Naciones Unidas E/CN.15/2002/8

Consejo Económico y Social

Distr.: General
29 de enero de 2002
Español
Original: Inglés

Comisión de Prevención del Delito y Justicia Penal
11º período de sesiones
Viena, 16 a 25de abril de 2002
Tema 5 del programa provisional*
Cooperación internacional en la lucha contra la delincuencia transnacional

Adopción de medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas

Informe del Secretario General

Índice

* E/CN.15/2002/1.

I. Introducción

1. En la reanudación de su décimo período de sesiones, celebrado del 6 a 7 de septiembre de 2001, la Comisión de Prevención del Delito y Justicia Penal aprobó un plan de acción[1] que trataba de la prevención y el control de los delitos de alta tecnología y relacionados con las redes informáticas como seguimiento y en aplicación del párrafo 18 de la Declaración de Viena sobre la delincuencia y la justicia: frente a los retos del siglo XXI, aprobada en el Décimo Congreso de las Naciones Unidas sobre la Prevención del Delito y el Tratamiento del Delincuente[2].

2. En su resolución 56/121, de 19 de diciembre de 2001, la Asamblea General, expresando su preocupación por el hecho de que los avances tecnológicos han abierto nuevas posibilidades de actividades delictivas, en particular la utilización de la tecnología de la información con fines delictivos, reconociendo la necesidad de facilitar la transferencia de tecnologías de la información, en particular a los países en desarrollo, subrayando la necesidad de fomentar la coordinación y la cooperación entre los Estados en la lucha contra la utilización de la tecnología de la información con fines delictivos y haciendo hincapié en la función que pueden desempeñar las Naciones Unidas y otras organizaciones internacionales y regionales, acogiendo con satisfacción la labor del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente y expresando su reconocimiento por la labor realizada por la Comisión de Prevención del Delito y Justicia Penal en sus períodos de sesiones noveno y décimo, decidió aplazar el examen del tema de la utilización de las tecnologías de la información con fines delictivos mientras se realiza la labor prevista en el plan de acción.

3. En su resolución 56/261, de 31 de enero de 2002, la Asamblea General tomó nota con reconocimiento de los planes de acción; pidió al Secretario General que velara por la difusión más amplia posible de los planes de acción; invitó a los gobiernos a que estudiaran con atención y utilizaran los planes de acción como orientación al emprender la formulación de leyes, políticas y programas; e invitó al Secretario General a que estudiara atentamente y aplicara los planes de acción, de conformidad con los planes de mediano plazo y los presupuestos por programas, y a reserva de la disponibilidad de recursos.

II. Situación de las actividades en marcha para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas

A. Tendencias y evolución general

4. El campo de los delitos de alta tecnología y relacionados con las redes informáticas se caracteriza por la rápida evolución de las actividades de los delincuentes, de las actividades de prevención, legislativas y de represión del delito, y de las propias tecnologías. Durante 2001, varios Estados establecieron o mejoraron sus capacidades para hacer frente a los delitos de alta tecnología y relacionados con las redes informáticas como una esfera especializada de la legislación y la represión del delito. Las reformas legislativas incluyeron la creación de nuevos delitos, la ampliación de delitos existentes y la modernización de los medios de investigación, incluida la autoridad para realizar allanamientos e incautaciones, y para interceptar comunicaciones telefónicas a fin de combatir la delincuencia en los nuevos entornos electrónicos. Se prevé la continuación de esta tendencia, en particular en Europa, donde los Estados están poniendo en práctica la Convención sobre el delito cibernético, aprobada por el Consejo de Europa en Budapest, el 23 de noviembre de 2001[3].

