Naciones Unidas E/CN.15/2001/4

Consejo Económico y Social

Distr. general
30 de marzo de 2001
Español
Original: inglés

Comisión de Prevención del Delito y Justicia Penal
10º período de sesiones
Viena, 8 a 17 de mayo de 2001
Tema 4 del programa provisional*
Cooperación internacional en la lucha contra la delincuencia transnacional

Conclusiones del Estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas

Informe del Secretario General

Resumen

El presente informe responde, en parte, a la solicitud formulada por el Consejo Económico y Social, en su resolución 199/23, de 28 de julio de 1999, de que el Secretario General 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. Ofrece un examen preliminar del tema y recomienda que se realice un estudio más detallado y se presente a la Comisión de Prevención del Delito y Justicia Penal para examen en su 11º período de sesiones como cuestión de alta prioridad. Recomienda además que la Comisión examine en ese período de sesiones una serie de opciones para adoptar otras medidas, incluida la posible redacción de un instrumento internacional contra la delincuencia relacionada con las redes informáticas, y opciones para una estrategia a plazo más breve, incluida la creación de un programa mundial de las Naciones Unidas contra los delitos de alta tecnología y relacionados con las redes informáticas. Ofrece también información sobre las actividades de otras organizaciones internacionales e intergubernamentales competentes y trata de responder a algunas de las preocupaciones planteadas por distintos Estados Miembros.

* E/CN.15/2001/1.

V.01-82402 (S) 030501 030501

Índice

I. Introducción

1. El problema de las actividades delictivas que implican modernas tecnologías de computadora, redes informáticas y telecomunicaciones supone un desafío importante para la justicia penal y las entidades encargadas de aplicar la ley de los Estados Miembros. Cabe considerar que ese desafío presenta las siguientes características:

a) El desafío es mundial. Hasta la fecha, la mayoría de los usuarios de tecnologías modernas y, por consiguiente, la mayoría de los delincuentes y víctimas se encontraban en países desarrollados. La extensión a los países en desarrollo del acceso a la informática se ha señalado como prioridad importante para lograr que una sociedad de información mundial se convierta en factor que apoye el desarrollo, en lugar de ser un obstáculo más[1]. Los países en desarrollo serán vulnerables a la delincuencia relacionada con las redes informáticas y de telecomunicaciones y podrían verse excluidos del acceso a esas redes por las tecnologías de prevención del delito o de seguridad, si no pueden participar en la elaboración y aplicación de políticas de lucha contra la delincuencia;

b) El desafío es dinámico. El rápido desarrollo de nuevas tecnologías lleva a un desarrollo igualmente rápido de innovaciones delictivas, y la naturaleza mundial de las tecnologías se traduce en la rápida difusión de nuevas técnicas delictivas. Por ello, el seguimiento tanto del desarrollo legítimo como de las innovaciones delictivas a fin de mantener al día las respuestas nacionales e internacionales, será de importancia crítica, en particular en los países en donde los recursos técnicos son limitados. El proceso es impulsado principalmente por el desarrollo tecnológico y, por consiguiente, tiene carácter abierto.

c) El desafío es multidisciplinario. El desarrollo de tecnologías relacionadas con las redes informáticas y de telecomunicaciones supone un importante desplazamiento desde las actividades sociales y económicas que suponen actividades físicas y productos materiales hacia las que suponen información o conocimientos puros. Ello tiene consecuencias importantes en esferas como los derechos humanos y el desarrollo social y económico sostenible. Será importante que la lucha contra la delincuencia se convierta en elemento de esos programas, y a la inversa. Las tecnologías de la información y la estructura de las redes informáticas y de telecomunicaciones son también, en gran parte, productos del desarrollo del sector privado, y la elaboración de medidas contra la delincuencia de alta tecnología y relacionada con las redes informáticas debe tener en cuenta factores como la viabilidad comercial y la competitividad económica de las tecnologías de que se trate.

II. Antecedentes

A. Examen de la cuestión por otras organizaciones intergubernamentales o internacionales

2. La creciente preocupación de los Estados por la naturaleza y la dimensión del problema y la necesidad de medidas mundiales eficaces para combatirlo se pone de relieve en el número de foros en que se ha examinado.

