

## I. Les défis en matière de répression antidrogue à l'ère de la mondialisation et des nouvelles technologies

1. La mondialisation et les nouvelles technologies des communications ont apporté à la société d'innombrables avantages, sur le plan économique, éducatif et culturel, qui ont permis de combler des lacunes qui semblaient insurmontables il y a seulement 10 ans. Depuis la fin de la guerre froide, les restrictions auxquelles étaient soumises les opérations commerciales et financières internationales ont disparu et la déréglementation et la libéralisation ont donné un coup de fouet au commerce mondial, tandis que la chute du communisme dans l'ancien bloc de l'Est a stimulé la croissance de nouvelles économies de marché et intensifié la circulation transfrontière des personnes, des marchandises et des capitaux. Le nombre d'utilisateurs d'Internet dans le monde, qui double pratiquement tous les six mois, était estimé à 700 millions à la fin de 2001. L'industrie des technologies de l'information est devenue un secteur producteur de richesse à l'échelle mondiale qui constitue un enjeu important pour les pays développés comme pour les pays en développement.

2. Au-delà de la dimension économique, l'intégration des économies nationales dans un système mondial unique, dominé par la performance des places boursières et des marchés de capitaux touche l'essence même de l'identité culturelle et sociale. L'effondrement des barrières idéologiques s'est accompagné, d'une part, d'une homogénéisation économique et, d'autre part, d'une atomisation politique et sociale. Dans de nombreux endroits du monde, la prospérité économique coexiste avec des foyers de marginalisation et de pauvreté grandissantes, tandis que, dans les pays en développement particulièrement, les liens traditionnels qui assuraient la cohésion sociale ont été affaiblis par la rapidité du changement. Les revendeurs et trafiquants de drogues exploitent ces disparités pour tenter de développer de nouveaux marchés. En outre, au cours des 10 dernières années, l'expansion de l'activité commerciale et financière a permis aux délinquants de mieux dissimuler les transferts illicites de marchandises comme les drogues et les précurseurs placés sous contrôle international, et les profits qu'ils en tirent. Autrement dit, l'évolution technologique et la mondialisation des échanges commerciaux et

financiers ont favorisé le progrès social, mais ont aussi encouragé des formes traditionnelles et nouvelles de criminalité liée à la drogue.

3. L'Organe international de contrôle des stupéfiants a décidé de considérer la mondialisation et les nouvelles technologies dans le présent rapport, non dans l'intention de les condamner, mais parce que les avantages que ces phénomènes procurent à la société risquent d'être remis en cause par des individus et des groupes criminels qui les utilisent pour réaliser des gains illicites. En particulier, elles soulèvent de nouveaux problèmes pour l'application des trois traités internationaux relatifs au contrôle des drogues. L'Organe, qui est chargé de veiller au respect de ces traités, se doit d'attirer l'attention des gouvernements et du grand public sur ces problèmes.

4. L'Organe se préoccupe depuis quelque temps de l'utilisation détournée des nouvelles technologies s'agissant des substances placées sous contrôle international. Dans son rapport annuel pour 1997<sup>1</sup>, il attirait l'attention sur le fait qu'en violation de l'article 3 de la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes de 1988<sup>2</sup>, des informations diffusées par voie électronique ou par d'autres moyens de communication semblaient inviter ou inciter à la consommation de drogues. Dans ses rapports pour 1997<sup>3</sup> et 1998<sup>4</sup>, l'Organe notait qu'Internet permettait d'échanger des informations et des conseils sur l'usage et la fabrication illicites de drogues. Dans son rapport pour 2000<sup>5</sup>, il a également exprimé sa préoccupation devant l'essor non contrôlé des pharmacies Internet qui font la promotion de substances placées sous contrôle et les vendent sans ordonnance. De telles pratiques vont à l'encontre de l'article 10 de la Convention de 1971 sur les substances psychotropes<sup>6</sup>, qui exige que les Parties, tenant dûment compte des dispositions de leurs constitutions, interdisent les annonces publicitaires ayant trait aux substances psychotropes et destinées au grand public.

## A. Impact de la mondialisation et des nouvelles technologies sur la criminalité liée à la drogue et sur les organisations criminelles

### La cybercriminalité: définition

5. Le terme “cybercriminalité” recouvre de nombreux types d’activités, mais s’applique principalement aux infractions commises et/ou facilitées grâce aux médias électroniques<sup>7</sup>. Comparée à la criminalité ordinaire, la cybercriminalité nécessite moins de ressources proportionnellement aux dommages susceptibles d’être causés; elle peut s’exercer dans un État sans que le délinquant y soit présent physiquement et, dans de nombreux pays, les infractions en question sont définies de façon inadéquate ou ne sont pas définies du tout, de sorte que leurs auteurs s’exposent à peu de risques et que la probabilité qu’ils soient découverts est faible.

### *Impact sur la criminalité organisée liée à la drogue*

6. La criminalité organisée a ses propres modes opératoires, qui font fi de la légalité et reposent sur la violence. elle a toutefois suivi certaines des tendances commerciales propres à l’économie légitime. Elle s’est internationalisée, restructurée et décentralisée, en d’autres termes, elle s’est elle aussi mondialisée.

7. Le groupe criminel organisé indépendant, avec sa structure pyramidale, a tendance à faire place à des réseaux fluctuants structurés en cellules, dans lesquels l’identité nationale importe moins que la compétence, bien que la nationalité elle-même puisse conduire à une fonction si elle permet d’accéder à un nouveau marché ou de pénétrer ou corrompre une institution particulière. Les criminels transnationaux n’ont que faire des frontières: en menant leurs activités dans plusieurs États, ils réduisent au minimum les risques de répression tout en maximisant leurs profits; ainsi, aucun État ne peut considérer qu’une affaire criminelle particulière relève entièrement de sa compétence.

8. Le réseau est la forme d’organisation caractéristique de la mondialisation, tant dans le secteur licite que dans le secteur illicite. Pour une organisation qui se livre au trafic de drogues, la structure en réseau présente des avantages incontestables par rapport au système hiérarchique

traditionnel: elle comprend un “noyau dur” bien protégé d’organisations ou de personnes, connecté à une “périphérie” plus lâche par une multitude de liens, ce qui accroît sa capacité à échapper à l’action des services de répression.

9. Les nouvelles technologies sont utilisées par les trafiquants de drogues de deux façons différentes: pour améliorer l’efficacité de la livraison et de la distribution des produits au moyen de communications sûres et instantanées, et pour se protéger et protéger leurs activités illicites des enquêtes menées par les services de répression, parfois en contre-attaquant. Elles leur permettent de commettre des délits classiques selon de nouvelles méthodes – par exemple, d’organiser des envois de drogues illicites à l’aide de messages codés ou de blanchir des capitaux liés à la drogue grâce à des virements électroniques – et de nouveaux types de délits par de nouveaux moyens – par exemple, de lancer une “guerre de l’information” ou une “attaque” électronique pour contrer l’action de renseignement des services de détection et de répression en matière de drogues.

10. Les trafiquants de drogues se servent d’ordinateurs et d’agendas électroniques pour stocker des informations (telles que numéros de comptes bancaires, noms, adresses et autres renseignements concernant leurs collaborateurs, données concernant les actifs, les opérations financières, les ventes et autres documents commerciaux, coordonnées géographiques de pistes d’atterrissage clandestines, et recettes de fabrication de drogues synthétiques) ainsi que pour envoyer des courriers électroniques et d’autres formes de correspondance<sup>8</sup>. Les auxiliaires reçoivent par téléphone, télécopieur, alphanpage ou ordinateur les instructions leur indiquant où livrer les envois de marchandises, les personnes à contacter pour le transport et celles à qui verser les profits réalisés. Les trafiquants s’assurent une meilleure protection en recourant à des cartes téléphoniques prépayées, à des fréquences radio à large bande, à des forums de discussions sur Internet à accès limité, au chiffrement des données, à la téléphonie par satellite et à des téléphones mobiles “clonés” (ainsi baptisés lorsque les codes d’identification fournis aux utilisateurs légitimes sont interceptés et programmés sur les téléphones utilisés par les délinquants)<sup>9</sup>. Les membres d’organisations de trafiquants de drogues peuvent programmer leurs ordinateurs de manière à détecter toute tentative d’intrusion et à y répondre par des

techniques de contre-attaque visant à endommager les systèmes de ceux qui enquêtent. Ces techniques sont particulièrement utiles à ceux qui organisent le trafic de drogues, du fait qu'ils sont rarement obligés de quitter leur repaire pour organiser ou superviser leurs opérations.