5. Una cuestión que siguió ocupando la atención en muchos países, tanto en el plano de las políticas y la legislación como en el plano de las investigaciones y la represión del delito, fue la relación entre las actividades del gobierno de lucha contra la delincuencia y la función de las compañías del sector privado que producen equipo y programas informáticos y las que prestan servicios. Entre los temas más importantes figuraron la medida en que debían incorporarse en las nuevas tecnologías elementos de ayuda para las investigaciones y la lucha contra la delincuencia, el costo del almacenamiento, la intercepción y la recuperación de datos que necesitan

los organismos de represión del delito, y una serie de cuestiones relacionadas con las políticas, la delincuencia y la responsabilidad civil dimanantes de las relaciones entre el Estado, los proveedores de servicios y los clientes individuales. Tras una serie de importantes ataques de introducción de virus y denegación de servicios que tuvieron lugar durante 1999 y 2000, un grupo de grandes empresas de alta tecnología estableció y financió un centro conjunto sin fines de lucro, el Centro de Análisis e Intercambio de Información sobre Tecnología, para superar las rivalidades competitivas y aunar los esfuerzos para combatir la delincuencia relacionada con las redes informáticas. En el seno de las principales compañías de tecnología, la incorporación de características de seguridad en los nuevos programas informáticos pasó a tener una prioridad más alta, como parte de los esfuerzos de las empresas por reducir su propia vulnerabilidad a los ataques y en reconocimiento de que el temor al delito y la presencia de características de seguridad eficaces habían pasado a ser un factor importante en las decisiones de los consumidores que adquirían nuevos productos.

6. El empleo de métodos técnicos de seguridad y prevención del delito continuó ampliándose durante 2001, como consecuencia de la naturaleza de las tecnologías, su continua expansión y las dificultades con que tropezaban los medios legislativos y de represión del delito tradicionales, en particular en casos que trascendían las fronteras. Estos métodos comprendían productos conocidos, como programas para identificar y eliminar de los datos almacenados y transmitidos programas hostiles como parásitos y virus, y productos que actuaban como barreras, como los programas informáticos de protección de la información (cortafuego). Fue aumentando el uso de programas de “geolocalización”, que identifican la fuente geográfica de las comunicaciones en línea, para denegar acceso a las situadas en jurisdicciones en que el juego, la pornografía y otras actividades son ilegales. Estos métodos fueron recibidos con entusiasmo por la comunidad de represión del delito, pero fueron criticados por los defensores de una Internet completamente abierta; los expertos señalaron que el uso efectivo de ese tipo de programas dependía de la voluntad de los operadores de sitios en la web para utilizarlos y de sus conocimientos de las restricciones legales impuestas por otros países. La mayoría de los expertos convinieron también en que esos programas prevenían efectivamente las violaciones accidentales y eran eficaces contra delincuentes sin muchos conocimientos pero no contra los más informados, que podían fácilmente ocultar su verdadera ubicación geográfica respecto del programa informático y de los operadores de sitios en la web que los utilizaban. También continuó ampliándose el empleo de programas de filtrado, que identifican y bloquean el contenido de programas no adecuados para niños y otros usuarios no autorizados, y muchos operadores de sitios para adultos incorporaron productos que ponían en marcha automáticamente esos filtros. También se utilizaron aplicaciones de criptografía para proteger comunicaciones confidenciales e impedir que usuarios no autorizados obtuvieran acceso a los datos confidenciales o sujetos a derechos de propiedad.

7. La comunidad de represión del delito reconoció que los investigadores con las capacidades necesarias para interceptar comunicaciones en medios digitales de alta velocidad, realizar con éxito búsquedas de datos almacenados, descifrar datos codificados y realizar otras funciones similares constituían un recurso muy raro, valioso y especializado. Muchos organismos cuentan ahora con dependencias especializadas, que ayudan a otros investigadores en campos que van desde las actividades contra el terrorismo hasta el tráfico de drogas y los delitos económicos. Entre los problemas principales figuran el alto costo y la inversión a largo plazo que exige la capacitación de investigadores, las dificultades para conservar a investigadores calificados que pueden obtener sueldos más altos en puestos del sector privado mejor financiados, y problemas sencillos, como asegurar que los investigadores se mantengan al día del despliegue de las nuevas tecnologías y las nuevas técnicas utilizadas por los delincuentes.

