Nations Unies E/CN.15/2002/8

Conseil économique et social

Distr.: Générale
29 janvier 2002

Français
Original: Anglais

Commission pour la prévention du crime et la justice pénale
Onzième session
Vienne, 16-25 avril 2002
Point 5 de l'ordre du jour provisoire*
Coopération internationale en matière de lutte contre la criminalité transnationale

Mesures efficaces à prendre pour prévenir les délits liés à l'informatique et lutter contre ces délits

Rapport du Secrétaire général

Table des matières

* E/CN.15/2002/1.

V.02-50947

I. Introduction

1. À la reprise de sa dixième session, tenue les 6 et 7 septembre 2001, la Commission pour la prévention du crime et la justice pénale a adopté un plan d'action[1] concernant les mesures à prendre pour prévenir les délits liés à la technologie et à l'informatique et lutter contre ces délits pour donner suite au paragraphe 18 de la Déclaration de Vienne sur la criminalité et la justice: relever les défis du XXIème siècle, adoptée par le dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants.[2]

2. Dans sa résolution 56/121 du 19 décembre 2001, l'Assemblée générale, préoccupée par le fait que les progrès technologiques avaient créé de nouvelles possibilités d'activités criminelles, et en particulier d'utilisation des technologies de l'information à des fins criminelles, et reconnaissant quíl fallait faciliter un transfert de technologies informatiques, en particulier aux pays en développement, a souligné la nécessité de resserrer la coopération entre les États pour combattre les utilisations délictueuses des technologies de l'information et a mis en relief le rôle que l'Organisation des Nations Unies et les autres organisations internationales et régionales pouvaient jouer à cet égard. En outre, elle a accueilli favorablement les travaux accomplis par le dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants et féliciter la Commission pour la prévention du crime et la justice pénale de l'oeuvre qu'elle avait accomplie à ses neuvième et dixième sessions. Elle a cependant décidé de repousser l'examen de la question de l'utilisation des technologies de l'information à des fins criminelles en attendant que les travaux prévus par le plan d'action soient achevés.

3. Dans sa résolution 56/261 du 31 janvier 2002, l'Assemblée générale a pris note avec satisfaction des plans d'action qui avaient été élaborés, a demandé au Secrétaire général d'assurer à ces derniers la plus large diffusion, à inviter les gouvernements à les prendre soigneusement en considération pour guider la formulation de leurs législations, politiques et programmes, et a invité le Secrétaire général à étudier soigneusement les plans d'action et à les mettre en oeuvre selon qu'il conviendrait, conformément au plan à moyen terme et au budget-programme, et sous réserve des ressources disponibles.

II. État des efforts entrepris pour prévenir les délits liés à la technologie et à l'informatique et lutter contre ces délits

A. Tendances et conjoncture générales

4. La délinquance liée à la technologie et à l'informatique continue d'être caractérisée par une évolution rapide des agissements des délinquants, des efforts de prévention et de répression et des législations et des technologies sous-jacentes elles-mêmes. En 2001, plusieurs États se sont dotés de moyens législatifs et policiers spécialisés pour faire face à la criminalité liée à la technologie et à l'informatique et ont renforcé ceux dont ils disposaient déjà. Ainsi, les législations ont été réformées pour créer de nouvelles infractions, étendre la qualification des infractions existantes et moderniser les moyens d'enquête, notamment pour ce qui est des autorisations de perquisition et d'installation de tables d'écoute pour combattre efficacement la criminalité dans l'environnement nouveau constitué par l'électronique. Il est probable que cette tendance se poursuivra, surtout en Europe, où les États s'emploient actuellement à mettre en oeuvre la Convention relative à la cybercriminalité adoptée à Budapest par le Conseil de l'Europe le 23 novembre 2001.[3]

