l'informatique pour commettre d'autres activités délictueuses

29. En règle générale, les réseaux informatiques et de télécommunication modernes et les autres technologies de ce type présentent les mêmes avantages pour les organisations criminelles que pour les entreprises

légitimes, à savoir qu'ils permettent, notamment, des communications mondiales rapides, fiables et peu onéreuses qui, dans la plupart des cas, sont plus sûres que les modes de communication plus traditionnels quant aux possibilités d'interception et de surveillance depuis l'extérieur. La nature des réseaux, la rapidité accrue des communications et les gros volumes de données qui circulent rendent l'interception de communications individuelles nécessairement plus difficile pour les services de répression. Les produits spécialement conçus à des fins de sécurité, comme les barrières de sécurité et les logiciels de chiffrement, protègent les communications frauduleuses des interceptions ou intrusions tout aussi efficacement que les communications légitimes. Parfois, les réseaux sont aussi utilisés à l'appui d'organisations criminelles d'un type entièrement nouveau. L'exemple le plus souvent cité est celui des délinquants pédophiles, qui sont en mesure de se localiser et d'échanger entre eux de la pornographie enfantine tout en restant anonymes, et qui peuvent coopérer selon des modalités qui ne correspondent pas aux concepts ou aux définitions actuels de la criminalité organisée. Ces technologies offrent également aux organisations criminelles plus classiques de nouvelles possibilités d'identifier des délinquants d'autres régions ou pays et de coopérer avec eux.

D. Évaluation de l'ampleur et du coût des délits technologiques et informatiques

30. À mesure que les réseaux informatiques et de télécommunications se sont étendus et perfectionnés, la dépendance à leur égard et le nombre d'utilisateurs ont progressé de façon spectaculaire. Dans un rapport à l'Assemblée du Millénaire des Nations Unies, le Secrétaire général a fait observer qu'Internet, lancé au début des années 90 comptait, en 1998, 143 millions d'utilisateurs et qu'en 2001, 700 millions de personnes seraient connectées. Le commerce électronique, phénomène plus récent, avait dégagé au total 2,6 milliards de dollars des États-Unis en 1996, chiffre qui devrait atteindre 300 milliards de dollars d'ici 2002[18]. Les statistiques complètes sur les délits technologiques ou informatiques sont rares mais celles dont on dispose laissent penser, avec d'autres données empiriques, que ce type de criminalité prend de l'ampleur à mesure que le nombre de délinquants et de victimes potentiels reliés à Internet augmente[19]. Il semble par ailleurs que l'éventail des activités délictueuses s'élargisse à mesure que les technologies ouvrent de nouvelles voies aux délinquants et que ces derniers trouvent de nouvelles façons de les exploiter. Actuellement, l'expansion rapide du commerce électronique et de l'infrastructure qui le sous-tend est particulièrement inquiétante, parce qu'elle risque d'être suivie d'une augmentation des délits économiques commis à l'aide de l'informatique comme la fraude, la manipulation des marchés financiers et le blanchiment de l'argent.

31. Le préjudice susceptible d'être causé par des infractions pénales croît en proportion de la dépendance par rapport aux réseaux. La plupart des pays industrialisés, où cette dépendance est la plus grande, considèrent maintenant les réseaux informatiques et de télécommunications, ainsi que leurs infrastructures, comme des cibles potentielles du terrorisme. Les attaques de systèmes informatiques pour des motifs stratégiques ou politiques demeurent rares, mais des actes délictueux perpétrés pour d'autres motifs occasionnent régulièrement des préjudices importants, parfois sans commune mesure avec ceux que leurs auteurs avaient prévus. Ainsi, la création et la diffusion, en mars 1999, du virus "Melissa" a causé plus de 10 millions de dommages directs pour les seuls États-Unis d'Amérique, tandis qu'en mai 2000, le virus "I love you" aurait causé de 7 à 10 milliards de dollars de dommages et infecté pas moins de 45 millions d'ordinateurs dans le monde entier. À la suite de cela, lors d'une série d'attaques par déni de service, des sites Internet ont été bombardés par de gros volumes de données inutiles, ce qui a entraîné en moins de deux heures la fermeture de 1 200 d'entre eux, dont des sites d'agences de presse et des sites consacrés au commerce électronique. Les pertes occasionnées par certains incidents, en particulier liés à des virus, s'accumulent dans la plupart des cas, lorsque d'autres délinquants copient le programme, le modifient de façon à ce que les utilisateurs ou le logiciel de filtrage n'en reconnaissent pas la nature, et le remettent en circulation[20].

32. Les pertes réelles sont difficiles à quantifier, mais elles englobent les frais directs de remise en état des systèmes et des logiciels, les dommages qui résultent de l'accès ou des services refusés aux usagers, la perte de données précieuses et le manque à gagner sur les recettes normalement générées par le site. Ce type d'infraction impose d'élaborer et d'appliquer des

mesures de sécurité et autres mesures préventives, dont le coût vient s'ajouter au reste. Le développement général de cette forme de criminalité et le caractère spectaculaire de certaines infractions créent par ailleurs une pression politique forte mais imprévisible en faveur de contrôles renforcés, de peines plus sévères et de précautions techniques de la part des fabricants de logiciels et de matériel ainsi que des fournisseurs d'accès à Internet. Ces incidents ont en outre un coût caché: la crainte de la cybercriminalité, qui risque de freiner l'utilisation des technologies concernées ou de dissuader les gouvernements et les populations des pays en développement d'en tirer le meilleur parti.

33. Il est également difficile de trouver des analyses fiables de la nature et de l'ampleur des infractions elles-mêmes. Quant à savoir s'il faut incriminer certains comportements et, dans l'affirmative, comment il faut les définir et les classer, la question n'est pas résolue. Tout système de classification dépend en partie des technologies visées, ce qui pose en même temps des problèmes de définition. Les réseaux informatiques, systèmes de diffusion par câble, réseaux téléphoniques cellulaires ou classiques et autres technologies deviennent rapidement indissociables les uns des autres à mesure que l'usage des réseaux informatiques se généralise et que des systèmes plus traditionnels adoptent les techniques numériques. Ainsi, actuellement, les ordinateurs de poche combinent des services de téléphonie cellulaire, de réseaux de diffusion et d'accès aux réseaux informatiques. Les chercheurs, analystes des politiques et législateurs auront donc fort à faire dans les années à venir, et des appels ont été lancés pour que l'on recoure à des notions et une terminologie technologiquement neutres afin d'éviter les vides et les incohérences.