11. La police des stupéfiants de la Région administrative spéciale de Hong Kong (Chine) signale qu'avec les progrès du commerce électronique et des services bancaires sur Internet, il est devenu plus difficile de déceler le blanchiment de capitaux liés à la drogue. Les trafiquants de drogues communiquent entre eux principalement par le biais de téléphones mobiles fonctionnant avec des cartes prépayées pouvant être achetées anonymement. La Chine a également signalé un cas, sans doute en rapport avec le trafic de drogues, où des délinquants, pour éviter d'être détectés, avaient pénétré la base de données des douanes pour falsifier les caractéristiques et la nature d'un envoi commercial de marchandises.

12. En Australie, les trafiquants tirent parti de la possibilité offerte à tous les clients de sociétés de messagerie internationale de suivre leurs envois sur le site Web de ces sociétés. Un retard peut indiquer aux trafiquants qu'une opération de livraison surveillée est sur le point d'être effectuée. Les services de répression doivent donc agir dans un délai extrêmement court pour éviter d'éveiller les soupçons.

13. La Commission interaméricaine de contrôle de l'abus de drogues (CICAD) de l'Organisation des États américains (OEA) a indiqué dans son *Rapport hémisphérique pour 1999-2000*<sup>10</sup> qu'Internet était devenu le moyen le plus utilisé pour développer la production de drogues synthétiques dans certains pays de la région et que la mondialisation, les communications instantanées et les transferts électroniques de fonds avaient été utilisés par les groupes criminels organisés pour améliorer l'efficacité de leurs activités de trafic de drogues.

14. Les services de détection et de répression des infractions en matière de drogues de la République tchèque signalent qu'aujourd'hui, des ventes et des achats de drogues illicites sont conclus en ligne dans des cybercafés ou par téléphone mobile. Du fait que des transactions sont conclues instantanément et sur de courtes distances, l'interception se révèle beaucoup plus difficile.

15. Depuis 1996, des sociétés basées aux Pays-Bas utilisent Internet pour vendre des semences de cannabis et des dérivés du cannabis. Selon l'Organisation internationale de police criminelle (Interpol), au début de l'année 2000 les autorités du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord ont identifié dans le monde plus de 1 000 sites Web proposant à la vente des drogues illicites, principalement du cannabis mais aussi de la méthylènedioxyméthamphétamine (MDMA, communément appelée ecstasy), de la cocaïne et de l'héroïne, en violation directe des traités internationaux relatifs au contrôle des drogues. C'est aux Pays-Bas et en Suisse que ces sites étaient les plus nombreux.

16. Aux États-Unis d'Amérique, les services de détection et de répression attribuent l'augmentation rapide des saisies opérées dans des laboratoires utilisés pour la fabrication illicite de méthamphétamine à l'évolution de la technologie et à l'usage accru d'Internet. Dans le passé, les recettes pour la fabrication de drogues étaient des secrets jalousement gardés, mais aujourd'hui, avec les techniques informatiques modernes et la tendance croissante des chimistes à partager leurs connaissances, cette information est à la disposition de quiconque a accès à un ordinateur. Il n'est pas nécessaire non plus d'être diplômé en chimie pour produire de l'amphétamine: moins de 10 % des suspects arrêtés pour fabrication illicite de méthamphétamine sont des chimistes qualifiés, ce qui explique les nombreux incendies, explosions et blessures dans les laboratoires clandestins<sup>11</sup>.

17. Une enquête conjointe des services antidrogue de la Colombie et des États-Unis a conduit à l'arrestation de 31 trafiquants en octobre 1999 et révélé que les trafiquants avaient communiqué par l'intermédiaire de forums Internet protégés par des pare-feux destinés à les rendre impénétrables. Les données détaillées concernant leurs activités quotidiennes avaient été enregistrées dans un ordinateur embarqué à bord d'un navire au large des côtes mexicaines, de sorte que même s'il avait été possible de pénétrer dans d'autres ordinateurs, le réseau n'aurait pu être démantelé dans sa totalité. Le même groupe avait eu recours à des techniques de chiffrement que les services de répression avaient été incapables de décoder en temps voulu pour pouvoir exploiter l'information. Ces méthodes, ainsi que le clonage de téléphones mobiles, avaient permis aux trafiquants de faire circuler des

centaines de tonnes de cocaïne durant des années avant d'être repérés<sup>12</sup>.

18. Les cartels de trafiquants colombiens et mexicains utilisent du matériel perfectionné pour espionner les agents chargés des enquêtes et intercepter leurs communications; ils rassemblent des photographies des agents antidrogue et d'autres informations les concernant. Cela s'est également produit en Europe. En 1995, un groupe de trafiquants aux Pays-Bas a recruté des informaticiens pour mener des opérations de piratage et coder ses communications. Les trafiquants utilisaient des ordinateurs de poche dotés d'un logiciel de cryptage pour stocker de manière sûre des données sur les véhicules banalisés de la police et des services de renseignement. Un ordinateur portable et des disquettes appartenant aux autorités chargées des enquêtes ont été volés et les renseignements qui en ont été tirés utilisés pour intercepter les communications entre les policiers, qui ont été ensuite surveillés et menacés.

#### *Impact sur la toxicomanie*

19. L'augmentation vertigineuse des ventes sur Internet de médicaments délivrés sur ordonnance constitue un défi sérieux pour les responsables chargés de la réglementation concernant l'innocuité des médicaments et les services de détection et de répression. Selon un comité de surveillance mis sur pied par le Congrès des États-Unis, le nombre de produits pharmaceutiques saisis dans ce pays entre 1998 et 1999 a progressé de 450 % – ce qui représente 7 586 saisies supplémentaires. Le comité a attribué cette évolution, dans une large mesure, aux achats effectués sur Internet. Au cours des cinq premiers mois de 2000, une trentaine d'enquêtes sur les ventes en ligne de produits pharmaceutiques ont été ouvertes<sup>13</sup>.

20. Dans le passé, l'Organe a attiré l'attention sur le fait qu'Internet est utilisé pour échanger des messages et des informations faisant l'apologie de la drogue, en particulier parmi les jeunes<sup>14</sup>. Une simple recherche sur Internet suffit pour, en quelques minutes, obtenir des instructions détaillées pour la fabrication de toute une gamme de drogues de synthèse, accéder à des critiques d'ouvrages sur les moyens de se procurer des précurseurs placés sous contrôle international et d'installer des laboratoires clandestins de fabrication de drogues, et être invité à acheter un large éventail de "livres de recettes" pour la fabrication de drogues.