1. El Consejo de Europa

3. El Consejo de Europa está terminando el texto de una Convención sobre el delito cibernético[2], que tratará de los delitos relativos a la interferencia con sistemas, el acceso no autorizado, el fraude y la falsificación electrónicos, el contenido ofensivo y los delitos contra la propiedad intelectual. El proyecto de texto trata de las facultades de investigación, incluido el rastreo de comunicaciones y la búsqueda, incautación y preservación de pruebas electrónicas. Definirá también los términos esenciales y establecerá normas para la asistencia judicial recíproca y otras formas de cooperación internacional. Cuando concluya con éxito, el texto constituirá el primer intento de un instrumento internacional amplio contra la delincuencia relacionada con las redes informáticas. El proyecto de texto terminado ha tenido una recepción variada. En general, los gobiernos, expertos y organismos encargados de aplicar la ley lo consideran una evolución positiva, aunque muchos estiman que todavía no se han abordado algunas de las cuestiones más difíciles. Muchos grupos de intereses adoptan la posición de que no deben regularse las redes internacionales, y han atacado ese instrumento como un intento de ampliar las

facultades de aplicación de las leyes nacionales a expensas de la intimidad individual y otros intereses.

4. Las negociaciones sobre el texto del instrumento se realizaron por un Comité de Expertos sobre la Delincuencia en el Espacio Cibernético, creado en febrero de 1997 a raíz de varios estudios anteriores del problema[3]. Además de los miembros regulares del Comité, se invitó a expertos del Canadá, el Japón y los Estados Unidos de América a participar en sus deliberaciones, y otros Estados se unieron al proceso en el curso de las negociaciones. El Comité preparó 25 proyectos de texto sucesivos durante su mandato, que concluyó en diciembre de 2000. El texto definitivo se ha sometido a la Asamblea Parlamentaria del Consejo de Europa. Ulteriormente se presentará al Comité Europeo para los Problemas de la Delincuencia, para su examen en junio de 2001 y, si se adopta, se comunicará al Comité de Ministros del Consejo de Europa, para su aprobación.

2. Grupo de los Ocho

5. A raíz de debates de los problemas derivados de la delincuencia transnacional en su reunión en la cumbre celebrada en Halifax (Canadá), en junio de 1995, los siete países industrializados principales y la Federación de Rusia (Grupo de los Ocho) crearon un Grupo de Expertos de Alto Nivel sobre la Delincuencia Transnacional Organizada (Grupo de Lyon), que incluía un subgrupo de expertos sobre la delincuencia relacionada con las redes informáticas. El subgrupo se ha reunido regularmente desde 1997 y ha elaborado cierto número de iniciativas. Las principales cuestiones que ha examinado han sido los problemas planteados por las búsquedas electrónicas transfronterizas, el rastreo de comunicaciones y la necesidad de cooperación entre los gobiernos y los intereses pertinentes del sector privado.

6. En diciembre de 1997, el Grupo de los Ocho aprobó un plan de acción de 10 puntos sobre la delincuencia cibernética que incluía el examen de legislación, medidas para garantizar la disponibilidad de personal de aplicación de la ley capacitado y equipado, el examen de cuestiones de la delincuencia cibernética al negociar acuerdos de auxilio judicial, el examen de métodos para preservar las pruebas electrónicas y ponerlas a disposición de procedimientos penales extranjeros, una mejor cooperación con las industrias, y normas forenses y otras normas técnicas para la seguridad informática y la utilización de pruebas electrónicas en los procedimientos judiciales[4].

7. En 1999, el Grupo de los Ocho aprobó algunos principios básicos preliminares para los organismos encargados de aplicar la ley que quisieran tener acceso a datos electrónicos almacenados en Estados extranjeros[5]. En general, se convino en que se podía acceder libremente a esos datos si estaban a disposición pública, como ocurriría por ejemplo, en el caso de un sitio web abierto, o cuando se obtuviera el consentimiento de alguien con autoridad legítima para tener acceso a los datos y revelarlos. Cuando se trata de datos no disponibles públicamente, los investigadores se enfrentan con un dilema. Si no copian rápidamente esos datos, los delincuentes normalmente los borrarán. Si los copian sin solicitar previamente la autorización del Estado en que se encuentren, se plantearán problemas graves con respecto a la soberanía de ese Estado y la protección de los derechos de las personas con interés en la incautación de esos datos. Los principios convenidos por el Grupo de los Ocho comprenden una solicitud de asistencia judicial recíproca acelerada. Se pediría al Estado en que se encontraran los datos que adoptara medidas inmediatas para preservarlos, en espera de un auxilio más oficial, a fin de asegurar su incautación y revelación al Estado solicitante. La transferencia de los datos al Estado solicitante se realizaría entonces utilizando los procedimientos y salvaguardias más tradicionales de la asistencia judicial recíproca.