8. Preocupa a los Estados Miembros la posibilidad de que las organizaciones de terroristas utilicen las nuevas tecnologías con fines defensivos y ofensivos, y esas preocupaciones han adquirido más importancia después de los ataques del 11 de septiembre de 2001. La experiencia muestra que los delincuentes terroristas sofisticados ya están utilizando la Internet como medio de comunicación. En ese contexto, se han utilizado productos complejos de codificación y otros productos de seguridad en forma defensiva para ocultar comunicaciones y datos almacenados. Los posibles usos ofensivos en apoyo de objetivos terroristas

también hicieron que muchos países establecieran organismos especializados para proteger el procesamiento de datos, las comunicaciones y otras infraestructuras críticas de alta tecnología contra ataques cibernéticos.

9. Las investigaciones realizadas inmediatamente después de los ataques de septiembre revelaron también el uso de la Internet para obtener la información necesaria para planificar ataques, o para obtener los materiales necesarios para fabricar o improvisar armas químicas, biológicas o radiológicas. Varios Estados que respondieron a una encuesta de las Naciones Unidas que trataba, entre otras cosas, del uso indebido de explosivos con fines delictivos, expresaron su preocupación por la disponibilidad en la Internet de información sobre cómo producir explosivos y como fabricar dispositivos explosivos[4]; además, fuentes de los medios de difusión informaron de que una persona arrestada en relación con un intento de hacer detonar un dispositivo explosivo oculto en su zapato abordo de un vuelo comercial de París a Miami había confesado a los investigadores que había construido el dispositivo utilizando información obtenida de la Internet. Organismos que realizan actividades de represión de drogas expresaron preocupaciones similares con respecto a la disponibilidad en la Internet de información sobre la forma de producir drogas sintéticas y sobre fuentes para obtener los ingredientes necesarios.

10. Otros delitos de alta tecnología y relacionados con las redes informáticas siguieron siendo objeto de preocupación durante 2001. Entre los más destacados figuraron el uso de tecnologías digitales y de la Internet para producir y difundir pornografía infantil. Varios participantes en el Segundo Congreso Mundial contra la Explotación Comercial Sexual de Niños, celebrado en Yokohama (Japón), del 17 al 20 de diciembre de 2001, vincularon los posibles aumentos en la explotación de niños y el volumen general de la pornografía infantil a la ampliación del mercado[5] pero señalaron que las actividades de colaboración en la represión del delito habían desbaratado con éxito varias operaciones en gran escala de pornografía infantil en la Internet, muchas de ellas de carácter transnacional. En las monografías presentadas en el Congreso Mundial también se estableció una vinculación entre la Internet y otras actividades de paidofilia, incluido el turismo sexual de niños y el secuestro de niños.

11. Se expresó también preocupación por el aumento del robo de identidades, en que los delincuentes utilizan datos personales para hacerse pasar por el individuo al que han robado los datos. Los robos de identidades, en combinación con el anonimato de las transacciones en línea y otras actividades, se utilizaron para cometer una serie de delitos que comprendían desde el fraude hasta las actividades terroristas. Otras actividades delictivas comunicadas incluyeron el fraude, la extorsión en línea, el blanqueo de dinero y el contrabando con ayuda de computadoras, y los delitos contra sistemas de computadoras y sus usuarios, con utilización de virus y otras programas hostiles, así como ataques de denegación de servicios. Una novedad con respecto al fraude fue la utilización de entidades de caridad falsas en la Internet para atraer donaciones inmediatamente después de los ataques terroristas del 11 de septiembre, aprovechando los tiempos de reacción rápidos que permiten el establecimiento y la cancelación de nuevos sitios en la web.

12. Las actividades en línea crearon también varios problemas incipientes para los planes nacionales de aplicación de disposiciones normativas en esferas como la tributación, la regulación de las empresas y la aplicación de normas ambientales, en que el almacenamiento de datos en el extranjero, el uso creciente de la codificación y la capacidad de las empresas de un país para tratar directamente con clientes de otro país han planteado más dificultades a las actividades para reglamentar, inspeccionar y verificar el cumplimiento de la ley. Un ejemplo de esto es la utilización de farmacias en línea, que fue considerada como un problema en el informe de la Junta Internacional de Fiscalización de Estupefacientes[6], así como por expertos del Consejo de Cooperación Aduanera (también denominado La Organización Mundial de Aduanas) y por la Comisión de Estupefacientes. La preocupación principal de la Junta Internacional de Fiscalización de Estupefacientes se refiere al transporte ilícito de estupefacientes y sustancias sicotrópicas, pero otras fuentes opinan que el problema es más amplio, y que abarca muchas drogas medicinales y de otro tipo que están sujetas a controles aduaneros básicos y a regímenes de prescripción médica en varios países. Esto plantea un problema no sólo para las autoridades encargadas de hacer cumplir la ley, sino también para las autoridades sanitarias, los organismos de aduanas y otros órganos de reglamentación.