21. L'Organe juge alarmantes les conséquences probables de cet état de choses. La première est l'expansion potentielle de la toxicomanie en raison de l'incitation à produire et à consommer des drogues au sein d'une sorte de "club" étendu dont les membres s'encouragent et s'entraident. Une autre est l'"amateurisation" de la narcocriminalité: les fabricants ou les consommateurs potentiels de drogues n'ont pas besoin de ressources ni de contacts spéciaux, ni même de vivre dans une zone où des drogues sont disponibles; un moteur de recherche permet à l'utilisateur d'Internet de prendre facilement contact avec des personnes ayant les mêmes inclinations dans différentes parties du monde et d'accéder à des sources d'approvisionnement dont il n'aurait sinon pas eu connaissance. Les jeunes peuvent être entraînés dans la criminalité liée à la drogue par les activités de désinformation, de propagande ou d'endoctrinement auxquelles se livrent des individus anonymes qui cherchent à tirer profit d'une augmentation du nombre de consommateurs de drogues. Lorsque l'approche est "virtuelle", les signaux d'alarme qui pourraient dissuader ou effrayer les jeunes dans le monde réel sont réduits au minimum et le processus de filtrage par lequel passe un individu pour prendre physiquement contact avec une organisation criminelle disparaît. Psychologiquement parlant, on peut dire que la "virtualité" est un facteur qui facilite la commission de l'infraction.

#### *Impact sur le blanchiment d'argent*

22. L'Organe est conscient du fait que la déréglementation des marchés de capitaux et l'élimination quasi totale des contrôles des changes ont permis aux banques de réduire les coûts et d'offrir un choix plus large à leurs clients, ce qui procure des avantages importants à de larges secteurs de la société. Cependant, il craint que le recours accru aux virements électroniques ainsi que l'augmentation considérable du volume et de la rapidité des flux monétaires ne réduisent la possibilité de détecter les mouvements de capitaux illicites dans le monde, et ne se traduisent donc par une augmentation du blanchiment de l'argent de la drogue.

23. Le Groupe d'action financière sur le blanchiment de capitaux (GAFI) a attiré l'attention sur le fait qu'Internet présentait trois caractéristiques qui pourraient aggraver certains risques "classiques" de blanchiment d'argent: facilité d'accès,

dépersonnalisation des contacts entre le client et l'établissement bancaire; et rapidité des transactions électroniques<sup>15</sup>. La mondialisation des marchés financiers pouvait être considérée comme un facteur de risque supplémentaire.

24. Bien que le paiement en liquide soit probablement encore le mode de paiement le plus courant pour l'achat des drogues au niveau local, la création de nouveaux marchés mondiaux de valeurs mobilières, d'obligations, d'opérations à terme, de devises et de produits dérivés a élargi l'éventail des opérations permettant de déplacer des sommes importantes par des moyens électroniques avec rapidité, facilité et dans le secret, autant de conditions idéales pour ceux qui se livrent au blanchiment de l'argent de la drogue. L'utilisation de cartes à puce et de services bancaires en ligne a réduit les contacts personnels entre les employés des banques et les clients, et donc l'efficacité des mécanismes permettant de vérifier la légitimité des transactions financières.

25. Les casinos étant depuis longtemps utilisés pour le blanchiment de fonds provenant du trafic de drogues et d'autres activités criminelles, il est logique que ce type d'activité se développe sur Internet. Alors que de nombreux établissements classiques appliquent désormais des procédures antiblanchiment, les "casinos virtuels" sont devenus une activité florissante qui n'est soumise à aucune réglementation. En mars 2001, un site de passionnés du jeu recensait 12 000 liens Internet et 2 045 "casinos virtuels".

26. Ces dernières années, le secteur des services financiers est devenu de plus en plus concurrentiel, ce qui a dissuadé de nombreuses banques de procéder à des contrôles préalables de crainte que leurs clients ne déposent leurs fonds chez un concurrent. Sur ce marché de plus en plus concurrentiel, les établissements financiers risquent de considérer le respect des mesures antiblanchiment comme incompatible avec la bonne marche des affaires, d'y attacher un faible degré de priorité et d'y consacrer des ressources peu importantes et du personnel peu qualifié. De surcroît, dans la plupart des pays, presque toutes les déclarations de transactions suspectes concernent encore des transactions en liquide. Dans des sociétés où l'argent liquide est de moins en moins utilisé, cela donne à penser que les mesures antiblanchiment, même si elles sont respectées, n'ont pas suivi l'évolution technologique.

## **B. Impact de la mondialisation et des nouvelles technologies sur les structures et les moyens dont disposent les pouvoirs publics pour lutter contre la narcocriminalité**

27. Les structures, en particulier les organes judiciaires et services de répression, mises en place par les pouvoirs publics pour faire face à la narcocriminalité transnationale se heurtent depuis longtemps à des difficultés tenant au fait qu'elles doivent mener leur action dans des limites bien définies de compétence et de souveraineté territoriales. Depuis la ratification de la Convention de 1988, de nombreux obstacles ont été surmontés grâce à des accords bilatéraux et multilatéraux et à des traités d'entraide judiciaire. Cependant, l'Organe craint que cette coopération internationale renforcée contre la criminalité liée à la drogue ne soit menacée par l'adoption, par les organisations qui se livrent au trafic et à la production illicite de drogues, de techniques leur permettant d'éviter d'être identifiées et de faire l'objet de poursuites. Il ne fait aucun doute que les services de détection et de répression n'ont pas tiré parti des nouvelles technologies aussi promptement que les criminels.

28. Les difficultés en matière de détection et de répression des infractions liées à la drogue peuvent être classées en quatre catégories: structurelles/liées aux mentalités; juridiques; techniques/matérielles; relatives à la vie privée/à la liberté d'expression.

### **Questions structurelles/liées aux mentalités**

29. À la fin de la guerre froide, les services de répression et de renseignement ont été contraints d'entreprendre des réformes structurelles et une révision de leurs priorités, processus qui n'est pas encore entièrement achevé. Aujourd'hui, la lutte contre la criminalité liée à la drogue au niveau transnational exige un nouveau bond en avant, qui suppose de faire évoluer non seulement les structures, mais aussi les mentalités, c'est-à-dire d'adopter une approche globale. Les organes de répression sont traditionnellement des structures hiérarchiques opérant à l'intérieur de délimitations géographiques claires. La criminalité transnationale liée à la drogue remet en cause cette approche, en partie parce que ses opérations ne se limitent pas à un seul territoire, et en

partie parce qu'elle est maintenant dominée par des réseaux dont la structure est peu visible.

30. La libéralisation du secteur des télécommunications a eu, en matière de lutte contre la criminalité, des répercussions non souhaitées, qui obligent les gouvernements à relever un défi ardu: essayer de contrecarrer l'usage illicite des télécommunications sans amoindrir les avantages, maintenant indispensables pour l'économie, que procure leur utilisation licite. Les stratégies traditionnelles des services de police et d'enquête sont paralysées par l'absence d'un cadre de coopération conceptuel et pratique, à l'intérieur duquel des mesures pourraient être prises contre la criminalité de haute technologie. Il s'agit encore d'un domaine flou, dans lequel les infractions sont mal définies et où il est difficile d'identifier et de localiser leurs auteurs.

31. Pour faire face à ces problèmes, les services de répression antidrogue devront définir de nouvelles formes de coopération, adopter de nouvelles stratégies et se doter de nouvelles compétences professionnelles, ce qui aura d'importantes incidences financières. Ils doivent mettre sur pied des réseaux opérationnels et fonctionnels au niveau mondial, s'ils veulent réussir à démanteler de manière efficace les organisations de trafiquants de drogues. Ils devront aussi établir des relations en matière de renseignement et en matière opérationnelle avec d'autres services de détection et de répression pour éviter des chevauchements et un gaspillage des ressources. Bien que l'on ait commencé à le réduire, l'écart entre les capacités des criminels et les capacités d'enquête est encore on ne peut plus évident.