5. Dans de nombreux pays, la relation entre les efforts déployés par les pouvoirs publics pour maîtriser la criminalité et le rôle des entreprises du secteur privé dans la fabrication de matériel et la production de logiciels et dans la fourniture de services a continué d'être un sujet extrêmement controversé au niveau des politiques générales et de la législation ainsi qu'en ce qui concerne les pouvoirs d'enquête de la police. L'on s'est interrogé surtout sur le point de savoir dans quelle mesure des moyens de nature à faciliter la prévention du crime et des enquêtes devraient être incorporés aux nouvelles technologie, sur le coût des moyens de stockage, d'interception et de recherche des données dont souhaitaient se doter les services de répression et sur toute une série de questions concernant les politiques générales et la responsabilité pénale et civile liées à la relation entre l'État, les prestataires de services et les usagers. Après la série de virus destructeurs qui ont été lancés sur la Toile et les

interruptions de service causées par les cyberpirates en 1999 et 2000, plusieurs grandes entreprises de pointe ont créé et financé un Centre conjoint à but non lucratif, le Technology Information Sharing and Analysis Centre, pour conjuguer leurs efforts, au-delà de la concurrence qu'elles se font, pour combattre la cybercriminalité. Ces grandes sociétés ont accordé une priorité plus élevée à l'incorporation de mécanismes de sécurité aux nouveaux logiciels, non seulement pour réduire leur propre vulnérabilité à des attaques de cyberpirates, mais aussi parce que la crainte suscitée par la délinquance et la présence de mécanismes de sécurité efficace était devenue des éléments pesant beaucoup dans la décision des acheteurs de nouveaux produits.

6. Les techniques de sécurité et méthodes de prévention de la délinquance ont continué d'être de plus en plus largement utilisées en 2001 parallèlement à l'expansion continue des nouvelles technologies et manque d'efficacité des législations et des méthodes policières traditionnelles, en particulier dans les affaires comportant un élément transnational. C'est ainsi qu'il a été mis au point des programmes permettant d'identifier et d'éliminer des programmes hostiles comme vers et virus des données stockées et transmises et des logiciels "coupe-feu". Des programmes de "géolocalisation", qui identifient la source géographique des communications électroniques, ont été de plus en plus largement utilisés pour couper l'accès aux systèmes situés dans des pays où le jeu, la pornographique ou d'autres types d'activités sont illégaux. Cette évolution a été applaudie par les organismes chargés de l'application des lois mais critiquée par les partisans d'une ouverture totale de l'Internet et par les experts, qui ont fait observer que de tels programmes ne pouvaient être efficaces que si les opérateurs de sites web étaient disposés à les utiliser et savaient quelles étaient les restrictions juridiques imposées par d'autres pays. La plupart des experts sont également convenus que de tels programmes pouvaient efficacement empêché des atteintes accidentelles à la sécurité des communications et pouvaient constituer un obstacle pour des délinquants peu au fait de l'informatique mais pas contre des criminels ayant une meilleure connaissance de l'informatique, lesquels pouvaient facilement cacher l'endroit où ils se trouvaient réellement aux logiciels et opérateurs de sites web qu'ils utilisaient. L'utilisation de logiciels de filtrage, qui identifient et bloquent les communications qui ne sont pas pour les enfants ou auxquelles ne doivent pas avoir accès d'autres usagers non autorisés, a également été de plus en plus fréquente, et nombre d'opérateurs de sites web pour adultes y ont incorporé des mécanismes tendant à déclencher de tels logiciels. Des applications cryptographiques ont été utilisées aussi pour protéger des communications confidentielles et empêcher les usagers non autorisés à avoir accès à des données brevetées ou névralgique.

7. Par ailleurs, les organismes chargés de l'application des lois se sont rendus compte, de plus en plus, que les enquêteurs ayant la compétence nécessaire pour intercepter des communications numériques extra-rapides, faire des recherches dans les données stockées, déchiffrer des données et mener à bien d'autres tâches semblables étaient une ressource rare, précieuse et spécialisée. Nombre d'organismes ont maintenant créé des unités spécialisées pour aider les enquêteurs dans des domaines allant du contre-terrorisme au trafic de drogues et à la délinquance économique. Le coût élevé et l'investissement à long terme que suppose la formation des enquêteurs, la difficulté qu'il y a à fidéliser des enquêteurs qualifiés qui se voient offrir des traitements plus élevés dans des emplois du secteur privé et le simple problème consistant à faire en sorte que les enquêteurs se tiennent au courant des dernières technologies et des derniers stratagèmes employés par les criminels pour les exploiter représentent néanmoins des problèmes majeurs à cet égard.