8. Se están examinando también principios básicos para el rastreo de las comunicaciones en las redes informáticas. La mayoría de los proveedores de servicios mantienen registros electrónicos de la fuente y el destino de comunicaciones como el correo electrónico, pero sólo por períodos limitados. En la mayoría de los países, sólo se puede acceder a los registros que pueden utilizarse para rastrear las comunicaciones e identificar a los usuarios del sistema utilizando operaciones de busca e incautación judicialmente controladas. Ello no plantea un obstáculo grave para rastrear la mayoría de las comunicaciones nacionales, pero en los casos transnacionales las demoras aumentan por la necesidad adicional de formular las solicitudes por los cauces de la asistencia judicial recíproca. Este problema es conocido por los delincuentes que utilizan técnicas avanzadas, los cuales se aprovechan de ellas dirigiendo sus comunicaciones a

través de un gran número de países entre la fuente y el destino, o a través de países en donde no hay leyes o infraestructura para realizar rastreos con éxito, a fin de ocultar el verdadero origen o destino de sus comunicaciones.

9. Para facilitar una rápida cooperación entre los organismos encargados de aplicar la ley en los casos transnacionales, el Grupo de Lyon recomendó el establecimiento de una red de contactos en cada Estado a la que pudiera recurrirse las 24 horas diarias y los siete días de la semana, a fin de que prestara asistencia competente en la investigación. La red se compuso inicialmente de los Estados Miembros del Grupo de los Ocho, pero actualmente se ha ampliado a 19 países, y su competencia operacional se ha transferido a la Organización Internacional de Policía Criminal (Interpol).

10. Para armonizar los intereses oficiales y del sector privado, el Grupo de los Ocho ha celebrado varias conferencias en cooperación con la industria[6]. En general, los representantes de la industria comprenden empresas que fabrican equipo informático y de telecomunicaciones, programas informáticos y otros elementos de infraestructura, y empresas que prestan servicios a los usuarios individuales. En las deliberaciones se han examinado cuestiones relativas a la disposición y capacidad de las empresas para cooperar en la aplicación de la ley, la necesidad de prevenir el delito mediante la educación de los usuarios y la incorporación de elementos de seguridad en las tecnologías nuevas y en desarrollo.

3. Otras organizaciones internacionales o intergubernamentales

11. La cuestión de la delincuencia de alta tecnología y relacionada con las redes informáticas se ha tratado también por otras organizaciones intergubernamentales e internacionales, como tema distinto o en el contexto de otras consideraciones relacionadas con la delincuencia, como el blanqueo de dinero y la delincuencia organizada transnacional. El Commonwealth comenzó a examinar esas cuestiones en 1998, incluyendo el tema en el programa de una reunión de Ministros de Justicia del Commonwealth celebrada en mayo de 1999. Esa reunión estableció un grupo de trabajo de expertos en delincuencia informática y relacionada con las redes informáticas, para que elaborara una legislación modelo para los países del Commonwealth, pero aplazó sus trabajos sobre el proyecto hasta la conclusión de la Convención del Consejo de Europa sobre el delito cibernético. Los trabajos se reanudaron en julio de 2000 y se está preparando un proyecto de legislación modelo. El Commonwealth ha comenzado también a distribuir materiales sobre acontecimientos internacionales a sus Estados miembros y a examinar los sistemas del Commonwealth que se ocupan de los delincuentes fugitivos y la asistencia judicial recíproca para garantizar que esos sistemas amplíen las formas de cooperación necesarias en la nueva esfera de la delincuencia de alta tecnología.

12. La Interpol se ha ocupado también, estableciendo una serie de grupos de trabajo regionales sobre delincuencia de la tecnología de información. La investigación realizada y los materiales elaborados por la Interpol han solido reflejar las necesidades y preocupaciones de la aplicación de la ley. Entre los materiales para su utilización en la formación de investigadores se encuentra un manual para investigadores novatos y otro más complejo sobre delincuencia informática, que expone las técnicas y prácticas mejores para los investigadores avanzados. La Interpol tiene conciencia también de la necesidad de utilizar medios de alta tecnología para difundir información a los organismos encargados de aplicar la ley y está creando con ese fin un sitio web. Ha asumido la responsabilidad de mantener un directorio actualizado de la red de contactos establecida en un principio por el Grupo de Lyon. La Interpol proyecta nuevas actividades, especialmente en la esfera de la capacitación en materia de aplicación de la ley, y seguirá las actividades de otras organizaciones internacionales o participará en ellas, a fin de compartir informaciones y evitar la duplicación de esfuerzos.