### Questions juridiques

32. La faiblesse la plus flagrante à laquelle sont confrontés les services de répression en matière juridique est l'absence de législation globale concernant les infractions commises dans un environnement électronique. Certains pays n'ont pris aucune disposition dans ce domaine d'autres ont adopté des mesures qui ont été intégrées maladroitement dans la législation existante, et relativement peu ont mis à jour comme il convenait leur code pénal. Et, même s'ils promulguent une législation au niveau national, les gouvernements continueront à se heurter à de nombreux problèmes s'ils ne prennent pas, dans le même temps, des mesures

adaptées à la dimension transnationale de la criminalité de haute technologie, qui peut prendre naissance dans un pays et avoir des conséquences dans un deuxième, et dont les traces peuvent être réparties dans beaucoup d'autres. Il n'existe actuellement aucune règle indiquant quelle législation nationale devrait prévaloir pour poursuivre l'auteur d'une infraction, comment les décisions de justice peuvent être exécutées si les prévenus résident à l'étranger et quels protocoles régissent les enquêtes internationales<sup>16</sup>.

33. Deux enquêtes ont montré que beaucoup de pays n'étaient pas préparés à faire face à la criminalité de haute technologie. Selon une enquête, effectuée par une société de conseil en gestion sur la législation en matière de criminalité de haute technologie dans 52 pays du monde entier, 33 n'avaient procédé à aucune mise à jour de leur législation, 9 avaient promulgué une législation partielle, jugée incomplète, et 10 avaient adopté une législation permettant d'engager des poursuites contre les auteurs des formes les plus graves de cybercriminalité<sup>17</sup>. Parmi ceux qui avaient mis à jour leur législation, certains, comme les Philippines, ne l'avaient fait qu'après un événement marquant, à savoir l'attaque par le virus "ILOVEYOU", qui avait infecté 80 % des ordinateurs du Gouvernement fédéral des États-Unis et occasionné des dommages estimés à 10 milliards de dollars. L'auteur de cette attaque avait été retrouvé dans une banlieue de Manille, mais comme aucune loi, aux Philippines, n'interdisait ce genre d'activité, il n'avait pu ni être tenu responsable des dommages occasionnés, ni être extradé vers les États-Unis pour y être jugé<sup>18</sup>.

34. En Europe occidentale, les réponses à un questionnaire sur les infractions liées à la drogue commises par l'intermédiaire d'Internet ont montré que, d'une manière générale, les gouvernements n'avaient pas promulgué de législation spécifique visant ces infractions et que quand il y avait une coopération entre les services de répression et les fournisseurs de services sur Internet, c'était sur une base volontaire et informelle. Dans la plupart des pays, les fournisseurs de services Internet opéraient en dehors d'un cadre juridique spécifique et étaient peu contrôlés, voire pas du tout. Internet avait été utilisé principalement pour communiquer et échanger des informations sur la production et la vente illicites de drogues. Pratiquement aucun pays n'avait enregistré de cas de trafic de drogues où les trafiquants avaient communiqué par l'intermédiaire d'Internet, mais

certaines ne disposaient pas d'informations suffisantes pour évaluer le phénomène. Dans tous les pays, sauf deux, il y avait eu un recours au chiffrement par des criminels dans d'autres domaines. Presque tous les pays avaient un point de contact pour l'échange d'informations sur les infractions commises par l'intermédiaire d'Internet, mais celui-ci variait selon les pays: police, douanes, télécommunications et groupes de recherche sur les délits informatiques.

35. La localisation et la saisie des preuves ainsi que les règles relatives à la recevabilité de la preuve sont des questions essentielles. Vu la procédure à suivre pour demander et obtenir des mandats de perquisition dans plusieurs pays et le délai nécessaire pour les exécuter – ce qui pose déjà suffisamment de problèmes –, il peut être impossible d'intervenir en temps réel, ce qui permet aux auteurs des infractions de détruire ou de faire disparaître des pièces à conviction, par exemple la preuve d'une vente de drogue. D'autres problèmes tiennent à la nature des données électroniques. Les procédures à suivre pour obtenir l'autorisation de consulter des données stockées (au su du suspect) et l'autorisation d'intercepter des données (à son insu) sont variables, ces dernières étant soumises à des contrôles plus rigoureux. Toutefois, des données électroniques telles que le courrier électronique constituent à la fois des données stockées et des données en cours de transmission<sup>19</sup>. Un examen des normes juridiques dans ce domaine paraît indispensable.

36. La recevabilité par un tribunal de preuves d'infractions commises par voie électronique pose un problème particulièrement difficile du fait que les données électroniques peuvent être modifiées sans laisser de trace. Les services de répression devront établir des procédures transparentes et sûres permettant de prouver l'authenticité des données électroniques transcrites sur papier. Si ce processus nécessite un décodage, il faudra redoubler de précautions pour veiller à ce que les autorités chargées des poursuites ne puissent être accusées d'avoir altéré des éléments de preuve. Il est en outre difficile d'établir l'authenticité du contenu et de l'origine des données sans dévoiler en audience publique (et donc aux criminels) les techniques et méthodes employées pour lire ce contenu.

### Questions techniques et matérielles

37. Les questions techniques et matérielles auxquelles se heurtent les organes de répression dans leur lutte contre la criminalité de haute technologie liée à la drogue sont considérables. Pour ne pas se laisser distancer par la technologie, il leur faut constamment moderniser leur matériel, recycler leur personnel et maintenir 24 heures sur 24, 7 jours sur 7, des points de contact de façon à pouvoir enquêter en temps réel. Pour de nombreux pays en développement, cela peut représenter une charge très lourde, qui risque de se traduire par un écart croissant entre les capacités criminelles et les capacités d'enquête. Certains de ces pays risquent de devenir des "paradis des données" où les délinquants trouveront des fournisseurs de services et stockeront leurs données les plus sensibles, et où les données chiffrées seront hors d'atteinte des organes de répression. Les pays qui n'équipent pas de manière adéquate leurs services de répression ou dans lesquels le niveau de sécurité électronique est médiocre risquent d'être ignorés des sociétés de commerce électronique et d'être, de ce fait, désavantagés sur le plan économique ou encore de voir leurs messages électroniques bloqués par le reste du réseau<sup>20</sup>. Même les pays développés connaissent une pénurie d'enquêteurs et de magistrats du ministère public ayant les compétences voulues, d'autant que les rémunérations dans le secteur public sont toujours inférieures à celles offertes dans le secteur privé.

### Chiffrement

38. Le chiffrement peut être considéré par les services de répression à la fois comme une bénédiction et comme une malédiction. Il facilite le commerce électronique en assurant des conditions de sécurité relativement bonnes, il permet de protéger la vie privée et, combiné à l'utilisation de signatures numériques, il contribue à empêcher l'accès non autorisé aux systèmes d'information. Il est également très utile aux services de répression pour leurs communications et pour la protection de leurs sources et de leurs données. Pour nombre d'entre eux, toutefois, ces avantages semblent de peu de poids devant la protection que le chiffrement offre aux criminels.

39. Faute de pouvoir intercepter et comprendre les communications, les efforts des services de répression en matière de prévention, de détection et de poursuites sont, en grande partie, vains. Dès 1994, il a été indiqué

que dans toutes les enquêtes importantes sur la criminalité organisée menées aux États-Unis, le Federal Bureau of Investigation avait fait appel à la surveillance électronique<sup>21</sup>. Au Royaume-Uni, en 1996 et 1997, l'interception des communications a joué un rôle – souvent crucial – dans des opérations qui ont conduit à 1 200 arrestations et à la saisie de 115 tonnes de drogues et de plus de 450 armes à feu<sup>22</sup>.