B. Novedades en el seno de las Naciones Unidas

13. En su resolución 1999/23 de 28 de julio de 1999, titulada "Labor del Programa de las Naciones Unidas en materia de prevención del delito y justicia penal", el Consejo Económico y Social pidió al Secretario General que, teniendo presentes las actividades del curso práctico sobre delitos relacionados con las redes informáticas, celebrado durante el Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuentes, efectuara un estudio sobre medidas eficaces que podrían adoptarse en los planos nacional e internacional para prevenir y controlar los delitos relacionados con las redes informáticas. En su décimo período de sesiones, la Comisión tuvo ante sí el informe del Secretario General sobre las conclusiones del estudio (E/CN.15/2001/4). Varios oradores reconocieron la gravedad de los delitos de alta tecnología y relacionados con las redes informáticas y destacaron la importancia de tomar medidas contra esos delitos en el plano internacional, incluso en el marco de las Naciones Unidas. Se señaló que la lucha contra la delincuencia de alta tecnología y relacionada con las redes informáticas exigía la realización de numerosas investigaciones complejas, y que la adopción de una enfoque común a la lucha contra ese tipo de delitos revestía mucha importancia.

14. Los planes de acción que figuran en los anexos de la resolución 56/261 de la Asamblea General relativos a la aplicación y el seguimiento de la Declaración de Viena incluían un plan de acción contra los delitos de alta tecnología y relacionados con las redes informáticas, en el que se disponía que el Centro para la Prevención Internacional del Delito:

a) apoyará las actividades nacionales e internacionales de investigación de nuevas formas de delitos informáticos y evaluara sus efectos en esferas decisivas como el desarrollo sostenible, la protección de la intimidad y el comercio electrónico, y la medidas de respuesta adoptadas;

b) divulgará materiales acordados internacionalmente, como directrices, manuales jurídicos y técnicos, reglas mínimas, prácticas de utilidad demostrada y leyes modelo para ayudar a los legisladores y a los encargados de hacer cumplir la ley, así como a otras autoridades, en la formulación, adopción y aplicación de medidas eficaces contra los delitos relacionados con la alta tecnología y la informática y sus autores, tanto en general como en casos concretos;

c) promoverá, apoyará y pondrá en práctica, según proceda, proyectos de cooperación y asistencia técnicas. Esos proyectos facilitarían los contactos entre expertos en materia de prevención del delito, delitos contra la seguridad informática, legislación y procedimientos penales, enjuiciamiento, técnicas de investigación y cuestiones conexas, y los Estados que deseen solicitar información o asistencia en esas esferas.

15. De conformidad con el párrafo 5 de la resolución 56/261, en que la Asamblea General invitó al Secretario General a que estudiara atentamente y aplicara, según procediera, los planes de acción, incluido el plan de acción contra los delitos relacionados con la alta tecnología y la informática, de conformidad con los planes de mediano plazo y los presupuestos por programas, y a reserva de la disponibilidad de recursos, y teniendo en cuenta los comentarios de la Comisión en su décimo período de sesiones[7], se realizará, cuando se disponga de los recursos necesarios, un estudio más detallado del problema y de la medidas establecidas en el plan de acción.