B. Actividades de las Naciones Unidas

13. La cuestión de la delincuencia que utiliza tecnologías informáticas y de telecomunicaciones se ha tratado en las actividades de las Naciones Unidas y sigue examinándose activamente. Además del presente estudio, realizado de conformidad con la resolución 1999/23 del Consejo Económico y Social, de 28 de

julio de 1997[7], se han adoptado las siguientes medidas para tratar la cuestión:

a) En la resolución 45/109 de la Asamblea General, de 14 de diciembre de 1990, y en la resolución 1996/11 del Consejo Económico y Social, de 23 de julio de 1996, se insta a los Estados Miembros a emplear tecnologías informáticas modernas para la administración más eficaz y eficiente de las operaciones de la justicia penal y los sistemas de información. El Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrado en La Habana del 27 de agosto al 7 de septiembre de 1990, recomendó la elaboración de un instrumento internacional que se ocupara de la informatización de los sistemas de justicia penal[8]. La cuestión se trató en un curso práctico de dos días organizado durante el Noveno Congreso de las Naciones Unidas sobre Prevención del Delito y el Tratamiento del Delincuente, celebrado en El Cairo del 29 de abril al 8 de mayo de 1995, que señaló que era necesaria la informatización a fin de hacer frente a las nuevas formas de delincuencia, pero había inquietudes por la vida privada, los derechos humanos y la interoperabilidad de los sistemas dentro de los países y entre ellos. El curso práctico señaló también la necesidad de asistencia técnica, tanto en forma de recursos financieros como de expertos[9]. En general, el proceso se centró en la utilización de la informatización en la administración de justicia penal y la reunión de información estadística y no en la utilización de redes informáticas como instrumento investigador u operacional. Más recientemente se incorporaron a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional disposiciones para fomentar la utilización de las tecnologías modernas en la lucha contra el delito[10] y la distribución electrónica de documentos desempeñó un papel importante en el proceso de negociación;

b) El Octavo Congreso examinó también el problema de la delincuencia relacionada con las redes informáticas en sí[11] y recomendó una serie de medidas relativas a:

i) La modernización de los delitos nacionales, procedimientos de investigación, normas sobre la prueba, incautación o restitución, asistencia judicial recíproca y disposiciones sobre extradición, a fin de garantizar su ampliación a los casos que implicaran delitos relacionados con las redes informáticas;

ii) El mejoramiento de la seguridad informática y otras medidas técnicas de prevención del delito;

iii) La educación del público y la capacitación de funcionarios en la investigación, enjuiciamiento y decisión de casos que implicaran delitos relacionados con las redes informáticas;

iv) La elaboración y difusión de normas éticas en la utilización de los sistemas informáticos;

v) La elaboración de políticas para las víctimas de delitos relacionados con las redes informáticas, incluidas medidas para fomentar la denuncia de tales delitos;

c) Como recomendó el Octavo Congreso en su resolución 9, en 1994 se publicó el *Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos*[12] como recurso para investigadores y encargados de formular políticas, que ha sido ampliamente difundido en la Internet;

d) La cuestión de los delitos relacionados con las redes informáticas se incluyó también en el programa del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrado en Viena del 10 al 17 de abril de 2000. Durante el Décimo Congreso, el Instituto de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente, de las Naciones Unidas, organizó un curso práctico de un día sobre el tema[13]. El curso práctico consistió en cuatro debates de grupo sobre los siguientes temas: criminología de los delitos relacionados con las redes informáticas; problemas que acompañan a la búsqueda e incautación en redes informáticas; problemas que acompañan al rastreo de comunicaciones en las redes informáticas; y relaciones entre los organismos encargados de aplicar la ley y las industrias informáticas y de la Internet. Expertos destacados en la materia informaron a los participantes sobre cuestiones actuales y los progresos de los debates en el Consejo de Europa, el Grupo de los Ocho y otros foros. Además de representantes de los Estados participaron también, varios representantes de la industria. El curso práctico hizo varias recomendaciones, entre ellas un llamamiento a una mayor cooperación entre los gobiernos y la industria, el

aumento de la cooperación internacional en el rastreo de delincuentes y nuevas medidas de las Naciones Unidas en relación con la prestación de cooperación y asistencia técnica[14];