### **Questions relatives à la vie privée et à la liberté d'expression**

40. Dans toutes les démocraties, la nécessité pour les services de répression d'enquêter sur la vie privée des suspects afin de prévenir ou de détecter des infractions doit être mise en balance avec le respect de la propriété privée et des communications. À mesure que progresse l'élaboration d'une législation sur la cybercriminalité, la conciliation de ces deux aspects se révèle difficile, d'autant que la position d'un secteur économique puissant doit être considérée au même titre que celle des groupes de citoyens et des services de répression. Trouver une solution en la matière constitue un autre défi majeur dans le cadre de la lutte contre la criminalité liée à la drogue. Les dispositions législatives récentes concernant le stockage des données vont dans le sens d'une plus grande protection de la vie privée et des données personnelles, les fournisseurs de services sur Internet n'étant généralement pas autorisés à conserver des informations sur leurs clients plus longtemps qu'il n'est nécessaire aux fins de la facturation. Les obliger à conserver de telles données aux fins d'enquêtes criminelles est délicat, tant du point de vue du respect de la vie privée que des incidences financières, et constitue un motif de préoccupation aussi bien pour les entreprises que pour les groupes de défense des libertés publiques.

41. L'utilisation d'Internet pour échanger des "recettes" de drogues et pour envoyer des messages faisant l'apologie de l'usage de drogues illicites pose des problèmes d'une autre nature aux services de répression: d'une part, l'incitation publique à produire ou à consommer des drogues constitue une violation de l'article 3 de la Convention de 1988; d'autre part, de nombreux États considèrent la liberté d'expression comme un droit inaliénable et refusent toute censure des communications. L'offre non autorisée de stupéfiants, de substances psychotropes ou de précurseurs à la vente devrait donner lieu à des

poursuites dans tout État partie aux traités internationaux relatifs au contrôle des drogues. L'offre de conseils sur la manière de se procurer des drogues ou des précurseurs à des fins illicites devrait également être considérée comme un encouragement ou une incitation, en violation de l'article 3 de la Convention de 1988. Toutefois, un site Web qui, par exemple, débat de la légalisation de l'usage des stupéfiants à des fins non médicales n'entre pas nécessairement dans cette catégorie, et l'interdiction de ce genre de sites pourrait, dans de nombreux pays, aller à l'encontre du principe de la liberté d'expression.

42. S'agissant d'infractions liées au contenu commises par l'intermédiaire d'Internet, le seul domaine dans lequel des progrès ont été réalisés est celui de la lutte contre la pornographie mettant en scène des enfants, mais cela n'a été possible que parce que les activités en question ont été universellement condamnées et que la simple possession d'images constitue, en la matière, un délit dans de nombreux pays. Dans de tels cas, la responsabilité juridique des fournisseurs de services sur Internet est engagée s'il peut être démontré qu'ils fournissaient sciemment un accès à des sites Web présentant de telles images. Les infractions liées à la pornographie enfantine sont les seuls actes criminels relatifs au contenu auxquels il est fait référence dans le projet de convention sur la cybercriminalité du Conseil de l'Europe<sup>23</sup> (voir par. 65 ci-après).

### **C. Défis futurs**

43. À la lumière de l'analyse qui précède et des événements de portée mondiale récemment survenus, l'Organe estime que l'on peut s'attendre aux développements suivants si aucune mesure n'est prise aux niveaux national et international:

a) *Les occasions de se livrer à toutes les formes de criminalité pourraient se multiplier* à mesure que les communications, les services financiers et le commerce en ligne se développeront. La croissance et l'interdépendance des économies nationales permettront aux organisations criminelles de fonder plus facilement leurs opérations dans l'activité économique légitime;

b) *La criminalité transnationale, facilitée par les réseaux, pourrait augmenter;*

c) *La criminalité organisée pourrait continuer à exploiter les progrès technologiques à des fins offensives et défensives.* Le “guerrier informatique” deviendra indispensable dans les groupes criminels organisés;

d) *Le blanchiment d’argent électronique pourrait augmenter* avec le développement des sociétés de services financiers en ligne, en particulier si la priorité accordée aux mesures de lutte contre le blanchiment de l’argent reste faible et si les sociétés offshore continuent à offrir anonymat et protection contre les enquêtes. Les opérations bancaires clandestines jouiront également d’une plus grande sécurité grâce aux technologies de l’information;

e) *La narcocriminalité pourrait progresser;* elle sera le fait d’un plus grand nombre de personnes, dont beaucoup ne seront pas membres d’un groupe criminel organisé et ne correspondront à aucun profil criminel;

f) *Les délits informatiques pourraient être de plus en plus souvent commis par des mineurs,* les nouvelles générations maîtrisant l’informatique de plus en plus tôt;

g) *Les organisations criminelles pourraient mettre à profit les progrès scientifiques pour investir davantage dans la production de drogues synthétiques destinées au marché illicite;*

h) *Les services de répression pourraient être de moins en moins capables de mener des activités d’interception et de surveillance* à mesure que les organisations de trafiquants de drogues auront davantage recours au chiffrement et à d’autres moyens de dissimulation;

i) *Les États n’ayant pas de législation appropriée pour lutter contre la criminalité liée aux technologies de l’information pourraient devenir des refuges pour cette dernière;*

j) *Les dispositifs traditionnels d’extradition et d’entraide judiciaire pourraient être poussés à leurs limites.*

## **D. Comment faire face à ces problèmes**

### **Nouvelles méthodes de lutte contre la criminalité de haute technologie appliquées au sein des structures de répression et dans le cadre de leur coopération**

44. Les polices nationales de plusieurs pays, dont le Canada, les États-Unis et le Royaume-Uni ont mis sur pied des services chargés exclusivement de la cybercriminalité. La Région administrative spéciale de Hong Kong (Chine), a renforcé ses capacités de renseignement et de répression au niveau international et créé une division pour la criminalité de haute technologie comprenant 76 agents spécialisés lutter contre cette criminalité à l’échelon national.

45. La Police fédérale australienne a mis au point un nouveau système de gestion en ligne des enquêtes appelé PROMIS (Police Realtime Online Management Information System). Ses bureaux de liaison dans le monde entier utilisent ce système pour échanger en temps réel avec leurs collègues des données, des photographies et d’autres informations relatives aux enquêtes.

46. En Espagne, le service central d’enquête sur les délits informatiques et le département des délits de haute technologie du Ministère de l’intérieur jouent un rôle actif dans la prévention de l’utilisation d’Internet pour proposer illicitement à la vente des substances placées sous contrôle, notamment des substances psychotropes. Le plan national antidrogue pour 2004-2008 prévoit la création d’un organisme chargé d’observer l’utilisation des nouvelles technologies, notamment l’Internet, par les organisations de trafiquants de drogues.

### **Utilisation des techniques de pointe pour lutter contre la criminalité liée à la drogue**

47. Depuis 1997, année où l’Organe a commencé à appeler l’attention des gouvernements sur le fait que les médias électroniques étaient utilisés pour diffuser des messages faisant l’apologie de l’usage de la drogue<sup>24</sup>, de nombreuses autorités sanitaires utilisent Internet comme un moyen rapide et économique de diffuser des informations concrètes sur les drogues et leur abus.

48. Aux États-Unis, le Counterdrug Technology Assessment Center de l’Office of National Drug

Control Policy finance des travaux scientifiques et technologiques de recherche-développement au profit des services de détection et de répression en matière de drogues. De nouvelles méthodes ont été mises au point pour analyser les effets des drogues sur l'être humain et détecter la présence de drogues dissimulées à l'intérieur ou à l'extérieur du corps, dans des conteneurs, des moyens de transport ou d'autres espaces clos. Les services des douanes et d'inspection des chargements disposent actuellement de moyens d'inspection non intrusifs, tels que des détecteurs à rayons X et à rayons gamma perfectionnés, des moyens portables ou transportables pour détecter la présence de drogues dans les navires, les compartiments et les conteneurs de toutes tailles lors d'inspections en mer et à quai, et des techniques de contrôle rapides et non invasives pour les personnes et les bagages.