16. La creciente utilización de nuevas tecnologías informáticas y de telecomunicaciones por los grupos de delincuentes organizados sigue causando mucha preocupación. Este es particularmente el caso de las organizaciones que se dedican a la producción y el tráfico de estupefacientes, que se cuentan entre los grupos delictivos más complejos y mejor financiados y, por lo tanto, tienen acceso a los mejores expertos y los dispositivos más avanzados disponibles. Los que se dedican a la producción y el tráfico emplean tecnologías más o menos de la misma forma que los usuarios comerciales legítimos. La información relativa a la entrega de remesas de drogas se pasa del remitente al receptor utilizando medios que el personal de represión del delito no puede interceptar o leer fácilmente. La contabilidad de los negocios se lleva en jurisdicciones extranjeras, oculta entre grandes volúmenes de otros datos y protegida por tecnologías como los cortafuegos y la codificación para ocultarla de los investigadores. Los traficantes utilizan el rastreo

electrónico de la carga para vigilar artículos en que se han ocultado drogas u otros contrabandos, y las demoras indebidas les sirven de alerta sobre el posible descubrimiento e intercepción de la remesa. El relativo anonimato de las remesas electrónicas de fondos se aprovecha cada vez más para efectuar pagos sin atraer la atención de los agentes de represión del delito, y los receptores de los pagos pueden blanquear posteriormente ese dinero por el mismo medio. La Internet se utiliza también para transmitir información básica, como instrucciones para la producción de drogas sintéticas y mensajes que estimulan el uso indebido de drogas.

17. En el informe de la Secretaría de 21 de diciembre de 2000 sobre la situación mundial con respecto al tráfico ilícito de drogas, se trata el problema de los delitos electrónicos y se recomienda que los gobiernos establezcan políticas nacionales que apoyen las actividades de represión del delito (E/CN.7/2001/5, párrafo 150). Se pide a los organismos encargados de hacer cumplir la ley que establezcan enlaces con proveedores de servicios a fin de que estos últimos conserven los datos pertinentes el tiempo suficiente para que puedan recuperarse con fines de investigación y participen en la lucha contra el blanqueo de dinero por conducto de la Internet. En enero de 2002, un órgano subsidiario de la Comisión, los Jefes de Organismos Nacionales Encargados de Combatir el Tráfico Ilícito de Drogas, Europa, celebró una reunión regional de expertos para examinar los problemas que enfrentaban los organismos de represión del delito cuando tropezaban con nuevas tecnologías en sus investigaciones relacionadas con las drogas. Entre los problemas señalados por el grupo figuraban los enormes volúmenes de datos almacenados y transmitidos sin los cuales no se podía identificar y encontrar información crítica; la creciente dependencia de los servicios de represión del delito respecto de los proveedores de servicios para buscar o interceptar datos y las consecuencias de esto relacionadas con el costo y la seguridad; y la aparición de una serie de nuevas tecnologías, como los teléfonos celulares digitales, los teléfonos por satélite y las salas de charlas seguras en la Internet, que eran mucho más difíciles de interceptar que los métodos de comunicaciones anteriores. Se expresó mucha preocupación por la aparición de complejos programas de codificación, que dificultaban o hacían imposible la intercepción o la incautación de datos y que eran cada vez más comunes, tanto como aplicaciones que los delincuentes podían adquirir y utilizar, o como elementos integrales de programas de correo electrónico, telefonía celular y otras tecnologías de expendio libre.

18. En sus informes correspondientes a 1997[8], 1998[9] y 2000[10], la Junta Internacional de Fiscalización de Estupefacientes expresó preocupación ante las diversas formas en que las nuevas tecnologías de la comunicación estaban pasando a ser un factor en las actividades ilícitas relacionadas con las drogas. En su informe correspondiente a 2001, la Junta examinó el problema a fondo e hizo una serie de recomendaciones. En general, la Junta observó que la delincuencia organizada se había mundializado y que la disponibilidad de nuevas tecnologías de las comunicaciones había sido un factor en esa evolución. En el caso de los problemas internacionales relacionados con las drogas, los efectos incluían una mayor eficacia de las operaciones de los productores, traficantes y otros delincuentes, y mayores dificultades para la investigación y el enjuiciamiento de esas actividades. La convergencia de las tecnologías permitiría a los delincuentes utilizar no sólo computadoras y la Internet, sino también máquinas de facsímil, notificadores de llamadas electrónicos, organizadores de bolsillo y teléfonos celulares. Esos dispositivos están protegidos mediante codificación, cortafuegos y otros programas informáticos de seguridad; la utilización de cuentas pagadas de antemano permite evitar el suministro a los proveedores de servicios de la verdadera identidad y la dirección geográfica con fines de facturación. La Junta observó también casos en que los sujetos de la investigación realizaban contra ofensivas contra los organismos encargados de hacer cumplir la ley. Algunos habían contratado a expertos profesionales en seguridad para que les ayudaran a proteger sus comunicaciones y sus datos almacenados, y otros habían utilizando técnicas de pirateo informático inverso para atacar las computadoras de los investigadores a fin de dañar las pruebas o sabotear las actividades de investigación. En un caso, se había robado equipo de los investigadores para obtener la información necesaria para interceptar sus comunicaciones, y el resultado fue que los investigadores fueron identificados y amenazados[11].