8. Les États Membres se préoccupent des utilisations offensives et défensives que les organisations terroristes peuvent faire des technologies nouvelles, et cette crainte a été considérablement avivée par les événements du 11 septembre 2001. L'on sait déjà, en effet, que les organisations terroristes les mieux organisées utilisent déjà l'Internet pour communiquer. Dans ce contexte, des moyens perfectionnés de chiffrage et d'autres dispositifs de sécurité ont été utilisés pour protéger le caractère confidentiel des communications et des données stockées. Le risque l'Internet soit utilisé à des fins offensives pour des actes de terrorisme a également conduit plusieurs pays à créer des organismes spécialisés chargés de protéger contre les agissements des cyberpirates les infrastructures de traitement des données et de communications et les autres systèmes de pointe qui revêtent une importance critique.

9. Les enquêtes qui ont été ouvertes immédiatement après les événements de septembre ont également montré que l'Internet pouvait être utilisé pour obtenir des informations utiles pour planifier les attaques ou obtenir les matériaux nécessaires pour fabriquer ou improviser des armes chimiques, biologiques ou radiologiques. Plusieurs des États qui ont répondu à une enquête de l'Organisation des Nations Unies sur, entre autres, l'utilisation qui était faite des explosifs se sont dits préoccupés par le fait que l'on pouvait trouver sur l'Internet des informations sur la fabrication d'explosifs et de dispositifs explosifs;[4] et un individu arrêté pour avoir essayé de faire exploser un engin dissimulé dans ses chaussures à bord d'un vol commercial de Paris à Miami le 22 décembre 2001 a apparemment, selon les médias, déclaré aux enquêteurs qu'il avait fabriqué cet engin explosif au moyen d'informations obtenues sur l'Internet. Les services nationaux anti-drogues ont exprimé des préoccupations semblables, des informations pouvant facilement être obtenues sur l'Internet quant aux méthodes de fabrication de drogues synthétiques et aux fournisseurs auprès desquels l'on pouvait se procurer les ingrédients nécessaires.

10. D'autres types d'infractions liées à l'informatique et à la technologie ont également continué de susciter des préoccupations en 2001. Il y a lieu de citer en particulier l'utilisation de technologies numériques et de l'Internet pour produire et diffuser de la pornographie infantile. Plusieurs participants au Deuxième Congrès mondial contre l'exploitation sexuelle commerciale des enfants tenu à Yokohama (Japon) du 17 au 20 décembre 2001 ont considéré que le volume croissant de la pornographie infantile diffusée sur un réseau électronique de plus en plus vaste risquait d'aggraver l'exploitation des enfants[5] mais ont relevé que les services de répression avaient réussi, en coopérant entre eux, à démanteler plusieurs opérations à grande échelle de diffusion de pornographie infantile sur l'Internet, souvent d'envergure transnationale. Les études présentées lors du Congrès mondial ont également établi une corrélation entre l'Internet et d'autres activités pédophiles, comme le tourisme orienté vers l'exploitation sexuelle des enfants et les enlèvements d'enfants.

11. De plus en plus préoccupante aussi est la recrudescence du vol d'identité, c'est-à-dire de données personnelles que les délinquants utilisent pour effectuer des opérations au nom de l'intéressé et à son insu. Joint à l'anonymat des transactions et autres activités en ligne, le vol d'identités a été un stratagème utilisé pour toute une série de délits et de crimes allant de simples fraudes à des activités terroristes. Les autres activités criminelles signalées sont notamment une gamme de plus en plus large de délits comme fraude, extorsion de fonds en ligne, blanchiment d'argent, contrebande assistée par ordinateur, délits dirigés contre les systèmes informatiques et leurs utilisateurs au moyen de virus, de programmes hostiles et d'interruption de services. Un élément nouveau, en ce qui concerne la fraude, a été la création sur l'Internet de fausses organisations philanthropiques pour attirer des dons immédiatement après les attaques terroristes du 11 septembre, en profitant des délais de réaction rapides que rendent possibles la création et la suppression des nouveaux sites web.