49. Des programmes spéciaux de criminalistique informatique permettent d'appliquer l'informatique et les techniques de saisie et de traitement des éléments de preuve, pour rechercher des informations à partir de systèmes informatiques à des fins d'enquêtes et de renseignement. Des logiciels sont capables de rechercher des mots ou expressions clés dans des trains de données ou de "renifler" des portions de communications électroniques qui correspondent à des critères de filtrage définis conformément à une décision de justice, par exemple les messages provenant d'un compte ou d'un utilisateur particulier ou qui lui sont destinés<sup>25</sup>. Des dispositifs de protection de l'intégrité permettent d'améliorer les programmes en indiquant sur les éléments de preuve comment ceux-ci ont été recueillis, pour montrer que ni les filtres ni les informations obtenues n'ont été modifiés. Ce type de dispositif renforce la preuve de l'authenticité et de l'intégrité de la "chaîne de responsabilité"<sup>26</sup>.

50. Les autres utilisations novatrices qui sont faites des techniques existantes concernant notamment la mise au point de modèles informatiques sophistiqués pour repérer en ligne des anomalies survenant dans le cadre d'opérations financières, la conception de logiciels pour ordinateurs ultrarapides permettant de vérifier l'identité de trafiquants de drogues à partir de leurs empreintes digitales et la constitution de réseaux grâce auxquels les services compétents peuvent rapprocher les données d'enregistrement de la propriété de biens d'autres données, comme celles qui figurent dans les déclarations d'impôt sur le revenu.

L'avantage que les outils de haute technologie confèrent apparemment aux criminels peut ainsi être exploité au profit des services de répression.

### **Évolution dans le secteur privé**

51. Le secteur privé a commencé à conclure des alliances avec les services de répression afin d'améliorer les moyens de lutte et de protection contre la criminalité de haute technologie. Les fournisseurs d'accès à Internet ont établi des réseaux internationaux de coopération avec les services de répression par le biais d'associations assurant un service de téléassistance, qui collaborent pour lutter contre la diffusion sur Internet de matériels pornographiques impliquant des enfants. Si du matériel de cette nature est repéré, le service de téléassistance le localise et, s'il se trouve sur place, demande à la police et/ou aux fournisseurs d'accès de le retirer, à l'aide de procédures de notification et de manipulation précises<sup>27</sup>. De nombreux pays ont des systèmes nationaux similaires.

52. Aux États-Unis, la collaboration entre le secteur privé et le secteur public permet aux services de répression d'échanger des informations sur les intrusions via Internet, les points faibles exploités et les autres menaces qui pèsent sur les propriétaires ou opérateurs d'infrastructures vitales telles que les installations de production d'électricité.

### **Réglementation des contenus**

53. Il existe divers moyens de réglementer l'accès à Internet et, par conséquent d'en contrôler les contenus. Les sites Web peuvent être complètement bloqués par la censure, comme c'est le cas dans les pays où l'État contrôle l'accès à Internet. Ailleurs, les fournisseurs d'accès à Internet ou bien les administrateurs de sites Web peuvent être tenus pénalement responsables s'ils diffusent, sciemment, du matériel considéré comme illicite ou préjudiciable en vertu de l'une quelconque des lois du pays hôte, y compris les lois sur la drogue. Les fournisseurs d'accès à Internet peuvent réglementer le contenu des sites qu'ils hébergent en introduisant volontairement des codes de bonne pratique, comme c'est le cas en Italie et au Japon, ou en établissant entre fournisseurs d'accès et administrateurs de sites Web des accords juridiquement contraignants qui précisent quelle est la juridiction compétente en cas de recours. Un fournisseur d'accès

canadien établit des contrats de louage de services avec les utilisateurs et les sites Web pour définir les conditions en ligne; les lois canadiennes sont appliquées au contenu des sites et les utilisateurs sont informés de cette politique.

54. Les utilisateurs ont la possibilité de trier le contenu d'Internet au moyen de logiciels disponibles dans le commerce qui bloquent ou filtrent tout contenu indésirable selon des critères spécifiés. Il existe de nombreux logiciels de ce type, dont certains comprenant des systèmes de notation et des processus d'enregistrement des plaintes. Une société de services et de conseil en informatique, aux États-Unis, filtre le contenu d'Internet selon sa propre liste de sites qui est constamment mise à jour: elle a établi une liste noire où figurent plus de 60 000 sites jugés inconvenants pour diverses raisons, dont l'incitation à la consommation de drogues illicites.

#### **Initiatives internationales et régionales contre la criminalité de haute technologie**

55. La criminalité de haute technologie liée à la drogue est un phénomène encore relativement nouveau, et peu de pays disposent de moyens pour mesurer son étendue ou son impact, d'où l'absence d'initiatives spécifiques pour la contrer. Toutefois, des organisations internationales et régionales telles que l'ONU, le Groupe des Huit, Interpol et le Conseil de l'Europe ont commencé à déployer de sérieux efforts pour faire face à la criminalité de haute technologie en général<sup>28</sup>. Ces initiatives offrent un modèle opérationnel pouvant inspirer des actions visant la criminalité de haute technologie liée à la drogue.

56. Depuis 1990, La Commission pour la prévention du crime et la justice pénale s'emploie activement à promouvoir les efforts internationaux en vue de l'élaboration d'un vaste ensemble de principes directeurs et de normes pour aider les États à lutter contre les délits liés à l'informatique. Ces efforts comprennent la publication en 1994, d'un manuel sur la prévention et la répression de la criminalité informatique<sup>29</sup>, qui contient des propositions en vue de l'harmonisation du droit positif et du droit procédural ainsi qu'un plaidoyer en faveur de la coopération internationale dans ce domaine. Des réunions d'experts ont eu lieu sous les auspices de l'Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient afin de préparer l'atelier

consacré au thème "Délits liés à l'utilisation du réseau informatique", qui s'est tenu à Vienne le 15 avril 2000 dans le cadre du dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants<sup>30</sup>.

57. Conformément à la résolution 1999/23 du Conseil économique et social, le Secrétaire général a mené une étude sur les mesures efficaces à prendre pour prévenir les délits liés à la haute technologie et à l'informatique et lutter contre ces délits. Plusieurs options sont envisagées dans ce rapport, dont l'élaboration d'un instrument international contre les délits informatiques ainsi qu'une stratégie à plus court terme, avec notamment la mise en place d'un programme mondial des Nations Unies contre les délits liés à la haute technologie et à l'informatique<sup>31</sup>. En septembre 2001, la Commission pour la prévention du crime et la justice pénale a adopté une série de plans d'action concernant la mise en œuvre et le suivi des recommandations issues du dixième Congrès. Le plan d'action contre les délits liés à la haute technologie et à l'informatique prévoyait, entre autres, des mesures nationales en vue de: a) criminaliser l'utilisation à mauvais escient des technologies de l'information; b) mettre au point et appliquer des règles et procédures propres à faciliter la détection et l'investigation des délits liés à la haute technologie et aux télécommunications; et c) faire en sorte que le personnel des services de répression soit dûment formé et équipé pour pouvoir répondre aux demandes d'assistance pour tracer les communications.

58. Interpol a accueilli en 1995 une conférence internationale sur la criminalité informatique et publié des manuels à l'intention des enquêteurs dans ce domaine, afin de définir les normes relatives aux enquêtes techniques. Une unité centrale (de coopération policière) et quatre groupes de travail sur la criminalité de haute technologie – représentant l'Afrique, les Amériques, l'Asie et l'Europe – ont été créés, avec pour objectif premier d'assurer la formation et la coopération au niveau régional. La sous-direction des drogues d'Interpol gère un site Web sécurisé accessible aux bureaux nationaux qui porte à l'attention des services de police, en temps réel, les saisies de nouvelles drogues, les trafics détectés et autres mises en garde. La sécurité des récents projets de lutte contre le trafic de drogues a été assurée grâce au chiffrage des communications entre les membres de l'équipe. Interpol coopère également avec le secteur

privé afin de protéger les entreprises commerciales et industrielles des cyberattaques.