19. Aunque la utilización de nuevas tecnologías para apoyar directamente el tráfico de drogas es

evidentemente un motivo de preocupación, la Junta destacó también la utilización de farmacias de la Internet como proveedoras de estupefacientes y sustancias sicotrópicas de venta con receta constituía un problema para los organismos de reglamentación nacionales y, en forma más general, puso de relieve las preocupaciones de los expertos por la disponibilidad de información que alentaba el uso de drogas ilícitas o minimizaba los riesgos conexos. La difusión de información sobre la forma de producir drogas ilícitas y la disponibilidad de precursores químicos e información conexa también se consideraron problemas[12].

20. La Junta señaló también un aspecto más positivo, que era el creciente uso de las comunicaciones seguras por la Internet como base para la cooperación internacional, y destacó que la Internet también podía ser utilizada por las organizaciones nacionales e internacionales con fines de prevención, para la difusión de información con fines educativos y para disuadir a posibles usuarios de drogas[13].

21. La Junta hizo también varias recomendaciones con miras a asegurar que el personal de los organismos de represión de drogas tuviera capacitación adecuada, recursos y facultades jurídicas para atacar efectivamente los problemas mencionados. La recomendaciones tenían que ver con los recursos necesarios para atraer personal calificado, y adquirir el equipo y los programas informáticos necesarios para realizar investigaciones, así como suficiente infraestructura crítica para proteger las investigaciones contra ataques con medios sofisticados. Varias recomendaciones se referían a la utilización positiva de tecnologías, en particular con fines de educación y prevención, así como para la cooperación entre los organismos de represión del delito, lo proveedores de servicios y los usuarios de tecnologías con miras a identificar y contrarrestar efectivamente los abusos. La Junta examinó también la necesidad de establecer la cooperación internacional y elaborar normas, y recomendó la rápida ratificación de la Convención sobre el delito cibernético del Consejo de Europa, así como el examen de la posibilidad de elaborar una convención de las Naciones Unidas contra los delitos cibernéticos[14].

22. Tras el Congreso Mundial celebrado en Estocolmo en agosto de 1996, el Gobierno del Japón dio acogida al Segundo Congreso Mundial contra la Explotación Comercial Sexual de Niños en Yokohama, del 17 al 20 de diciembre de 2001, organizado conjuntamente por el Fondo de las Naciones Unidas para la Infancia (UNICEF), End Child Prostitution in Asian Tourism (ECPAT) International y el Grupo de Organizaciones No Gubernamentales para la Convención sobre los Derechos del Niño. El UNICEF y otras organizaciones no gubernamentales y expertos individuales que asistieron al Congreso expresaron preocupación por las consecuencias de las nuevas tecnologías en la explotación sexual de los niños. Un importante aspecto de ese problema era la forma en que las tecnologías apoyaban, alentaban o facilitaban la producción y difusión de pornografía infantil. La aparición de la fotografía digital, por ejemplo, había facilitado mucho la producción, y la codificación y la esteganografía se utilizaban para encubrir la pornografía de los investigadores[15]. La propia Internet se utilizaba para difundir pornografía infantil, haciendo relativamente fácil el acceso de bajo riesgo, aumentando la demanda y dificultando la detección, interdicción, investigación e incautación. Se consideró que la facilidad de acceso y la reducción del riesgo para los delincuentes eran factores que contribuían a la mayor demanda de pornografía infantil, y que esto daba lugar a un mayor riesgo para los niños. Se expresaron también otras preocupaciones respecto de las nuevas tecnologías. El uso de la Internet por los paidófilos para establecer contactos anónimos con las niños, que en algunos casos daba lugar a secuestros, era uno de esos motivos de preocupación. En su declaración final, el Compromiso Mundial de Yokohama 2001, el Segundo Congreso Mundial instó a que se tomarán medidas adecuadas para contrarrestar los aspectos negativos de las nuevas tecnologías, en particular la función que correspondía al uso de la Internet en la pornografía infantil. Se reconoció también el potencial de las nuevas tecnologías para proteger a los niños mediante la difusión de información, y las posibilidades que ofrecen de poner en contacto a todos los interesados en el problema de la explotación sexual de los niños.