34. La collecte de statistiques précises présente également des problèmes, même lorsque les infractions sont clairement identifiées. La plupart des spécialistes estiment que, souvent, les délits informatiques les plus courants ne sont pas signalés, soit parce que les victimes ne se rendent pas compte qu'elles ont été prises pour cible, soit parce qu'elles ignorent que le comportement en question constitue une infraction, soit encore parce qu'elles choisissent de ne pas porter plainte car elles se trouvent dans une situation embarrassante ou craignent pour la crédibilité de l'entreprise. D'autres problèmes sont liés au fait que des infractions telles que la diffusion de virus font un tel nombre de victimes qu'il est impossible de les identifier et de les dénombrer, et que ce type de programme peut continuer à faire de nouvelles victimes longtemps après que son auteur a été arrêté et puni. La collecte et la comparaison de statistiques nationales relatives à la criminalité sont encore compliquées du fait que, par définition, les délits informatiques transnationaux sont commis ou ont des incidences dans au moins deux États et, souvent, dans un grand nombre d'États, d'où le risque de plaintes multiples ou d'absence totale de plaintes.

III. Conclusions et recommandations: élaboration de mesures mondiales visant à prévenir et à combattre les délits technologiques et informatiques

A. Nécessité de considérer les délits technologiques et informatiques comme un sujet distinct

35. Les activités criminelles dont il est question dans le présent rapport ont toutes trait aux technologies et possèdent de nombreuses caractéristiques communes. Certaines sont nouvelles, créées et définies par les technologies, d'autres sont des formes de criminalité plus traditionnelles qui ont été fortement influencées par ces mêmes technologies. Beaucoup de problèmes essentiels auxquels sont confrontés les gouvernements, notamment trouver un équilibre judicieux entre droits fondamentaux et pouvoirs d'enquête et intérêts nationaux et internationaux, se posent pour toutes les formes de délits technologiques et informatiques. Plus concrètement, les problèmes que rencontrent les enquêteurs et les magistrats du parquet en ce qui concerne notamment la localisation et l'identification des délinquants et la saisie, la conservation, l'authentification et l'utilisation des données informatiques ou électroniques en tant qu'éléments de preuve devant les tribunaux, sont sensiblement les mêmes, quelle que soit la nature des délits. Il est donc recommandé de considérer ce domaine comme un sujet distinct pour la recherche et lors des débats multilatéraux à venir. Cela étant, il convient de remarquer que de nombreux nouveaux domaines de préoccupation, notamment la diffusion de documents pornographiques mettant en scène des enfants, la

fraude et autres délits financiers, exigeront également l'intervention de spécialistes connaissant bien les délinquants impliqués ainsi que les méthodes particulières auxquelles ils ont recours.

B. Nécessité d'aider les pays en développement

36. Jusqu'à présent, le débat d'orientation consacré aux systèmes informatiques et aux délits informatiques a eu lieu principalement dans et entre les pays disposant de secteurs de haute technologie développés. Ces pays ont des intérêts substantiels qui pourraient être compromis par les délits informatiques. Leurs secteurs public et privé ont investi massivement dans les technologies et leur population est de plus en plus tributaire des réseaux informatiques. Cela étant, les pays en développement ont également des intérêts en jeu. Les nouvelles technologies représentent une occasion importante de faire progresser ces pays, notamment dans les domaines économique et social[21], mais elles peuvent également accroître les disparités existantes s'ils ne sont pas à même d'en profiter pleinement. En l'occurrence, s'ils ne prennent pas une part active aux discussions, les délits informatiques, de même que les efforts déployés par les pays développés et les industries de pointe pour combattre ce type de criminalité, risquent de faire obstacle au développement. Leur participation est nécessaire afin de définir précisément leurs intérêts et d'exprimer clairement leurs besoins en matière d'assistance technique et autres lors des différentes étapes du processus, de mettre au point des mesures de prévention et de répression de la criminalité applicables dans tous les pays et d'en assurer la mise en œuvre intégrale et efficace.

37. Du fait que des personnes peuvent exploiter les nouvelles technologies à des fins criminelles sans être inquiétées par les contraintes qu'imposent aux délinquants traditionnels les frontières nationales, des mesures efficaces de répression doivent être appliquées quasiment à l'échelon planétaire. Alors que les délinquants traditionnels sont limités par des facteurs comme la distance géographique, les contrôles aux frontières et l'accès physique aux victimes, les cyberdélinquants peuvent agir à distance et en toute impunité à partir d'un État, ou dans un État, qui ne dispose pas d'une législation appropriée, ou qui n'a pas la volonté ou la possibilité de la faire appliquer. Une large représentation et une participation effective seront essentielles pour faire en sorte que les stratégies et les mesures prises soient applicables dans tous les pays, et que tous les pays soient capables et désireux de les appliquer efficacement.

38. Afin de garantir une participation effective, l'aide des pays développés s'impose à différentes étapes du processus. Dans un premier temps, la participation des pays en développement sera nécessaire pour évaluer leurs intérêts dans le domaine technologique pour déterminer comment ces intérêts pouvaient être affectés par les délits informatiques et les mesures visant à les réprimer. Une aide à ce stade est donc essentielle. Certains pays utilisent activement les technologies depuis quelque temps déjà, mais pour beaucoup, elles sont encore méconnues et les questions techniques, juridiques et stratégiques qui risquent de se poser n'ont pas vraiment retenu l'attention. L'acquisition de connaissances spécialisées prend du temps, même lorsqu'on bénéficie d'une aide. Il est par conséquent important d'octroyer cette aide aussi rapidement que possible et pendant une période suffisante pour garantir une participation active tout au long des discussions. À plus long terme, une assistance technique suivie sera également nécessaire afin d'assurer l'efficacité des opérations. Étant donné l'évolution constante des technologies et des délits qui y sont associés, une stratégie mondiale s'impose pour suivre l'évolution de la situation, trouver des solutions efficaces, et les diffuser assez rapidement afin que les services de répression et les magistrats du parquet soient tenus informés des agissements des délinquants et puissent éventuellement les devancer.