59. À Lyon (France), en juin 1996, les chefs d'État et de gouvernement du Groupe des Huit ont adopté les 40 recommandations du Groupe d'experts de haut niveau sur la criminalité transnationale organisée. Dans la recommandation 16, les États étaient instamment priés de réviser leur législation pour faire en sorte que les délits commis en utilisant des technologies modernes qui méritent des sanctions pénales donnent lieu effectivement à des poursuites judiciaires et que les incidences techniques et en termes de ressources de ce mécanisme soient dûment prises en compte. En janvier 1997, le Groupe de Lyon a été créé afin de donner suite à cette recommandation. À la réunion des Ministres de la justice et de l'intérieur des Huit tenue à Washington en décembre 1997, les participants se sont mis d'accord sur des principes et un plan d'action pour lutter contre la criminalité de haute technologie, qui recommandent instamment aux États l'adoption de législations pour enquêter sur les délits de haute technologie et en poursuivre les auteurs, et renforcer les régimes internationaux d'extradition et l'entraide judiciaire. Les participants sont également convenus de la nécessité d'une approche commune pour s'attaquer au problème de la criminalité de haute technologie. Le Plan d'action demandait également que soient créés des organes internationalement reconnus chargés d'élaborer des normes pour fournir aux secteurs public et privé des normes de fiabilité et de sécurité pour les technologies des télécommunications et du traitement des données<sup>32</sup>.

60. Au début de 2001, les services de détection et de répression des membres du Groupe des Huit et de neuf autres États avaient des contacts quotidiens et échangeaient des informations par l'intermédiaire d'un réseau "24/7", accessible 24 heures sur 24 et 7 jours sur 7, qui a permis de mener à bien des enquêtes sur des infractions graves liées à l'utilisation de la haute technologie. Le Groupe de Lyon a également accueilli, en novembre 1998, une conférence internationale sur la criminalité informatique en vue de former les enquêteurs des services de détection et de répression des membres du Groupe des Huit. Il a élaboré des procédures standard relatives à l'accès transfrontière à des données informatiques stockées et à l'exécution rapide, en matière administrative, des demandes d'entraide judiciaire, et il s'emploie à mettre au point

des méthodes permettant de tracer les communication<sup>33</sup>.

61. Bien que la drogue ne soit dans la plupart des affaires qu'un élément marginal, dans toutes les régions du monde, on met au point des mécanismes permettant d'étudier la criminalité de haute technologie et de trouver les ripostes appropriées. Dans certaines régions, l'accent a été mis sur la lutte contre la fraude, la pornographie mettant en scène des enfants et le piratage informatique; dans d'autres, les principaux sujets de préoccupation sont le blanchiment d'argent et les crimes et délits économiques. Compte tenu des événements qui se sont produits récemment dans le monde, une attention particulière est actuellement accordée à l'utilisation des technologies nouvelles par les réseaux terroristes.

62. Le Gouvernement japonais, par l'intermédiaire de l'Agence nationale de la police, finance un réseau de contacts sur Internet regroupant 21 pays d'Asie, qui permet d'échanger des informations sur la criminalité de haute technologie. Huit pays participent déjà à la première phase de cette initiative.

63. Une étude sur la criminalité de haute technologie – dont le Conseil européen avait recommandé la réalisation (orientation politique n° 5) dans les 30 orientations politiques pour lutter contre la criminalité organisée adoptées en juillet 1997 – a été achevée en janvier 1998. À une réunion spéciale du Conseil européen tenue à Tampere (Finlande) en octobre 1999, les chefs d'État et de gouvernement des membres de l'Union européenne ont conclu que la criminalité utilisant les technologies avancées devait figurer au nombre des domaines dans lesquels il convenait de trouver des définitions et des sanctions communes. Dans le cadre du plan d'action antidrogue (2000-2004) de l'Union européenne, un groupe de travail sur le trafic des drogues dépendant du Conseil des ministres a évalué début 2001 la menace que fait peser l'utilisation d'Internet à des fins illicites liées aux drogues et examiné les dispositions juridiques qui existent dans les États membres. L'envoi par l'Office européen de police (Europol) d'un questionnaire (voir plus haut, par. 34) aux États membres constituait la première étape de cette analyse. La Commission européenne examinera comment renforcer l'efficacité des mesures prises pour lutter contre le trafic de drogues illicites sur Internet, dont l'ampleur a été

relevée dans la stratégie 2000-2004 de l'Union européenne.

64. En janvier 1999, le Parlement européen et le Conseil de l'Union européenne ont adopté un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux<sup>34</sup>.

65. La Convention du Conseil de l'Europe sur la cybercriminalité est à ce jour l'initiative la plus avancée en matière de collaboration internationale dans le domaine de la criminalité de haute technologie. Les 43 États membres du Conseil, le Canada, les États-Unis et le Japon – qui ont le statut d'observateur – et l'Afrique du Sud, ont tous participé à l'élaboration du texte et pourront le signer. La Convention traite des questions suivantes: compétence, extradition, interception des communications et production et conservation des données. Elle énumère les actes devant être érigés en infractions pénales en vertu du droit interne, à savoir l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données ou des systèmes, la falsification informatique, la fraude informatique et la complicité dans la commission de ces infractions. Elle restaure un mécanisme détaillé de coopération et de coordination internationales en matière d'enquêtes et de poursuites. Les Parties à la Convention devront habiliter leurs autorités nationales à perquisitionner des ordinateurs et à saisir des données informatiques, à exiger des sujets de données qu'ils produisent les données qui se trouvent sous leur contrôle et à préserver l'intégrité ou obtenir la conservation rapide des données susceptibles de perte ou de modification. La Convention s'appliquera dans les affaires liées à la drogue pour mettre en œuvre l'entraide judiciaire; par exemple, des autorités recherchant des preuves électroniques sur les activités des trafiquants de drogues, leurs clients ou leurs avoirs dans un autre État pourront demander à cet État de perquisitionner les bases de données utilisées par les trafiquants présumés ou d'intercepter leurs communications électroniques, notamment le courrier électronique. La Convention devait être adoptée le 8 novembre 2001 et ouverte à la signature le 23 novembre 2001.

66. Toutefois, des entreprises privées et des groupes de citoyens ont désapprouvé certaines clauses de la Convention sur la cybercriminalité. Selon un

consortium rassemblant des associations d'entreprises des technologies de l'information, ladite Convention imposerait aux fournisseurs d'accès à Internet de lourdes contraintes en matière de conservation des données, les exposerait à des actions intentées par des tiers et restreindraient les activités légitimes sur Internet. Les groupes de défense des libertés publiques se sont également déclarés préoccupés par certaines mesures prévues par la Convention, qu'ils considèrent comme attentatoires à la vie privée. Néanmoins, l'Organe estime que ce type d'instrument juridique peut contribuer aux efforts menés pour lutter contre le trafic et l'abus de drogues.

## E. Conclusions et recommandations

### Conclusions

67. Les technologies de communication avancées étant le moteur de l'économie mondialisée d'aujourd'hui, l'on ne peut pas, et l'on ne devrait d'ailleurs pas, freiner leur développement ni leur évolution. Il faut reconnaître cependant que la mondialisation et les nouvelles technologies ont facilité certaines opérations criminelles liées à la drogue, imposant ainsi un fardeau supplémentaire aux services de détection et de répression. Bien que les entreprises et les services de détection et de répression collaborent souvent fort bien, les préoccupations du secteur public et du secteur privé ne coïncident pas toujours de toute évidence, étant donné que les entreprises se doivent de protéger la vie privée de leurs clients et les bénéficiaires de leurs actionnaires.