e) La Declaración de Viena sobre la Delincuencia y la Justicia: Frente a los Retos del Siglo XXI, aprobada por el Décimo Congreso[15] y, hecha suya por la Asamblea General en su resolución 55/59, de 4 de diciembre de 2000, trató también de la delincuencia de alta tecnología y relacionada con las redes informáticas. En el párrafo 18 de la Declaración de Viena, los Estados Miembros decidieron formular recomendaciones de políticas orientadas a la acción para la prevención y control de los delitos relacionados con la informática, y se comprometieron a esforzarse por aumentar su capacidad de prevenir, investigar y enjuiciar esos delitos. Se invitó a la Comisión de Prevención del Delito y Justicia Penal a que emprendiera el desarrollo de esas recomendaciones de políticas, teniendo en cuenta la labor en curso en otros foros. La Asamblea General, en su resolución 55/60, de 4 de diciembre de 2000, pidió ulteriormente a la Comisión que siguiera examinando las conclusiones y recomendaciones recogidas en la Declaración de Viena y el informe del Décimo Congreso, y pidió al Secretario General que, en consulta con los Estados Miembros, preparase proyectos de plan de acción para su examen por la Comisión en su 10º período de sesiones;

f) Además de su participación en la preparación del curso práctico celebrado durante el Décimo Congreso sobre los delitos relacionados con las redes informáticas, el Instituto de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente, de las Naciones Unidas, ha organizado una serie de reuniones y cursos prácticos para señalar cuestiones y fijar un programa de actividades ulteriores. Ha realizado una encuesta entre los Estados Miembros sobre cuestiones que implican delitos relacionados con las redes informáticas, cuyos resultados son inminentes. Actualmente está recopilando y publicando también los materiales utilizados por las Naciones Unidas y los participantes individuales en el curso práctico celebrado durante el Décimo Congreso. Sus planes futuros se centran en la elaboración y difusión de información práctica para la investigación y enjuiciamiento de los delitos relacionados con las redes informáticas;

g) La Comisión, en su 10º período de sesiones, tendrá ante sí un informe del Secretario General sobre proyectos de plan de acción para la aplicación de la Declaración de Viena sobre la Delincuencia y la Justicia: Frente a los Retos del Siglo XXI (E/CN.15/2001/5). El informe del Secretario General trata también de los delitos de alta tecnología y relacionados con las redes informáticas, e incluye una serie de recomendaciones de políticas y medidas específicas que podrían adoptarse a fin de aumentar la capacidad, en los niveles nacional e internacional, para prevenir, investigar y enjuiciar esos delitos. Esas recomendaciones y medidas se basan en los materiales que se examinan en el presente informe;

h) La Asamblea General, en su resolución 55/63, de 4 de diciembre de 2000, toma nota del valor de los esfuerzos para luchar contra la utilización de la tecnología de la información con fines delictivos. Esos esfuerzos incluirían lo siguiente: eliminación de los refugios seguros para los delincuentes; cooperación en la vigilancia del cumplimiento de la ley en los casos internacionales; intercambio de información; capacitación y equipo adecuado del personal; protección del carácter confidencial; conservación y rápido acceso a los datos relativos a investigaciones criminales; mantenimiento de regímenes de asistencia jurídica mutua; aumento de la sensibilización del público con respecto al problema; diseño de sistemas de información para prevenir el delito y facilitar su investigación; y consideración de la necesidad de proteger las libertades individuales y el derecho a la intimidad al mismo tiempo que se preserva la capacidad de los gobiernos para combatir la utilización de la tecnología de la información con fines delictivos. La Asamblea decidió también mantener la cuestión de la utilización de la tecnología de la información con fines delictivos en el programa de su quincuagésimo sexto período de sesiones;

i) Por su resolución 55/25, de 15 de noviembre de 2000, la Asamblea General aprobó la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y dos protocolos a ella (resolución 55/25, anexos I a III). La Convención no se aplica en los casos en que los delitos de que se trate no sean delitos graves, cuando no participe un grupo delictivo organizado, o cuando no haya un elemento de transnacionalidad en ninguno de los delitos de que se trate[16], lo que excluiría algunos delitos electrónicos. Sin embargo, se aplicaría cuando

los delincuentes utilizaran redes informáticas o de telecomunicaciones para apoyar formas más tradicionales de delincuencia organizada transnacional. El apartado h) del párrafo 1 del artículo 29 pide concretamente que se adopten medidas nacionales y se utilice asistencia técnica para combatir la delincuencia organizada nacional mediante computadoras, redes de telecomunicaciones u otras formas de la tecnología moderna;