39. Il est par conséquent recommandé de prendre des mesures immédiates afin d'évaluer les besoins d'assistance technique des pays en développement qui sont demandeurs et d'y répondre aussi rapidement que possible. L'évaluation doit être réalisée dans le cadre des stratégies de développement électronique de ces pays et compte tenu de l'utilisation croissante, au niveau mondial, des technologies, de l'informatique et des télécommunications, et de la prévention de la criminalité. Elle doit se faire également en consultation avec les entreprises du secteur privé concernées, si possible avec leur assistance. Globalement, elle s'attachera en particulier à recenser les technologies clefs et à définir les priorités.

C. Nécessité d'envisager des mesures aux plans international et national ainsi qu'au niveau du secteur privé

40. Les spécialistes s'accordent généralement pour reconnaître que le caractère international des technologies modernes dans le domaine de l'informatique et des télécommunications a donné naissance à de nouvelles formes de criminalité transnationale et multinationale. Le concept de cyberespace et la facilité avec laquelle les actes délictueux commis dans une aire géographique donnée peuvent avoir des répercussions dans une autre rendent primordiale la coordination des mesures nationales et internationales. Sans cette coordination, les mesures de lutte contre la criminalité pourraient s'avérer inefficaces et avoir des conséquences regrettables et fortuites, notamment dissuader des populations d'utiliser les nouvelles technologies, porter atteinte aux droits fondamentaux ou créer des disparités dans le domaine de la compétitivité et du développement industriels.

41. Étant donné le rôle majeur joué par les entreprises dans l'élaboration et l'application des technologies, la coordination des mesures s'impose également au niveau du secteur public et du secteur privé. Le secteur privé est en général favorable à la prise de mesures efficaces pour combattre la criminalité, mais ses motivations, commerciales plutôt que politiques, et les méthodes qu'il utilise, de nature technique plutôt que juridique, doivent être harmonisées et si possible coordonnées avec les efforts des gouvernements aux plans national et international.

D. Rôle du système des Nations Unies

42. En prévision de l'Assemblée du Millénaire des Nations Unies, le Conseil économique et social a été prié d'examiner le rôle des technologies de l'information dans le domaine du développement et de la coopération internationale. Il a conclu que le développement et la diffusion des nouvelles technologies de l'information étaient un processus largement autonome mais que l'Organisation des Nations Unies pouvait apporter une assistance de diverses façons[22]. Elle pourrait notamment aider les pays en développement d'une part à s'adapter aux mutations technologiques, en particulier dans les régions et domaines où les progrès induits par le marché ne sont pas à même de répondre à leurs besoins, et d'autre part à mettre au point des technologies spécifiques qui pourraient s'avérer bénéfiques sur le plan social, sans être nécessairement viables du point de vue commercial. De façon plus générale, le Conseil a conclu que le rôle crucial du système des Nations Unies était de s'attacher à bâtir entre tous les intéressés, notamment les gouvernements, les établissements universitaires et les entreprises du secteur privé, un consensus et des partenariats. Le but du consensus était de rassembler les compétences et ressources nécessaires afin d'assurer l'accès de tous aux nouvelles technologies de l'information et leur donner l'occasion de tirer parti des possibilités offertes.

43. Les délits technologiques et informatiques représentent un obstacle majeur à l'accès à ce que le Conseil a appelé l'économie mondiale fondée sur le savoir et aux avantages qui y sont associés; il est donc tout aussi important de parvenir à un consensus dans la lutte contre la criminalité. Les États qui dépendent fortement des technologies et ont beaucoup investi dans ce domaine s'accordent en général pour reconnaître la nécessité d'adopter des mesures efficaces de lutte contre la criminalité, mais il ne s'agit là que d'un début. L'élaboration de telles mesures exigera d'évoluer et de concilier de nombreux éléments aux plans économique, social, culturel et juridique. Pour être efficaces, l'élaboration et l'application d'un grand nombre de mesures de lutte contre la criminalité devront s'appuyer sur un consensus quasi universel et sur des capacités techniques adéquates dans presque tous les pays. Le consensus devrait s'étendre non seulement aux pays et à leurs gouvernements, mais aussi aux grands acteurs multinationaux du secteur privé.

44. Dans l'immédiat, il est important de rassembler et de diffuser des informations précises sur la nature et l'ampleur du problème, et sur l'avis des États Membres quant aux mesures à prendre dans ce domaine, afin que les États puissent étudier différentes options et orienter l'action du système des Nations Unies. Les organisations intergouvernementales dont il est question dans le présent rapport, ainsi que certains gouvernements, ont déjà commencé à partager avec d'autres États leurs connaissances en matière de législation, poursuites, techniques et répression, tant en ce qui concerne les infractions transnationales que dans

un contexte plus général. Ce processus devrait être étoffé, moyennant l'élargissement de son champ d'application et l'augmentation du nombre de pays participant, mais pour ce faire, il conviendra d'évaluer avec précision les besoins et les ressources disponibles pour y répondre.

45. Il est donc recommandé que le Centre pour la prévention internationale du crime de l'Office pour le contrôle des drogues et la prévention du crime du Secrétariat soit chargé d'effectuer une étude plus détaillée du problème, qui sera présentée à la Commission pour la prévention du crime et la justice pénale à sa onzième session. Les thèmes susceptibles d'y être abordés seront examinés ci-après, mais l'étude devrait au moins faire le point des besoins essentiels des États Membres, de leur volonté d'apporter une aide par la fourniture de moyens financiers et d'expertise technique et de leur opinion quant à l'action à mener au plan mondial et à la forme qu'elle devrait prendre.

46. Il est également recommandé de créer un groupe intergouvernemental d'experts à composition non limitée afin d'analyser les résultats de l'étude et élaborer des solutions ainsi que des recommandations pour examen et suite à donner par la Commission à sa onzième session. Comme indiqué précédemment, il est important que l'ensemble des pays participent à toutes les étapes du processus. Le groupe doit être aussi diversifié que possible et s'adjoindre la participation de représentants des pays en développement. C'est pourquoi il est recommandé que cette participation soit financée, autant que possible, par des contributions volontaires d'autres États.

47. Il est en outre recommandé qu'un programme mondial contre les délits technologiques et informatiques soit créé une fois l'étude terminée et l'avis du groupe d'experts connu, et que les États intéressés fournissent des contributions volontaires afin de mettre au point et d'appuyer ce programme. Cette recommandation est analysée en détail dans la section F ci-après.