12. Les activités sur l'Internet ont également créé un certain nombre de problèmes nouveaux pour les organismes nationaux de réglementation dans des domaines comme la fiscalité, la réglementation des affaires et l'application des normes environnementales étant donné que le stockage de données à l'étranger, le recours accru au chiffrage et la possibilité qu'ont les entreprises d'un pays de traiter directement avec des clients situés dans un autre ont rendu plus difficile l'application des normes de réglementation et des règles d'inspection et d'audit. L'on peut en citer comme exemple les pharmacies qui vendent leurs produits sur l'Internet, problème déjà relevé dans le rapport de l'Organe international de contrôle des stupéfiants[6] ainsi que par les experts du Conseil de coopération douanière (également Organisation mondiale des douanes) et par la Commission des stupéfiants. L'Organe international de contrôle des stupéfiants, quant à lui, se préoccupe surtout de l'expédition illicite de stupéfiants et de substances psychotropes, mais il ressort d'autres sources que le problème est plus large et s'étend à nombre de médicaments et autres drogues qui sont soumis à un contrôle douanier et qui ne peuvent être dispensés que sur ordonnance dans différents pays. Cela pose un problème non seulement pour les organes chargés de l'application des lois pénales mais aussi pour les autorités sanitaires, les services des douanes et les autres organes de réglementation.

B. Travaux réalisés sous l'égide de l'Organisation des Nations Unies

13. Dans sa résolution 1999/23 du 28 juillet 1999, intitulée "Activités du Programme des Nations Unies pour la prévention du crime et la justice pénale", le Conseil économique et social a prié le Secrétaire général, compte tenu des activités de l'atelier sur les délits liés à l'informatique tenu à l'occasion du dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, d'entreprendre une étude sur les mesures efficaces qui pourraient être prises aux échelons national et international pour prévenir et combattre les délits liés à l'informatique. Le rapport du Secrétaire général sur les conclusions de cette étude a été soumis à la Commission à sa dixième session (E/CN.15/2001/4). Plusieurs orateurs ont reconnu la gravité des délits liés à la technologie et à l'informatique et ont souligné que des mesures devraient être prises pour combattre ce type de délits au plan international, notamment dans le cadre de l'Organisation des Nations Unies. Il a été noté qu'il fallait pour combattre les délits liés à la technologie et à l'informatique d'introduire un certain nombre de techniques d'enquête perfectionnées et qu'il importait au plus haut point de suivre une approche commune pour combattre ce type de criminalité.

14. Les plans d'action joints en annexe à la résolution 56/261 de l'Assemblée générale relative à l'application et au suivi de la Déclaration de Vienne comprennent un plan d'action contre les délits liés à la technologie et à l'informatique, dans lequel le Centre pour la prévention internationale du crime a été prié:

a) D'appuyer les activités de recherche entreprises aux échelons national et international pour identifier les nouvelles formes de délinquance liée à l'informatique et d'évaluer les effets de cette délinquance dans des domaines d'importance capitale comme le développement durable, la protection de la vie privée et le commerce électronique ainsi que les mesures adoptées pour y faire face;

b) De diffuser des matériels d'information ayant fait l'objet d'un accord international comme directives, manuels juridiques et techniques, normes minima, pratiques éprouvées et lois types, pour aider les responsables de la formulation et de l'application des lois et les autres autorités compétentes à mettre au point, adopter et appliquer les mesures efficaces pour combattre la délinquance liée à la technologique et l'informatique et l'action des délinquants, aussi bien en général que dans des domaines déterminés;

c) De promouvoir, d'appuyer et de réaliser, selon qu'il conviendra, des projets de coopération et d'assistance techniques, notamment pour rassembler des experts de la prévention du crime, de la sécurité des systèmes informatique, du droit et des procédures pénales, des poursuites, des techniques d'enquête et des questions connexes et les États ayant besoin d'une assistance ou d'informations dans ces domaines.

15. Conformément au paragraphe 5 de la résolution 56/261, aux termes duquel l'Assemblée générale a prié le Secrétaire général d'étudier soigneusement et d'appliquer, le cas échéant, les plans d'action et notamment le plan d'action contre la délinquance liée à la technologie et à l'informatique, conformément aux plans à moyen terme et aux budgets-programmes et sous réserve des ressources disponibles, ainsi que compte tenu des observations formulées par la Commission à sa dixième session,[7] une étude plus détaillée des problèmes et des mesures envisagées dans le plan d'action sera entreprise dès que les ressources nécessaires seront disponibles.