j) A raíz de la aprobación de la Convención, otro curso práctico sobre el tema "El desafío del delito cibernético sin fronteras" formó parte del Simposio sobre el imperio de la ley en la aldea global: cuestiones de soberanía y universalidad, organizado en el marco de la Conferencia política de alto nivel para la firma de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos, celebrada en Palermo (Italia) del 12 al 15 de diciembre de 2000. Los temas tratados incluyeron los delitos relacionados con las redes informáticas y otras formas de delincuencia transnacional para las que se consideraban cada vez más insuficientes los controles basados exclusivamente en el derecho interno. Se señaló que esa delincuencia iba aumentando al proliferar las tecnologías en que se basaba y a medida que la comisión de delitos transfronterizos se hacía más fácil. Se consideró que la legislación a nivel nacional y un instrumento internacional amplio eran elementos importantes de una solución, pero se expresó también preocupación por el peligro de elaborar disposiciones legales prematuramente. El problema podía abordarse asimismo en parte utilizando medios como la seguridad técnica, la educación y la preparación de normas éticas para la utilización de las nuevas tecnologías. El curso práctico sugirió también que la gama de delitos cibernéticos podía desglosarse en las siguientes categorías básicas: acceso no autorizado a computadoras o sistemas informáticos; destrucción o alteración de datos; interferencia con la utilización legítima de computadoras o sistemas informáticos; robo de activos intangibles; y obtención de ganancias mediante el engaño.

C. Naturaleza de los delitos relacionados con las redes informáticas y de alta tecnología: tipología preliminar

14. El fenómeno de los delitos de alta tecnología y relacionados con las redes informáticas requiere la tipificación de delitos totalmente nuevos y la modificación de los tipos de delitos existentes para garantizar que se apliquen a la utilización abusiva de las nuevas tecnologías. Ha habido que examinar nuevas formas de comportamientos perjudiciales a fin de determinar si la aplicación del derecho penal resultaba apropiada como respuesta, y si el comportamiento de que se trataba debía considerarse siquiera como delito. Está surgiendo un consenso internacional con respecto al núcleo esencial de los comportamientos más graves y perjudiciales, pero quedan algunas esferas que algunos Estados consideran delitos, pero no todos. Los dos ejemplos principales son los problemas de propiedad intelectual, como la copia no autorizada de programas informáticos o de datos, y el problema de qué es lo que se denomina contenido ofensivo.

15. La explotación delictiva de las nuevas tecnologías ha llevado a formas totalmente nuevas de delito. En otros casos, formas de delito más tradicionales se cometen de nuevos modos que aumentan los beneficios o disminuyen los riesgos para los delincuentes. Una tercera categoría básica de actividad delictiva consiste en la utilización más general de las tecnologías por los delincuentes para organizar, comunicar y proteger de la vigilancia sus actividades. Entre otras esferas básicas de clasificación propuestas se encuentra la clasificación según si los delitos se cometen por los delincuentes para obtener ganancias económicas o materiales o por otros motivos, y si esos delitos implican otros delitos cometidos contra sistemas informáticos o de comunicaciones, o la utilización de esas tecnologías para hacer víctimas a otras personas.

16. A continuación se describen tipos básicos de delitos de alta tecnología y relacionados con las redes informáticas.

1. Delitos cometidos contra las tecnologías y sus usuarios

a) Obtención de acceso no autorizado a computadoras o sistemas informáticos

17. En la mayoría de los casos, la obtención de acceso no autorizado a computadoras o sistemas informáticos se considera como delito a causa de la preocupación por la invasión de la intimidad de los usuarios legítimos a cuyos datos se tiene acceso, y porque el acceso no autorizado acompaña a menudo a otros delitos o interfiere el uso legítimo del sistema.

b) Utilización no autorizada de sistemas informáticos

18. La utilización no autorizada de sistemas informáticos se superpone con el acceso no autorizado, ya que deben utilizarse los sistemas para obtener ese acceso. Sin embargo, una vez obtenido ese acceso, los sistemas se utilizan también para cometer otros delitos o para ocultar la verdadera identidad del delincuente. La utilización no autorizada se tipifica normalmente como delito porque la utilización de tiempo o servicios informáticos constituye un producto evaluable que los delincuentes no pagan y del que, en algunos casos, se priva a los usuarios legítimos que pagan honorarios.

c) Lectura, copia o utilización de datos sin autorización

19. Como en el robo tradicional, el daño de leer, copiar o tomar datos sin autorización consiste en una pérdida de valor para la víctima y una ganancia indebida para el delincuente. Sin embargo, en el caso de los datos esos aspectos son distintos, ya que los datos pueden copiarse sin borrarlos. El acto puede tipificarse también como una forma de invasión de la intimidad.