48. À plus long terme, de nombreux experts estiment que seul un instrument juridique général de lutte contre les délits technologiques et informatiques à l'échelon mondial permettra de mettre en place les stratégies, pouvoirs, procédures et mécanismes de coopération internationale voulus pour combattre efficacement la criminalité informatique transnationale. Quant au délai nécessaire à l'élaboration d'un tel instrument, les avis sont partagés. Comme précisé dans la section B ci-dessus, la participation d'un plus grand nombre de pays s'impose dans les premières phases du processus. Des questions importantes doivent être résolues lors de l'élaboration d'un tel instrument, concernant notamment la souveraineté nationale, l'application de garanties judiciaires et autres garanties liées aux droits fondamentaux, ainsi que le rôle des acteurs du secteur privé dans la mise au point des mesures visant à promouvoir la sécurité informatique et à lutter contre la criminalité. Ces questions doivent être prises en considération, tant lors de l'élaboration de l'instrument que lors du choix de sa forme et de son contenu. En général, un instrument assorti de dispositions plus étendues à caractère exécutoire est plus efficace mais requiert des négociations plus longues et est plus difficile et plus long à mettre en œuvre dans beaucoup d'États. Il n'est pour l'heure pas possible de tirer des conclusions, mais il est recommandé de demander au groupe d'experts d'étudier les modalités d'ordre procédural et technique qui pourraient être adoptées pour élaborer un instrument international et de formuler des recommandations dans son rapport qui sera présenté à la Commission à sa onzième session.

49. Les délits technologiques et informatiques semblent également prendre rapidement de l'ampleur, tant en ce qui concerne leur fréquence et leur étendue géographique que leur complexité technique, et cette tendance devrait se poursuivre, parallèlement à l'évolution et à la prolifération rapides de nouveaux ordinateurs, réseaux et moyens de télécommunication. Dans un tel contexte, un instrument juridique international représente une importante solution à long terme, mais dans l'immédiat, des mesures efficaces pourraient être également nécessaires. Il est donc recommandé de demander aussi au groupe d'experts de mettre au point d'autres solutions en vue d'une stratégie mondiale à court terme de lutte contre les délits technologiques et informatiques, axées par exemple sur l'assistance juridique et technique, générale ou spécifique; l'élaboration de normes techniques pour la collecte, la conservation, l'authentification et la divulgation de preuves électroniques; la mise en place d'agents de coordination ou la création de points de contact pour les demandes d'assistance. À cet égard, il convient de prendre en compte les travaux en cours dans les instances décrites dans la section II (sous-section A) du présent rapport.

E. Les éléments d'une étude détaillée

50. Dans l'état actuel des connaissances, le domaine de la criminalité informatique soulève encore beaucoup plus de questions qu'il n'apporte de réponses et des études plus approfondies sont nécessaires pour en définir la teneur, déterminer les intérêts lésés et la manière dont ils sont lésés et recenser les grandes options à envisager à l'avenir. Pour le moins, l'étude devrait prendre en compte ce qui suit:

a) Les vues des États concernant la nature et l'ampleur du problème et les solutions envisageables aux plans national et international;

b) Les vues des États affichant une grande diversité sur le plan industriel, juridique, social et économique;

c) Les infractions de caractère à la fois national et transnational. Si de nombreux États peuvent estimer que certaines questions ont un caractère essentiellement national, il ne faut pas oublier que la nature même des technologies fait disparaître les distinctions traditionnelles entre criminalité nationale et criminalité transnationale. Les chercheurs, décideurs et négociateurs éprouvent souvent des difficultés à faire la part des infractions nationales et transnationales, d'où la nécessité d'une approche intégrée, en particulier aux premiers stades du processus;

d) Les vues d'acteurs du secteur privé et l'aide qu'ils peuvent apporter, l'accent étant mis sur les points suivants:

i) Examen des vues et des apports des entreprises chargées d'élaborer et d'appliquer les technologies pertinentes, y compris en ce qui concerne le matériel et le logiciel, et les réseaux informatiques et de télécommunications;

ii) Examen des vues d'organisations non gouvernementales compétentes. Des organisations qui militent en faveur de causes comme la liberté d'expression et la protection de la vie privée ont formulé des critiques à l'égard des tentatives qui ont été faites pour établir des pouvoirs d'enquête effectifs et ont exprimé leur opposition aux efforts déployés par le Groupe des 8 et le Conseil de l'Europe dans ce domaine;

e) Diverses questions ne relevant pas de la lutte contre la criminalité, comme le développement durable, la protection de la vie privée, la liberté d'expression et d'autres droits fondamentaux, ainsi que certains intérêts de nature commerciale et autre. Ces derniers, ainsi que d'autres intérêts essentiels sont étroitement associés au développement technologique et ils risquent d'être lésés par la progression de la criminalité informatique et par les mesures prises par les pouvoirs publics et la communauté internationale pour la prévenir et la combattre;

f) Une évaluation de l'ampleur de la délinquance, tant d'une manière générale qu'au regard de certains facteurs présentant un intérêt statistique, comme des formes spécifiques de criminalité, la situation géographique ou d'autres caractéristiques sociales ou économiques. Les difficultés que soulèvent la collecte et l'analyse de statistiques précises ont déjà été examinées. Toutefois, à mesure que l'on s'oriente vers une interprétation commune de l'étendue du problème d'un point de vue technique et de la typologie des infractions qui y sont associées, un plus grand nombre de données fiables deviennent disponibles. En outre, compte tenu de la sensibilisation croissante du public aux types de comportement en cause et au fait que ces derniers sont ou devraient être considérés comme des délits, les taux de signalement, actuellement insuffisants, devraient s'améliorer. La collecte de données primaires est également importante pour consolider l'appui politique nécessaire à une lutte nationale et internationale efficace contre ces délits;

g) Examen de la définition et du classement des délits technologiques et informatiques. Le classement utilisé dans le présent rapport est conforme à d'autres travaux menés dans ce domaine et pourrait servir de base à un examen plus approfondi, encore qu'une étude plus fouillée et plus rigoureuse soit nécessaire pour définir un cadre susceptible de recueillir un consensus parmi les gouvernements, les groupes d'intérêt et les experts. Il s'agit là d'une des premières priorités, étant entendu que des définitions et classifications sont indispensables pour donner la cohérence voulue à la collecte de statistiques et de données de la recherche, à partir desquelles il sera possible d'élaborer de nouvelles politiques. Pour qu'une typologie soit viable, il faut analyser divers facteurs dans plusieurs grands domaines, notamment les suivants:

i) *Les technologies pertinentes*. Le domaine des délits technologiques et informatiques est subordonné dans une large mesure à la nature et à l'étendue des technologies en cause qui évoluent et convergent rapidement. De ce fait, l'expression générique "délits technologiques et informatiques" a été utilisée dans le présent rapport et dans d'autres documents consacrés à ce sujet. La recherche est nécessaire pour embrasser toute la gamme des technologies considérées et proposer plusieurs possibilités de classement général qui les engloberaient toutes. Il conviendrait également d'examiner plus en détail certains progrès technologiques et les modes d'activité criminelle qui y sont liés. Compte tenu de l'évolution rapide des technologies, une attention devrait être accordée non seulement aux technologies actuelles, mais aussi aux évolutions technologiques potentielles;

ii) *La nature et les motivations des délinquants*. Les délinquants qui commettent des délits à l'aide des nouvelles technologies représentent un domaine d'étude relativement nouveau. Les motivations des délinquants plus traditionnels, comme les pédophiles, les escrocs ou les trafiquants de drogue internationaux sont bien connues. L'adaptation de ces délinquants aux nouvelles technologies doit être examinée sous l'angle de la criminalité informatique;

iii) *Les aspects géographiques des délits informatiques*. Du point de vue géographique, les délits informatiques diffèrent des délits plus classiques pour au moins deux grandes raisons. La première est que deux "géographies" principales sont superposées. L'emplacement physique réel des délinquants et ses facteurs situationnels spécifiques, comme les conditions sociales, économiques ou culturelles sont importants. Mais la géographie électronique – les considérations liées au cyberespace maintes fois citées – qui influe sur les caractéristiques du délit est également importante.

F. Solutions envisageables et recommandations particulières en vue des travaux à mener dans le domaine des délits technologiques et informatiques

1. Instrument international envisageable contre les délits technologiques et informatiques

51. Une fois que l'étude sera achevée, il est recommandé que le groupe d'experts donne à la Commission des conseils sur les questions et les options à examiner pour déterminer s'il est possible et souhaitable d'élaborer un instrument international contre les délits technologiques et informatiques. Il s'agira notamment:

a) D'établir si un tel instrument, sous réserve qu'il soit réalisable, doit être normatif ou juridiquement contraignant. Il pourrait viser à définir des obligations impératives, par exemple, aux infractions pénales, aux pouvoirs d'enquête et aux mécanismes de coopération internationale ou il pourrait simplement proposer des principes directeurs pour aider les États à élaborer des mesures efficaces et pour promouvoir la normalisation internationale des lois et des procédures. Un compromis entre ces deux options, illustré par la Convention des Nations Unies contre la criminalité transnationale organisée, consisterait à élaborer un instrument aux termes duquel certaines dispositions créeraient des obligations impératives tandis que d'autres énonceraient des principes directeurs plus généraux ou laisseraient les questions d'exécution à la discrétion des États parties;

b) De déterminer quelle serait la relation, le cas échéant, d'un nouvel instrument avec la Convention des Nations Unies contre la criminalité transnationale organisée. En général, certaines dispositions de la Convention pourraient servir de précédent, mais d'autres ne conviendraient peut-être pas à la question des délits technologiques et informatiques. Le fait que le champ d'application de la Convention soit limité aux activités de "groupes criminels organisés", par exemple, exclurait un nombre

important de délits technologiques et informatiques, en ce sens que ces derniers sont commis par des individus ou des groupes qui ne répondent pas à la définition retenue dans la Convention[23]. La possibilité d'élaborer un nouveau protocole à la Convention pour les délits de ce type semble donc écartée[24];

c) D'établir comment un instrument, une fois conclu, pourrait être actualisé. Comme noté dans l'introduction au présent rapport, le domaine à l'étude se caractérise par l'évolution dynamique des technologies et des activités criminelles qui y sont associées, et il sera important de veiller à ce que tout cadre tendant à intégrer des mesures nationales et internationales puisse suivre le rythme des évolutions. Parmi les options envisageables, on pourrait prévoir de déléguer certains pouvoirs législatifs à un organisme d'experts représentant les États parties et constitué à cette fin, d'utiliser des protocoles pour aborder des questions particulières à mesure qu'elles se posent, d'employer une terminologie assez large et neutre du point de vue technique, ou d'appliquer d'autres mesures;

d) De savoir comment incorporer des intérêts connexes comme la vie privée, la liberté d'expression et d'autres droits individuels fondamentaux et intérêts commerciaux dans un instrument international. Certes, le sujet à l'étude exige qu'un tel instrument soit axé sur la répression et la prévention de la criminalité, mais d'autres intérêts doivent également être pris en considération, tant dans le processus d'élaboration de l'instrument que dans son contenu.

2. Stratégie à court terme applicable aux délits technologiques et informatiques

52. Comme noté ci-dessus, les délits technologiques et informatiques soulèvent un problème urgent qui pourrait exiger une solution internationale concertée à court et à long terme. Il est recommandé que l'étude passe en revue les mesures qui pourraient être prises dans l'immédiat et que le groupe d'experts formule des recommandations concernant une stratégie à court terme pour examen par la Commission à sa onzième session. Une telle stratégie suppose notamment ce qui suit:

a) Il faudrait rassembler et distribuer à tous les États Membres des données sur les délits technologiques et informatiques et sur les solutions envisageables pour y faire face, afin d'informer, le plus rapidement possible, ceux qui ne participent pas encore aux discussions. L'étude proposée serait un élément clef du dossier, mais d'autres sources pourraient être mises à profit, notamment:

i) Le *Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique*, publié en 1994, pourrait être mis à jour et réédité;

ii) Les comptes rendus et la documentation de l'atelier sur les délits liés à l'utilisation du réseau informatique, qui s'est tenu lors du dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, pourraient être publiés et diffusés[25];

iii) Des documents d'autres organisations intergouvernementales, en particulier du Conseil de l'Europe, d'Interpol et du Groupe de Lyon créé par le Groupe des 8, pourraient être plus largement diffusés;