C. Novedades en la labor de otras entidades

23. La labor de otras entidades se describe detalladamente en el informe del Secretario General de 30 de marzo de 2001 (E/CN.15/2001/4). Gran parte de

esa labor continúa, pero un órgano puso fin con éxito a su labor en 2001. Las reuniones del Comité de Expertos sobre la Delincuencia en el Espacio Cibernético del Consejo de Europa concluyeron con la aprobación de la Convención sobre el delito cibernético por el Consejo el 23 de noviembre de 2001. La Convención ha sido firmada por 26 Estados miembros del Consejo, así como por los cuatro estados no europeos que participaron en su negociación. Entrará en vigor cuando la hayan ratificado cinco países, de los cuales por lo menos tres deben ser Estados miembros del Consejo. Otros Estados que no son miembros del Consejo también pueden adherirse a la Convención por invitación del Comité de Ministros del Consejo, para lo cual se requiere el consentimiento de los Estados quizá son partes. En el momento de su publicación, el proyecto de convención recibió comentarios positivos de la comunidad de organismos encargados de hacer cumplir la ley, pero también fue objeto de algunas críticas de parte de grupos de derechos humanos preocupados por los poderes de investigación, y de parte de proveedores de servicios de la Internet, a los que preocupaba el costo de almacenar información y prestar otros tipos de asistencia a los organismos de represión del delito.

24. La Organización Internacional de Policía Criminal (Interpol) continuó realizando durante 2001 una serie de actividades contra la delincuencia relacionada con la alta tecnología y las redes informáticas. Con frecuencia, ofreció una base para la cooperación entre las fuerzas nacionales de policía en la realización de investigaciones multinacionales de delitos cometidos en línea, en particular la distribución de pornografía infantil. Continuó sus esfuerzos por ayudar a los organismos de represión del delito de países en desarrollo, mediante la difusión de una serie de manuales para investigadores y la organización de una serie de grupos de trabajo regionales sobre la delincuencia relacionada con la tecnología de la información. A finales de 2000 amplió también su sitio en la web para incluir una página sobre la delincuencia relacionada con la tecnología de la información, y posteriormente volvió a ampliar el sitio para incluir alertas sobre virus.

25. El Grupo de Expertos de la Organización Mundial de Aduanas sobre la delincuencia electrónica también continuó su labor en 2001, examinando diversas actividades ilícitas de interés para sus miembros. Se expresó también particular preocupación por el fraude o robo de identidad, utilizado algunas veces por los contrabandistas para ocultar sus identidades o evitar la vigilancia; el rastreo electrónico de las remesas, utilizado para alertar a los contrabandistas del posible descubrimiento del contrabando; las actividades de blanqueo de dinero en línea; y el aumento de las farmacias de la Internet, que permitía eludir las leyes nacionales y los controles a la exportación y la importación de productos medicinales y de drogas de expendio bajo receta. El Grupo de Expertos examinó también muchos de los mismos problemas planteados por otros organismos de represión del delito, incluido el fraude electrónico, los virus y otros programas hostiles, y la extorsión cibernética.