d) Creación o propagación de programas hostiles

20. Los virus, “gusanos” y otros programas informáticos interfieren el funcionamiento de los sistemas, al consumir capacidad de procesar y almacenar. En la mayoría de los casos se propagan también a sí mismos utilizando el correo electrónico o la transferencia de disquetes contaminados, de forma que los delincuentes pierden rápidamente el control del ámbito de los daños causados, una vez liberado el programa. Muchos programas hostiles infligen también daños reales a los datos, borrando o deformando los archivos. El daño, que puede ser considerable, consiste en la pérdida de operaciones del sistema, la pérdida de datos valiosos y el costo de eliminar los programas y restablecer las funciones del sistema.

e) Vandalismo o sabotaje informáticos

21. Los daños pueden causarse directamente por los delincuentes que han obtenido acceso no autorizado, intencionalmente o no, al tratar de utilizar el sistema o de ocultar el hecho de haber obtenido acceso a él. Esos delitos se cometen también en algunos casos por personas que tienen acceso autorizado al sistema de que se trate. La categoría comprende los ataques de denegación de servicios, en los que el delincuente obtiene acceso no autorizado a gran número de computadoras en red y las utiliza para bombardear el sistema que constituye su objetivo con datos aleatorios, sobrecargando el sistema y haciendo que se colapse. Ello puede constituir simple vandalismo o utilizarse como distracción para ocultar otros delitos, al desactivar mecanismos de seguridad técnica. También pueden utilizarse programas hostiles, como los virus, para actos específicos de vandalismo o sabotaje, pero estos actos pueden distinguirse de las acciones directas de los delincuentes porque, una vez que se propagan, normalmente producen efectos indiscriminados.

2. Delitos tradicionales cometidos mediante la utilización de tecnologías informáticas o de comunicaciones

a) Delitos que implican un contenido ofensivo

22. Los delitos que implican un contenido ofensivo consisten en la utilización de los sistemas informáticos para producir o difundir imágenes, textos u otra información que son objeto de sanciones penales. Hay discrepancias entre los tipos de contenido tipificados como delitos en los distintos Estados. La mayoría de los Estados penalizan actualmente la creación o distribución de pornografía infantil, pero hay menos consenso con respecto a qué materiales se consideran obscenos, pornográficos o blasfemos, o propaganda del

odio. La protección de los principios constitucionales de los derechos humanos, incluida la libertad de expresión o palabra, limita el grado en que muchos Estados pueden tipificar penalmente algunas formas de contenidos.

b) Secuestro relacionado con la Internet

23. Los delincuentes pedófilos han comenzado a utilizar la Internet como medio para tener acceso a los niños sin revelar su verdadera identidad. Inician diálogos en espacios de conversación electrónica y, una vez que ganan su confianza, organizan un encuentro personal y secuestran a la víctima. Los funcionarios encargados de aplicar la ley han detenido a algunos delincuentes haciéndose pasar por niños en la Internet. En algunos casos, los delincuentes han inducido a sus víctimas a borrar archivos que registraban sus conversaciones, a fin de ocultar las pruebas del secuestro.

c) Fraude

24. La categoría de fraude incluye la mayoría de los delitos en que se envían indebidamente fondos electrónicamente o se dan informaciones falsas a los usuarios de las tecnologías, a fin de privarlos de fondos o activos. Esos delitos pueden cometerse por personas de la propia empresa, como empleados, o por personas no pertenecientes a ella, utilizando un acceso no autorizado a sistemas privados o introduciendo información falsa en sistemas públicos. Se prevé que el fraude y otros delitos económicos aumentarán considerablemente a medida que se extienda el comercio electrónico. Un problema creciente en esta esfera es la utilización de tecnologías para manipular los mercados financieros.

d) Espionaje comercial o industrial

25. El aumento de la utilización por las empresas de sistemas de redes informáticas para crear y transferir información las ha hecho también objetivo del espionaje industrial. Ese espionaje puede realizarse para obtener acceso no autorizado desde el exterior, o por personas de la propia empresa, que utilizan tecnologías para reunir información valiosa y enviarla a competidores, sin ser descubiertas.

e) Delitos contra la propiedad intelectual

26. La capacidad de las nuevas tecnologías para almacenar, transmitir y copiar información hace que la copia y utilización no autorizadas sean una importante esfera de inquietud. Sin embargo, no todos los Estados tratan esos actos como cuestiones penales. Algunos los consideran cuestiones civiles entre las partes directamente participantes.