iv) Des ateliers, séminaires ou réunions d'information pourraient être organisés avec des fonctionnaires des États intéressés et, éventuellement, avec la participation de représentants du secteur privé;

b) Les matériels de formation des enquêteurs et des magistrats du parquet pourraient être plus accessibles. L'Organisation des Nations Unies n'a pas établi de tels matériels, mais un certain nombre d'États Membres l'ont fait pour former leurs propres fonctionnaires et, dans certains, cas pour réaliser des projets d'assistance technique avec le concours d'autres États;

c) Une assistance technique directe sera nécessaire dans certains États. Une telle assistance pourrait notamment servir à dispenser une formation aux juges, aux magistrats du parquet, aux enquêteurs et aux experts techniques ou légistes, dont bon nombre seraient ensuite en mesure d'assurer eux-mêmes une formation. Dans certains cas, ces projets pourraient être intégrés à des projets de développement plus généraux visant à aider les États à acquérir et à utiliser de nouvelles technologies au service du développement. Comme noté ci-dessus, il sera important que la prévention et la répression de la criminalité deviennent partie intégrante de ces projets si l'on veut éviter que les délits informatiques aient des effets néfastes sur le développement;

d) Il faudrait promouvoir, dans chaque État Membre, la création de centres de liaison ou de points de contact, qui pourraient être chargés, notamment, d'assurer une aide immédiate dans les enquêtes portant sur les délits informatiques[26], ou encore d'entretenir des relations plus générales dont l'objet serait de rassembler des informations sur l'évolution de la situation dans chaque État, de recevoir des informations de la communauté internationale et de les diffuser;

e) Un engagement important de ressources financières et techniques sera nécessaire. Une telle assistance pourrait prendre la forme de contributions volontaires au Fonds des Nations Unies pour la prévention du crime et la justice pénale ou de la prestation de services d'experts ou de matériels à l'appui d'un programme mondial contre les délits technologiques et informatiques ou de projets spécifiques de l'ONU. L'universalité des technologies et leur vulnérabilité à l'exploitation que peuvent en faire les délinquants partout dans le monde devraient inciter les États dotés de ressources financières ou techniques à aider les autres États. Les entreprises qui établissent et exploitent des réseaux informatiques et de télécommunications disposent également de ressources financières et techniques qui peuvent être mises à profit, et elles devraient également être incitées à apporter une contribution, étant entendu que de nombreuses formes de la criminalité informatique menacent la viabilité commerciale de leurs produits.

3. Mise en place d'un programme mondial contre les délits technologiques et informatiques

53. Il ressort des données disponibles qu'un nombre considérable d'activités est mené dans le domaine de la recherche et de l'élaboration de mesures stratégiques, juridiques et techniques, mais que ces activités sont assez peu coordonnées. Leur étendue varie selon les pays. Un certain nombre d'organisations intergouvernementales et non gouvernementales ainsi que divers départements de l'ONU et organismes des Nations Unies y participent, et les entreprises commerciales de même que des groupes d'intérêt non gouvernementaux y attachent une grande importance. L'attention et également l'allocation des ressources sont en général axées sur des sujets qui préoccupent plus particulièrement les gouvernements ou les organisations directement intéressés, ce qui accroît les risques de déséquilibres ou d'incohérences dans la recherche. De par sa vocation mondiale, l'Organisation des Nations Unies occupe une place exceptionnelle pour étudier et coordonner les activités menées dans le domaine à l'étude. Il est recommandé, une fois que les besoins et les vues des États Membres auront été examinés, de mettre en place un programme mondial contre les délits technologiques et informatiques. Il est également recommandé que les États concernés versent des contributions volontaires pour créer et mettre en œuvre un tel programme.

54. Le mandat de ce programme mondial, le cas échéant, devrait être examiné par la Commission, à sa onzième session, lorsque les résultats de l'étude et les avis du groupe d'experts auront été obtenus. Ce mandat pourrait prendre en compte les activités énoncées dans le paragraphe 52 ci-dessus, de même que les activités suivantes:

a) Recensement des États Membres demandant une aide et analyse de leurs besoins particuliers;

b) Mise au point de matériels pour aider les décideurs, les législateurs, les services de répression, les magistrats du parquet et d'autres fonctionnaires spécialistes de la question à instruire les affaires aux plans national et transnational;

c) Rassemblement, classement et diffusion de matériels établis par d'autres entités;

d) Fourniture d'une assistance judiciaire, technique et autre aux États qui en font la demande, sous réserve de disposer de ressources suffisantes;

e) Établissement d'un inventaire des compétences techniques disponibles auprès de particuliers et d'organismes désireux d'apporter une aide aux États qui en font la demande;

f) Coordination des activités avec d'autres départements de l'ONU et organismes des Nations Unies, en particulier dans les domaines des droits de l'homme et du développement, en vue d'inscrire les délits informatiques dans le cadre d'autres programmes, le cas échéant, et de veiller à ce que les éléments d'autres programmes soient pris en compte dans l'élaboration des stratégies de prévention et de répression de la criminalité;

g) Coordination des activités avec d'autres organisations intergouvernementales et des

gouvernements et organismes menant des activités dans le domaine des délits technologiques et informatiques;

h) Coordination des activités avec des groupes d'intérêt non gouvernementaux et des entreprises du secteur privé et mobilisation de ressources monétaires et de compétences techniques auprès des entreprises dans le cadre d'une stratégie mondiale de lutte contre les délits technologiques et informatiques.

4. Inventaire préliminaire des questions de fond à examiner

55. Un grand nombre des mêmes questions de fond devront être abordées en tant qu'éléments des stratégies à court terme et à long terme. Compte tenu des délibérations qui ont déjà eu lieu dans le cadre de l'Organisation des Nations Unies et d'autres instances mentionnées dans le présent rapport, il faudra examiner les questions ci-après:

a) Recensement des comportements préjudiciables associés aux nouvelles technologies et création de nouvelles infractions ou modification des infractions existantes pour ériger ces comportements en infractions pénales;

b) Élaboration de principes applicables à la localisation transnationale des communications, y compris pouvoirs d'obtenir, de conserver et de divulguer des données sur les communications[27];

c) Élaboration de principes régissant les recherches électroniques transfrontières intentionnelles ou non intentionnelles;

d) Élaboration de principes communs régissant l'interception des communications transmises sur des réseaux informatiques et des médias analogues;