16. L'utilisation croissante que les groupes de criminels organisés font des nouvelles technologies informatiques et des nouveaux moyens de télécommunications demeure fort préoccupante, en particulier lorsque cela est le fait d'organisations qui se livrent à la fabrication et au trafic de stupéfiants, lesquels sont parmi les groupes criminels les mieux structurés et les mieux financés et qui ont par conséquent accès aux meilleurs compétences et aux appareils les plus perfectionnés. L'informatique est en effet utilisée par les fabricants et trafiquants de drogues, tout comme le font les usagers commerciaux légitimes. Les informations concernant les livraisons de drogues sont transmis de l'expéditeur au destinataire par des moyens qu'il est difficile pour la police d'intercepter ou de lire. Le registre des transactions est tenu dans des pays étrangers, dissimulé parmi d'autres données volumineuses et protégé par des technologies comme murs coupe-feu et mécanismes de chiffrage pour les mettre à l'abri des enquêteurs. Les systèmes de suivi électronique des marchandises sont utilisés par les trafiquants pour contrôler le mouvement des marchandises parmi lesquelles sont dissimulés des drogues ou autres articles de contrebande et, en cas de

retard injustifié, pour lancer l'alarme pour le cas où l'expédition aurait été découverte et interceptée. L'anonymat relatif des virements électroniques de fonds est de plus en plus utilisée pour payer des expéditions sans attirer l'attention des services de répression, et est exploité aussi par les destinataires des paiements pour qu'ils puissent ensuite blanchir l'argent ainsi reçu. En outre, l'Internet est utilisé pour communiquer des informations de caractère général, comme des modes d'emploi pour la fabrication de drogues synthétiques ou des messages qui encouragent l'abus de drogues.

17. Dans son rapport du 21 décembre 2000 sur la situation mondiale en ce qui concerne le trafic illicite de drogues, le secrétariat a examiné le problème posé par la délinquance électronique et a formulé une recommandation tendant à ce que les gouvernements élaborent des politiques nationales pour appuyer les efforts entrepris par les services de répression pour combattre ce phénomène (E/CN.7/2001/5, par. 150). Les services de répression ont été invités à se tenir en contact avec les prestataires de services pour veiller à ce que ces derniers conservent les données pertinentes assez longtemps pour qu'elles puissent être récupérées aux fins d'enquête, ainsi qu'à travailler la main dans la main pour combattre le blanchiment d'argent par l'Interne. En janvier 2002, un organe subsidiaire de la Commission, la Réunion des chefs des services nationaux pour l'application des lois relatives à la drogue en Europe, a organisé une réunion régionale d'experts pour étudier les problèmes rencontrés par les services de répression lorsqu'ils se trouvaient en présence de nouvelles technologies dans leurs enquêtes. Les problèmes identifiés par le groupe étaient notamment le volume énorme des données stockées et transmises parmi lesquelles il fallait identifier et retrouver des informations critiques; le fait que les services de répression étaient de plus en plus tributaires des prestataires de services pour rechercher ou intercepter des données et les incidences de cette situation sur le plan des coûts et de la sécurité; et l'apparition de toute une série de technologies nouvelles comme les téléphones cellulaires numériques, les téléphones par satellite, les salons de discussion sécurisés sur l'Internet, qu'il était plus difficile d'intercepter que les méthodes de communication établies. Les experts se sont dits particulièrement préoccupés par le lancement sur le marché de systèmes de chiffrage perfectionnés qui rendent difficile ou impossible l'interception des données ou la lecture des données saisies et qui deviennent de plus en plus usuels, comme les applications que les délinquants peuvent se procurer et utiliser comme éléments tout faits de logiciels de courrier électronique, de téléphones et d'autres technologies.

18. Dans ses rapports pour 1997,[8] 1998[9] et 2000,[10] l'Organe international de contrôle des stupéfiants a exprimé sa préoccupation devant les utilisations qui étaient faites des nouvelles technologies de communication dans le cadre des activités liées au trafic illicite de drogues. Dans son rapport pour 2001, l'Organe a examiné le problème en détail et a formulé une série de recommandations. D'une manière générale, l'Organe a noté que la criminalité organisée s'était mondialisée, mouvement qu'avait encore facilité la disponibilité de nouvelles technologies de communication. S'agissant des problèmes de trafic international de drogues, ces technologies avaient accru l'efficacité des opérations des fabricants, des trafiquants et des autres délinquants qu'avaient compliqué les enquêtes et les poursuites. Du fait de la convergence des technologies nouvelles, les délinquants utilisaient non seulement des ordinateurs et l'Internet, mais aussi des télécopieurs, des répondeurs, des organisateurs de poche et des téléphones cellulaires. Ces appareils sont protégés par des systèmes de chiffrage, des murs coupe-feu et d'autres logiciels sécurisés et des comptes prépayés sont utilisés pour éviter de devoir divulguer aux prestataires de services, pour la facturation, une identité et une adresse authentiques. L'Organe a également noté que, dans certains cas, les individus et bandes faisant l'objet d'enquêtes de la police avaient lancé des contre-offensives contre celle-ci. Certains avaient recruté des experts professionnels spécialisés dans la sécurité pour les aider à protéger leurs systèmes de communication et de stockage des données, tandis que d'autres avaient eu recours à des méthodes de "contre-espionnage" pour attaquer les ordinateurs des enquêteurs et essayer ainsi d'altérer les éléments de preuve ou de saboter l'enquête. Il était même arrivé que le matériel des enquêteurs leur avait été volé pour pouvoir avoir accès aux informations nécessaires pour intercepter leurs communications et identifier et menacer ainsi les enquêteurs.[11]