III. Observaciones finales

26. En el presente informe se proporciona una breve descripción de las actividades en marcha para prevenir y combatir la delincuencia relacionada con la alta tecnología y las redes informáticas, poniendo de relieve las tendencias generales y las novedades dentro y fuera del sistema de las Naciones Unidas. Con sujeción a la disponibilidad de recursos, el Centro de Prevención Internacional del Delito de la Oficina de Fiscalización de Drogas y de Prevención del Delito de la Secretaría, seguirá en sus futuras actividades las orientaciones de la Comisión de Prevención del Delito y Justicia Penal y otros órganos normativos, tanto en la ejecución del plan de acción para aplicar la Declaración de Viena como en relación con cualquier otra recomendación específica que haga cualquiera de esos órganos. De conformidad con la resolución 56/121 de la Asamblea General, el Secretario General puede ser llamado a informar a la Asamblea, en su quincuagésimo octavo período de sesiones, acerca de los nuevos progresos logrados. Por consiguiente, la Comisión quizá desee examinar la labor futura del Centro, y proporcionar orientación a ese respecto, y las opciones disponibles, en el contexto de las prioridades existentes.

Notas

[1] *Documentos Oficiales del Consejo Económico y Social, 2001, Suplemento Nº. 10* (E/2001/30/Rev.1), segunda parte, cap. II, secc. A, proyecto de resolución II, secc. XI.

[2] Véase *Décimo Congreso de las Naciones Unidas sobre la Prevención del Delito y el tratamiento del Delincuente, Viena, 10 a 17 de abril de 2000;informe preparado por la Secretaría* (publicación de las Naciones Unidas, Nº de venta. S.00.IV.8).

[3] Consejo de Europa, *European Treaty Series*, Nº 185.

[4] Véase el informe del Secretario General sobre los resultados del estudio relativo a la fabricación y el tráfico ilícitos de explosivos por delincuentes, y su utilización con fines delictivos (E/CN.15/2002/9/Add.1). El grupo de expertos sobre la fabricación y el tráfico ilícitos de explosivos también recomendó que los países tomaran medidas para desalentar la difusión de información de ese tipo, en particular por la Internet (E/CN.15/2002/9, párr. 37 g)).

[5] Véase "Profiting from abuse: an investigation into the sexual exploitation of our children", UNICEF, 2001 (Nº de venta E.01.XX.14); y ECPAT International, "Child pornography", págs. 19 a 21.

[6] *Informe de la Junta Internacional de Fiscalización de Estupefacientes correspondiente a 2000* (publicación de las Naciones Unidas, Nº de venta S.01.XI.1), párrs. 30, 100 y 133 a 137.

[7] *Documentos oficiales del Consejo Económico y Social, 2001, Suplemento Nº 10* (E/2001/30/Rev.1), primera parte, cap. III, párrs. 36 a 38.

[8] *Informe de la Junta Internacional de Fiscalización de Estupefacientes 1997* (publicación de las Naciones Unidas, Nº de venta S.98.XI.1), párr. 23.

[9] *Informe de la Junta Internacional de Fiscalización de Estupefacientes correspondiente a 1998* (publicación de las Naciones Unidas, Nº de venta S.99.XI.1), párr. 241.

[10] *Informe de la Junta Internacional de Fiscalización de Estupefacientes correspondiente a 2000* (publicación de las Naciones Unidas, Nº de venta S.01.XI.1), párrs 30, 100 y 133 a 137.

[11] *Informe de la Junta Internacional de Fiscalización de Estupefacientes correspondiente a 2001* (publicación de las Naciones Unidas, Nº de venta S.02.XI.1), párrs. 5 a 83.

[12] Ibid., párrs. 19 a 21.

[13] Ibid., párrs. 44 a 66.

[14] Ibid., párrs. 72 a 83.

[15] La codificación mezcla el contenido digital de conformidad con un algoritmo, que impide descifrar o leer la información sin una clave o contraseña, que por lo general sólo conoce el propietario o el destinatario previsto de los datos. La esteganografía emplea programas informáticos para ocultar datos incluidos en un archivo de computadora entre los datos de otro archivo, por lo general mucho más grande. Se utiliza normalmente para ocultar textos o imágenes pornográficos en fotografías digitales inocuas sin modificar su apariencia en forma visible. Las imágenes ocultas normalmente se pueden identificar y recuperar (a menos que también estén codificadas), pero sólo si los investigadores sospechan su existencia. La fotografía digital se puede utilizar para crear pornografía infantil directamente utilizando niños, o indirectamente mediante la alteración o "morphing" de imágenes de adultos para hacer que éstos parezcan niños.