e) Évaluation des intérêts touchant la confidentialité et la vie privée qui sont inhérents à diverses formes de stockage et de transmission de données, en vue d'élaborer des contrôles de procédures pour les opérations de saisie et d'interception, conformément à ces intérêts. La plupart des États imposent peu ou n'imposent pas de restrictions à l'accès des services de répression aux sites Internet publics ou aux communications sur le Web, par exemple, alors qu'ils en appliqueraient en ce qui concerne la saisie de données émanant de sources plus privées;

f) Élaboration de normes ou de pratiques communes pour recenser les utilisateurs de réseaux informatiques ou de services de télécommunications, compte tenu de la nécessité de protéger la vie privée et l'anonymat;

g) Élaboration de principes communs afin d'adapter les pratiques médico-légales et les règles de preuve juridiques pour faire en sorte que les preuves informatiques puissent être sauvegardées, authentifiées et utilisées dans les poursuites pénales;

h) Élaboration de principes communs en vue de protéger les droits fondamentaux, tant dans la mise au point des politiques et mesures internationales de lutte contre les délits technologiques et informatiques que dans l'application de ces mesures à des cas particuliers;

i) Élaboration de principes communs régissant la confidentialité et l'intégrité des données et recherche d'un équilibre pour concilier ces principes avec la nécessité de mesures efficaces de répression;

j) Mise au point et financement de programmes d'assistance technique et de matériels pour les États qui en font la demande. Ces programmes et matériels seront nécessaires à la fois pour aider les États à prendre part effectivement à l'élaboration des politiques mondiales et faire en sorte que les autorités nationales soient convenablement formées et équipées pour répondre efficacement et rapidement aux demandes d'assistance en cas d'enquête sur des délits informatiques transnationaux;

k) Collecte, analyse et échange d'informations sur les progrès technologiques, les délinquants et les techniques qu'ils appliquent et sur les méthodes permettant efficacement de prévenir les infractions, d'enquêter sur les infractions et d'en poursuivre les auteurs;

l) Formation, équipement et dotation en ressources des spécialistes de la répression afin qu'ils soient à même de mener des enquêtes et d'engager des poursuites efficacement dans le cadre d'affaires nationales, et de coopérer utilement avec d'autres États dans le cadre d'affaires transnationales;

m) Nécessité d'évaluer et de préciser le rôle du secteur privé dans sa relation avec les pouvoirs publics, aux plans tant national qu'international. Une attention

devra être accordée aux éléments ou aspects particuliers de cette relation, notamment:

i) À la nécessité d'établir un équilibre entre les mesures efficaces de répression et les contraintes d'ordre technique et commercial qui s'exercent sur leur élaboration et application. La répression devrait être envisagée par les entreprises dès le stade de la conception des nouvelles technologies, mais il faut que les services de répression admettent que certaines mesures ne sont peut-être pas techniquement réalisables ou risquent d'introduire des changements qui rendraient ces technologies inopérantes ou moins concurrentielles. Les exigences de la répression ne devraient pas porter préjudice à la viabilité fondamentale ou à la compétitivité des nouvelles technologies, mais le coût de la criminalité et de sa prévention doit être pris en compte dans les évaluations globales coûts-avantages des pouvoirs publics et des entreprises et il devrait être imputé, le cas échéant, sur les bénéfices dégagés par les technologies utilisées au service de la criminalité;

ii) À la nécessité pour les pouvoirs publics et les entreprises de coopérer efficacement pour optimiser les avantages et réduire au minimum les coûts. Il faut notamment recenser et élaborer des techniques efficaces de sécurité et autres méthodes de prévention de la criminalité, les incorporer dans les nouvelles technologies dès que possible dans le processus d'élaboration et former et préparer le personnel des services de répression et du parquet aux nouvelles technologies avant que des délinquants potentiels n'y aient accès. Le progrès technologique enregistré par les entreprises concernées en fait des facteurs importants, voire essentiels, du succès des programmes d'assistance technique, et les intérêts commerciaux des entreprises elles-mêmes justifieront dans de nombreux cas leur participation à ces programmes;

iii) À la nécessité d'élaborer des systèmes et de mener des activités de nature à rendre plus efficaces les enquêtes pénales et les mesures de prévention de la criminalité, compte tenu également de la nécessité de protéger la vie privée et d'autres droits des utilisateurs des technologies. À cet égard, on peut citer, par exemple, les systèmes qui peuvent conserver pendant un délai raisonnable la preuve d'une communication, qui pourrait être indispensable à une enquête, et la nécessité de pouvoir identifier les clients;

iv) À la nécessité de procéder à une évaluation globale du rôle potentiel du secteur privé dans la lutte contre la criminalité. Il s'agit là d'un problème complexe auquel sont déjà confrontés de nombreux prestataires de services qui, à l'instar du grand public, souhaitent que la criminalité soit efficacement réprimée, mais qui ont aussi conscience des dangers et des difficultés qui pourraient surgir s'ils se substituaient aux services de répression de l'État. Les entreprises doivent faire face à des pressions contradictoires les incitant à incorporer dans les nouvelles technologies des mesures sécuritaires qui ne sont peut-être pas commercialement viables ou qui lèsent les intérêts fondamentaux de leurs clients[28]. Elles subissent également le poids des pressions exercées par les pouvoirs publics pour les amener à contrôler ou à exclure des contenus jugés illégaux ou inconvenants, ou à aider les services de répression nationaux à conduire des enquêtes pénales. Ces pressions soulèvent des problèmes éthiques et juridiques et des questions de fond qu'il conviendrait d'examiner, aux plans national et international, afin d'assurer le niveau de cohérence le plus élevé possible à l'échelle mondiale.

Notes

[1] Voir "Combler le fossé numérique" dans le rapport du Secrétaire général à l'Assemblée du Millénaire des Nations Unies (A/54/2000, par. 150 à 167). Voir également le rapport du Secrétaire général sur le développement et la coopération internationale au XXI^{e} siècle: le rôle des technologies de l'information dans le cadre d'une économie mondiale à forte intensité de connaissances (E/2000/52, sect. III à V).