19. Si l'utilisation qui est faite des technologies nouvelles pour faciliter le trafic de drogues est

manifestement un problème préoccupant, l'Organe en a relevé un autre, à savoir les pharmacies qui vendent sur l'Internet des stupéfiants et des substances psychotropes qui ne doivent être prescrites que sur ordonnance et, d'une manière générale, a pris note des préoccupations exprimées par les experts au sujet de la disponibilité sur l'Internet d'informations encourageant la consommation illicite de drogues ou minimisant les risques que celle-ci représente. D'autres problèmes étaient la diffusion d'informations sur la marche à suivre pour fabriquer des drogues illicites et la possibilité de se procurer au moyen de l'Internet des produits chimiques précurseurs et des informations connexes.[12]

20. D'un côté plus positif, l'Organe a relevé que les communications sécurisées sur l'Internet étaient de plus en plus largement diffusées dans le contexte de la coopération internationale et a relevé que l'Internet pouvait être utilisé aussi par les organisations internationales et nationales comme moyen de prévention en diffusant des informations pour éduquer et dissuader ceux qui seraient tenter par l'abus de drogues.[13]

21. L'Organe a formulé plusieurs recommandations tendant à faire en sorte que le personnel des brigades anti-drogues reçoivent une formation, des ressources et des pouvoirs suffisants pour pouvoir s'attaquer efficacement aux problèmes susmentionnés. Il s'agit notamment des ressources nécessaires pour attirer du personnel qualifié et acheter le matériel et le logiciel indispensables aux enquêtes ainsi que de moyens de protection de l'infrastructure pour mettre les enquêtes à l'abri d'attaques perfectionnées. Plusieurs recommandations concernaient l'utilisation positive qui pouvait être faite des nouvelles technologies, en particulier à des fins d'éducation et de prévention, ainsi que la coopération entre les services de répression, les prestataires de services et les usagers afin d'identifier les abus qui étaient faits des nouvelles technologies et de s'y attaquer efficacement. L'Organe a également évoqué la nécessité d'une coopération internationale, notamment pour l'élaboration de normes, et a recommandé aux États de ratifier sans tarder la Convention du Conseil de l'Europe sur la cyberdélinquance et d'envisager la possibilité d'élaborer sous l'égide de l'Organisation des Nations Unies une convention contre la cybercriminalité.[14]

22. À la suite du Congrès mondial qui a eu lieu à Stockholm en août 1996, le Gouvernement japonais a accueilli le Deuxième Congrès mondial contre l'exploitation sexuelle commerciale des enfants, qui a eu lieu à Yokohama du 17 au 20 décembre 2001, sous la parrainage conjoint du Fonds des Nations Unies pour l'enfance (UNICEF), de l'organisation End Child Prostitution in Asian Tourism (ECPAT) International et du Groupe des ONG pour la Convention relative aux droits de l'enfant. L'UNICEF et plusieurs des organisations non gouvernementales et experts participant au Congrès ont manifesté leur préoccupation devant l'impact des nouvelles technologies sur l'exploitation sexuelle des enfants; et notamment devant la façon dont cela facilitait ou encourageait la production et la diffusion de pornographie infantile. L'apparition de la photographie numérique, par exemple, avait beaucoup facilité la production, tandis que des systèmes de chiffrage et de stéganographie étaient utilisés pour éviter que la police ne découvre la diffusion de cette pornographie.[15] L'Internet lui-même était utilisé pour diffuser les pornographie infantile: il était relativement facile et peu risqué d'y avoir accès, de sorte que la demande allait croissante et qu'il était de plus en plus difficile de la détecter, de l'intercepter, de la saisir et de la poursuivre. La facilité d'accès et l'atténuation des risques que couraient les délinquants avaient continué à accroître la demande de pornographie infantile et ainsi intensifier les risques auxquels les enfants étaient exposés. Les nouvelles technologies suscitaient également d'autres préoccupations, comme l'utilisation de l'Internet par les pédophiles qui pourraient ainsi prendre contact avec des enfants de façon anonyme, qui avait parfois débouché sur des enlèvements. Dans sa déclaration de clôture, intitulée Engagement mondial de Yokohama de 2001, le Deuxième Congrès mondial a demandé que des mesures adéquates soient prises pour s'attaquer aux aspects négatifs des nouvelles technologies et en particulier à l'exploitation qui était faite de l'Internet pour promouvoir la pornographie infantile. Il a simultanément reconnu que les nouvelles technologies pouvaient contribuer à mieux protéger les enfants en diffusant des informations et en conjuguant les efforts de ceux qui cherchaient à combattre l'exploitation sexuelle des enfants.