68. L'Organe a noté l'ensemble des efforts faits pour contrer la menace de la cybercriminalité en général. Bien que l'on se préoccupe surtout actuellement de la pornographie impliquant des enfants et des délits économiques tels que la fraude, le piratage et le vol de propriété intellectuelle, certains signes donnent à penser que l'utilisation des nouvelles technologies pour la fabrication illicite et le trafic des drogues prend de l'ampleur. C'est pourquoi l'absence de dispositions relatives à la drogue dans les lois existantes sur la cybercriminalité est un sujet de préoccupation. Si l'on veut résoudre les problèmes auxquels sont confrontés les services de détection et de répression, il faut un programme d'action aux niveaux national et international, dans le contexte des initiatives actuelles de lutte contre la cybercriminalité, programme d'action

qui aura pour objectif la prévention de la criminalité de haute technologie liée à la drogue. De nombreux pays en développement se tourneront instinctivement vers le système des Nations Unies et vers l'Organe pour obtenir des orientations d'ordre technique et législatif à cet effet.

69. En ce qui concerne le contenu relatif à la drogue des sites Internet, il est nécessaire d'utiliser des outils technologiques, d'appliquer des lois et d'informer, en particulier en ce qui concerne la mobilisation des parents et la responsabilisation des utilisateurs. Étant donné les problèmes que posent l'identification des innombrables sites Web faisant l'apologie de la drogue et les enquêtes sur ces sites, des logiciels de filtrage et de blocage peuvent grandement contribuer à empêcher l'utilisation d'Internet pour diffuser des messages favorables à l'usage de drogue et constituent peut-être une solution plus pratique et plus réaliste que le recours au droit pénal.

70. S'il est essentiel que les services de détection et de répression et les autres structures nationales responsables de la lutte contre la narcocriminalité se voient accorder les moyens techniques et législatifs leur permettant de se doter de la capacité d'intervention requise, cela ne suffit pas. L'Organe est convaincu que pour relever le défi en matière de répression antidrogue, il faut des partenariats entre les gouvernements, les entreprises de technologies de l'information et les citoyens, dont les divers intérêts doivent être reconnus et conciliés. Les craintes exprimées par les groupes de défense des libertés publiques quant aux atteintes à la vie privée et aux restrictions potentielles de la liberté d'expression sont légitimes et doivent être prises en compte.

71. Dans le cadre de la coopération entre les pouvoirs publics et les entreprises, la participation de ces dernières est nécessaire pour repérer les vulnérabilités, aider les services de détection et de répression à évaluer les menaces et contribuer à résoudre les problèmes qui apparaissent. Parallèlement, les entreprises doivent comprendre que l'autodiscipline et les moyens de coopération informels avec les services de détection et de répression ne suffisent pas nécessairement pour éviter le danger. Les événements qui se sont produits récemment dans le monde ont déjà eu de profondes répercussions en termes d'enquêtes et de poursuites relatives aux actes criminels, mais c'est seulement avec le temps qu'on saura leur impact

véritable dans ce domaine. À l'heure actuelle, on peut simplement affirmer que les services chargés de la détection et de la répression doivent de façon encore plus prioritaire se moderniser et s'adapter à des circonstances changeantes et à de nouveaux défis. Les nouvelles technologies doivent être considérées non comme un adversaire dans la lutte contre la narcocriminalité, mais comme des outils potentiels de prévention de la consommation, de la production, de la fabrication illicites et du trafic de drogues. L'Organe, en tant qu'institution chargée de veiller au respect des trois traités internationaux relatifs au contrôle des drogues dont les objectifs sont la santé et le bien-être de la société, propose que la société de l'information fasse l'objet d'une "tutelle partagée", dans l'idée de contribuer à son développement et à sa sécurité futurs.

### Recommandations

72. La tâche la plus urgente pour les gouvernements est de faire en sorte que des règles de fond et de procédure appropriées soient introduites dans leur droit interne pour lutter contre la criminalité informatique. Des circonstances aggravantes pourraient être retenues lorsque les infractions sont commises à des fins de trafic de drogues ou par un membre d'un groupe criminel organisé (au sens de la Convention des Nations Unies contre la criminalité transnationale organisée)<sup>35</sup>. Ces mesures devraient être autant que possible harmonisées afin que les infractions, les sanctions et les critères d'établissement de la preuve soient analogues dans le monde entier, de manière à empêcher la prolifération des cyberparadis. Une assistance devrait être fournie aux pays en développement considérés comme vulnérables à ce type d'exploitation.

73. Il faudrait donner aux services de détection et de répression en matière de drogues et aux autorités judiciaires les ressources et le matériel appropriés pour enquêter sur les délinquants qui ont recours aux technologies nouvelles dans leurs activités de trafic de drogues illicites et pour les identifier, les appréhender et les poursuivre.

74. Des services interinstitutions spécialisés dans la haute technologie devraient être mis en place au niveau national. La formule des réseaux "24/7" devrait être étendue à d'autres pays, l'idée étant qu'"il faut des réseaux pour combattre les réseaux". Ces services

devraient entretenir des relations de collaboration avec les autres organismes luttant contre la cybercriminalité.

75. Il faudrait protéger les infrastructures sensibles des organes de répression en matière de drogues pour mettre à l'abri des cyberattaques leurs bases de données et de renseignement.

76. Des fonds devraient être dégagés pour fournir aux décideurs et au personnel des services de détection et de répression et aux agents chargés des enquêtes le matériel et la formation appropriés dans les domaines de la police scientifique et de la technologie. Les gouvernements devraient faire le nécessaire pour recruter des spécialistes hautement qualifiés appelés à travailler dans les services de répression en matière de drogues.

77. Il faudrait faire en sorte que la Convention sur la cybercriminalité puisse être ratifiée dès que possible, et accorder un appui à d'autres initiatives dans ce domaine ailleurs dans le monde.

78. Les gouvernements devraient exiger que les pharmacies en ligne soient soumises à une autorisation d'exercer, où qu'elles se trouvent ou distribuent des médicaments sous ordonnance, et devraient mettre en place un système de surveillance de ce type d'activités. La vente en ligne de stupéfiants et de substances psychotropes devrait être purement et simplement interdite car elle tourne les systèmes nationaux et internationaux de contrôle existants.

79. Les gouvernements devraient contribuer à sensibiliser l'opinion publique, notamment parents et enseignants, aux dangers des messages prônant l'usage de la drogue que les jeunes peuvent trouver sur Internet et faire en sorte que soient en place les moyens technologiques nécessaires pour bloquer ou filtrer ce type de messages.

80. Les gouvernements devraient appuyer la création de sites Web fournissant des informations objectives et présentées de façon attrayante sur l'usage illicite de drogues, par exemple pour expliquer les lois visant le trafic ainsi que la possession, la consommation illicites de drogues dans un pays donné et décrire les drogues et leurs effets.

81. On pourrait envisager l'élaboration d'une convention des Nations Unies contre la cybercriminalité. Une telle convention fournirait une classification mondiale et une définition de la

criminalité de haute technologie et de la criminalité informatique ainsi qu'un cadre pour l'harmonisation des législations et la coopération internationale dans les enquêtes sur les infractions transfrontières commises par voie électronique ou facilitées par cette voie et la poursuite de leurs auteurs. Elle pourrait aussi comporter une section sur la criminalité liée à la drogue, rappelant aux gouvernements que toute forme de promotion des stupéfiants et des substances psychotropes doit être interdite. Cette convention devrait tenir compte à la fois des considérations de sécurité et de protection face à la criminalité et des considérations relatives aux libertés civiles, à la dignité et au respect de la vie privée.

82. Les fournisseurs d'accès à Internet devraient mettre en service des numéros d'urgence pour que le public puisse signaler tout contenu offensant ou illégal de sites Internet et comprendre que le contenu de certains sites Web ayant trait à la drogue peut enfreindre les dispositions des traités internationaux relatifs au contrôle des drogues.

83. Les institutions financières devraient revoir leurs méthodes de lutte contre le blanchiment de l'argent pour tenir compte de l'évolution technologique.