[2] Comité européen pour les problèmes criminels, Comité d'experts sur la criminalité dans le cyberespace, "Projet de convention sur la cybercriminalité" (PC-CY (2000)), projet n° 25, rev.5, disponible en ligne à l'adresse Internet suivante: http://conventions.coe.int/treaty/FR/projets/cybercrime25.htm

[3] Les conclusions de ces études sont présentées dans les recommandations R(89) 9 et R(95) 13 du Conseil de l'Europe. Le Comité d'experts a été créé par le Comité des ministres du Conseil de l'Europe à la 583e réunion des délégués des ministres, le 4 février 1997.

[4] Voir l'annexe du communiqué publié à l'issue de la réunion des ministres de la justice et de l'intérieur du G-8, tenue à Washington le 10 décembre 1997.

[5] Voir le communiqué publié à l'issue de la Conférence ministérielle des pays du G-8 sur la lutte contre la criminalité transnationale organisée, tenue à Moscou les 19 et 20 octobre 1999 (par. 17 et annexe I).

[6] Des réunions se sont tenues à Paris du 15 au 17 mai 2000 et à Berlin du 24 au 26 octobre 2000. Une nouvelle réunion est prévue à Tokyo en mai 2001.

[7] Au paragraphe 14 de la résolution 1999/23, le Conseil économique et social a prié le Secrétaire général d'entreprendre une étude sur les mesures efficaces qui pourraient être prises aux niveaux national et international pour prévenir les délits informatiques et lutter contre eux, dont éventuellement un examen de l'opportunité d'élaborer des manuels, des directives et des recommandations, et de faire rapport sur les conclusions de cette étude à la Commission pour la prévention du crime et la justice pénale, à sa dixième session.

[8] Voir les résolutions 45/109 et 45/121 du 14 décembre 1990 de l'Assemblée générale et le *huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, La Havane, 27 août-7 septembre 1990: rapport établi par le Secrétariat* (publication des Nations Unies, numéro de vente: F.91.IV.2), chap. premier, sect. C, p. 149.

[9] Voir A/CONF.169/16/Rev.1, par. 370 à 385.

[10] Voir résolution 55/25 de l'Assemblée générale en date du 15 novembre 2000, annexe I, art. 18, par. 8 à 18.

[11] Voir *huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants ...*, chap. premier, sect. C.

[12] Revue internationale de politique criminelle nos 43 et 44 (publication des Nations Unies, numéro de vente: F.94.IV.5).

[13] Voir les résolutions 52/91 et 53/110 de l'Assemblée générale en date respectivement du 12 décembre 1997 et du 9 décembre 1998, Voir également le document A/CONF.187/10 et le d*ixième Congrès des Nations Unies sur la prévention du crime et le traitement des délinquants, Vienne, 10-17 avril 2000: rapport établi par le Secrétariat* (publication des Nations Unies, numéro de vente: F.00.IV.8) par. 161 à 174.

[14] Voir A/CONF.187/L.10. par. 14.

[15] Voir d*ixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants ...*, chap. premier.

[16] Voir les articles 2 (Terminologie) et 3 (Champ d'application) de la Convention (résolution 55/25, annexe I).

[17] Le Groupe d'action financière sur le blanchiment de capitaux (GAFI) de l'Organisation de coopération et de développement économiques (OCDE) a récemment examiné ce type d'infractions. Voir le "Rapport sur les typologies du blanchiment de capitaux, 2000-2001" du GAFI (Paris, OCDE, février 2001), par. 5 à 18.

[18] A/54/2000, par. 152.

[19] Ainsi, le Directeur du Federal Bureau of Investigation (FBI) des États-Unis d'Amérique indiquait, dans une déclaration sur la cybercriminalité prononcée devant la Commission des affaires juridiques du Sénat le 28 mars 2000, qu'entre 1998 et 1999, le nombre d'affaires traitées par ses services avait doublé, passant de 547 à 1 154, mais qu'il était difficile de savoir si cette évolution était due à une progression des infractions, à une augmentation du nombre de plaintes ou aux deux. Voir également P. Graboski, "Computer crime: a criminological overview", *Forum on Crime and Society*, vol. 1 (2001), p. 40.

[20] Aux États-Unis, un programmateur de 31 ans a avoué être l'auteur du virus "Melissa". Un Canadien de 15 ans a plaidé coupable sur 56 chefs d'accusation liés à des attaques par déni de service. Aucune accusation n'a été portée dans le cas du virus "I love you", qui semblerait toutefois provenir des Philippines. Les estimations les plus variées ont circulé quant aux dommages causés par chacun de ces incidents, dont le coût réel ne sera probablement jamais connu. Les chiffres cités ici donnent une indication du volume des pertes subies et du niveau de l'intérêt politique porté à la menace que font peser des infractions d'une telle ampleur.

[21] Voir E/2000/52, sect. III à V.

[22] Voir E/2000/52, par. 79 à 99.

[23] Voir les articles 2 et 3 de la Convention (résolution 55/25, annexe I).

[24] Les trois protocoles en vigueur contiennent tous des dispositions relatives au champ d'application et à l'application de la Convention, *mutatis mutandis*. Nombre des dispositions de la Convention ont été rédigées sachant qu'elles ne s'appliqueraient qu'aux affaires impliquant des groupes criminels organisés et, de ce fait, il serait difficile de les appliquer à des affaires

ayant trait à des délits informatiques commis par des particuliers.

[25] L'Institut des Nations Unies pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient, qui a organisé l'atelier, prépare actuellement ces documents pour les publier.

[26] Ce processus a déjà été engagé par le Groupe des 8 puis repris par Interpol.

[27] On entend en général par "données sur les communications" les données stockées par les prestataires de services qui consignent la source et la destination d'une communication électronique. Il peut s'agir à la fois de la source et de la destination ultimes ainsi que des sources ou destinations intermédiaires dans le cadre d'un réseau informatique. Dans ce contexte, les prestataires de services emploient aussi l'expression "données sur l'abonné" ou "données sur l'utilisateur" pour identifier les clients.

[28] Un exemple récent en a été donné par la décision d'un tribunal français enjoignant la société Internet Yahoo! Inc. de mettre au point une technique particulière pour empêcher ses abonnés en France d'accéder au site Web de vente aux enchères d'objets nazis. La vente de ces articles est interdite en France mais légale sur les territoires où les sites à proprement parler sont situés. En général, les prestataires sont disposés à prendre de telles mesures, pour autant qu'elles soient techniquement réalisables, mais seulement lorsqu'un tribunal compétent ou une autre autorité publique a établi que le contenu lui-même était illégal.