C. Travaux entrepris sous l'égide d'autres entités

23. Les travaux entrepris sous l'égide d'autres entités étaient décrits en détail dans le rapport du Secrétaire général en date du 30 mars 2001 (E/CN.15/2001/4). Pour une large part, ces travaux se poursuivent mais un organe a mené à bien ceux qu'il avait entrepris en 2001. Ainsi, les réunions du Comité d'experts sur la cyberdélinquance du Conseil de l'Europe ont débouché sur l'adoption, par le Conseil, le 23 novembre 2001, de la Convention sur la cyberdélinquance, qui a été signée par 26 États membres du Conseil ainsi que par les quatre États non européens qui avaient participé à la négociation du texte. Elle entrera en vigueur lorsque cinq pays, dont au moins trois États membres du Conseil, l'auront ratifiée. Les autres États qui ne sont pas membres du Conseil peuvent également adhérer à la Convention sur invitation du Comité des Ministres du Conseil, avec l'assentiment de trois États déjà parties. Lorsque le texte a été publié, le projet de convention a été favorablement accueilli par les organes chargés de l'application des lois mais a été critiqué à certains égards par des groupes de défense des droits de l'homme qui étaient préoccupés par l'élargissement des pouvoirs d'enquête et par les prestataires de services Internet, inquiets du coût que représenteraient le stockage de l'information et les autres types d'assistance à fournir aux services de répression.

24. L'Organisation internationale de police criminelle (Interpol) a continué de mener à bien en 2001 différentes activités tendant à combattre la délinquance liée à la technologie et à l'informatique. Elle a souvent constitué un cadre de coopération pour les forces de police nationale qui menaient des enquêtes transnationales sur la criminalité informatique, et en particulier sur la distribution de pornographie infantile. Elle a poursuivi ses efforts pour aider les services de répression des pays en développement en diffusant une série de manuels à l'intention des enquêteurs et en organisant une série d'ateliers régionaux sur la délinquance liée à l'informatique. En outre, elle a étoffé son site web auquel a été incorporée à la fin de 2000 une nouvelle page consacrée à la délinquance liée aux technologies de l'information, une autre page étant consacrée aux alertes aux virus et y ayant été ajoutée par la suite.

25. Le Groupe d'experts sur la criminalité électronique de l'Organisation mondiale des douanes a également poursuivi ses travaux en 2001 et a examiné une série d'activités illicites présentant un intérêt pour les membres de l'Organisation, en particulier le vol d'identité, auquel ont parfois recours les contrebandiers pour dissimuler leurs propres identités et éviter une surveillance, le suivi électronique des expéditions sont se servent les contrebandiers pour lancer l'alarme lorsqu'il existe un risque de découverte des marchandises clandestines, les activités blanchiment d'argent en ligne et l'expansion des pharmacies qui vendent leurs produits sur l'Internet en éludant les dispositions des législations nationales et de la réglementation des importations et des exportations applicables aux médicaments et drogues prescrits sur ordonnance. En outre, le Groupe d'experts a examiné nombre des mêmes problèmes généraux que ceux dont s'occupent d'autres services de répression, comme la fraude électronique, les virus et autres programmes hostiles et la cyber-extorsion de fonds.

III. Conclusions

26. L'on a donné plus haut un bref aperçu des efforts entrepris pour prévenir et combattre la délinquance liée à la technologie et à l'informatique, l'accent étant mis sur les tendances générales et les travaux entrepris sous l'égide de l'Organisation des Nations Unies ou d'autres entités. Si des ressources sont disponibles, le Centre pour la prévention internationale du crime de l'Office pour le contrôle des drogues et la prévention du crime du secrétariat exécutera le Plan d'action pour la mise en oeuvre de la Déclaration de Vienne et réalisera les autres activités spécifiques recommandées par la Commission pour la prévention du crime et la justice pénale et les autres organes directeurs. Conformément à la résolution 56/121 de l'Assemblée générale, le Secrétaire général pourra être appelé à soumettre un rapport à l'Assemblée à sa cinquante-huitième session sur l'avancement des activités entreprises dans ce domaine. La Commission voudra donc peut-être donner des indications sur les travaux futurs du Centre et sur les options pouvant être envisagées, dans le contexte des priorités existantes.

[1] *Documents officiels du Conseil économique et social, 2001, Supplément No. 10* (E/2001/30/Rev.1), deuxième partie, chapitre II, section A, projet de résolution II, section XI.

[2] Voir *Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, Vienne, 10-17 avril 2000; rapport préparé par le secrétariat* (publication des Nations Unies, numéro de vente: F.00.IV.8).

[3] Conseil de l'Europe, *Recueil des traités européens*, No. 185.

[4] Voir le rapport du Secrétaire général sur les résultats de l'étude sur la fabrication et le trafic illicite d'explosifs par des criminels et leur utilisation à des fins criminelles (E/CN.15/2002/9/Add.1). Le Groupe d'experts sur la fabrication et le trafic illicites d'explosifs a également recommandé aux pays d'adopter des mesures pour décourager la diffusion de ce type d'informations, en particulier sur l'Internet (E/CN.15/2002/9, par. 37 g)).

[5] Voir "Profiting from abuse: an investigation into the sexual exploitation of our children", UNICEF, 2001 (numéro de vente: E.01.XX.14); et ECPAT International, “Child pornography”, p. 19-21.

[6] *Rapport de l'Organe international de contrôle des stupéfiants pour 2000* (publication des Nations Unies, numéro de vente: F.01.XI.1), par. 30, 100 et 133-137.

[7] *Documents officiels du Conseil économique et social, 2001, Supplément No. 10* (E/2001/30/Rev.1), première partie, chapitre III, par. 36 à 38.

[8] *Rapport de l'Organe international de contrôle des stupéfiants pour 1997* (publication des Nations Unies, numéro de vente: F.98.XI.1), par. 23.

[9] *Rapport de l'Organe international de contrôle des stupéfiants pour 1998* (publication des Nations Unies, numéro de vente: F.99.XI.1), par. 241.

[10] *Rapport de l'Organe international de contrôle des stupéfiants pour 2000* (publication des Nations Unies, numéro de vente: F.01.XI.1), par. 30, 100 et 133-137.

[11] *Rapport de l'Organe international de contrôle des stupéfiants pour 2001* (publication des Nations Unies, numéro de vente: F.02.XI.1), par. 5 à 83.

[12] Ibid., par. 19-21.

[13] Ibid., par. 44-66.

[14] Ibid., par. 72-83.

[15] Les systèmes de chiffrage mélangent le contenu numérique du message conformément à un algorithme mathématique, de sorte qu'il est impossible de le déchiffrer ou de lire en l'absence de clé ou de mot de passe, lequel n'est généralement connu que par l'expéditeur ou le destinataire. La stéganographie utilise un logiciel pour dissimuler les données constituant un fichier informatique à l'intérieur des données d'un autre fichier, habituellement beaucoup plus lourd. Ce système est communément utilisé pour dissimuler des textes ou images pornographiques dans des photographies numériques innocentes sans que l'apparence de ces dernières soit visiblement changée. Les images dissimulées peuvent habituellement être identifiées et récupérées (à moins qu'elles ne soient également chiffrées), mais seulement si les enquêteurs ont des raisons de soupçonner qu'elles s'y trouvent. La photographie numérique peut être utilisée pour créer de la pornographie infantile directement en utilisant des enfants ou indirectement en altérant l'image d'adultes pour la faire ressembler à des enfants.