f) Juego

27. La creación de infraestructura para apoyar el comercio electrónico en pequeña escala ha permitido también el juego por medio de la Internet. El derecho penal interviene cuando sitios web situados en jurisdicciones en donde el juego es legal son utilizados por jugadores de otras jurisdicciones en que constituye un delito. Prescindiendo de consideraciones morales, el juego se reglamenta a menudo para obtener ingresos fiscales y lograr una inspección que excluya la delincuencia organizada y proteja del engaño a los jugadores. Más recientemente, el juego por medio de la Internet se considera también como un posible medio para realizar operaciones de blanqueo de dinero.

g) Blanqueo de dinero

28. Se prevé que el actual aumento del comercio electrónico y de otras actividades comerciales que utilizan redes informáticas creará numerosas oportunidades de blanqueo de dinero. En general, las tecnologías permiten a los delincuentes ocultar su verdadera identidad y ubicación, aprovechar las diferencias entre las jurisdicciones utilizando cuentas extranjeras o jurisdicciones múltiples, y ocultar la verdadera naturaleza de sus transacciones utilizando tecnologías como el cifrado. En algunos casos pueden intervenir otros delitos, como el juego o el fraude[17].

3. Utilización de las tecnologías para apoyar otras actividades delictivas

29. En general, las modernas redes informáticas y de telecomunicaciones y otras tecnologías análogas ofrecen a las organizaciones delictivas las mismas ventajas que a las empresas legítimas. Entre esas ventajas se encuentran comunicaciones mundiales

rápidas, fiables y de bajo costo, que en la mayoría de los casos están más seguras contra la intercepción o la vigilancia exteriores que los métodos más tradicionales. La naturaleza de las redes y las mayores velocidades y volúmenes de datos transferidos hacen intrínsecamente más difícil que los organismos encargados de aplicar la ley intercepten las comunicaciones individuales. Los productos de seguridad especializados, como cortafuegos y programas de cifrado, protegen las comunicaciones delictivas de la intercepción o la intrusión, tan eficazmente como protegen las comunicaciones legítimas. Tecnologías de redes pueden servir de apoyo también, en algunos casos, a formas totalmente nuevas de organización delictiva. El ejemplo más comúnmente citado es el de los delincuentes pedófilos, que pueden localizarse mutuamente y compartir pornografía infantil sin dejar de permanecer anónimos, y cooperar también de formas no comprendidas en los conceptos o definiciones existentes de delincuencia organizada. Organizaciones delictivas más tradicionales pueden encontrar asimismo nuevas oportunidades de identificar y cooperar con delincuentes de otras regiones o países.

D. Evaluación del alcance y los costos de los delitos relacionados con las redes informáticas y de alta tecnología

30. A medida que las redes informáticas y de telecomunicaciones han aumentado de alcance y complejidad, el número de personas que las utilizan y el grado de dependencia de ellas han aumentado también espectacularmente. En un informe a la Asamblea de las Naciones Unidas dedicada al Milenio, el Secretario General señaló que, desde su comienzo en los primeros años del decenio de 1990, la Internet había llegado a 143 millones de usuarios en 1998, y se esperaba que, en 2001, había 700 millones de personas conectadas. El mercado del comercio electrónico, fenómeno más reciente, había alcanzado un valor total de 2.600 millones de dólares de los Estados Unidos en 1996, y se esperaba que en 2002 aumentaría hasta los tres mil millones de dólares[18]. Hay pocas estadísticas amplias relativas a los delitos de alta tecnología o relacionados con las redes informáticas, pero las pruebas anecdóticas y las estadísticas disponibles sugieren que el ámbito de esos delitos está aumentando al crecer el número de posibles delincuentes y víctimas conectados[19]. La gama de actividades delictivas parece estar aumentando también a medida que las tecnologías crean nuevas oportunidades delictivas y que los delincuentes encuentran nuevas formas de aprovecharlas. Actualmente preocupa en particular la rápida expansión del comercio electrónico y de su infraestructura de apoyo, que pueden ir acompañados de los consiguientes aumentos de los delitos económicos relacionados con las redes informáticas, como el fraude, la manipulación de mercados financieros y el blanqueo de dinero.

31. A medida que aumenta el grado de confianza puesta en las redes, aumentan también los posibles daños de los delitos. La mayoría de los países industrializados, en donde la confianza es mayor, consideran ahora las redes informáticas y de telecomunicaciones, y su infraestructura de apoyo, como posibles objetivos para el terrorismo. Los ataques a los sistemas informáticos por motivos estratégicos o políticos son todavía raros, pero actos delictivos basados en otros motivos causan regularmente daños en gran escala, en algunos casos desproporcionados con los realmente previstos por los autores. Entre los ejemplos recientes se encuentra la creación y propagación del virus “Melissa”, en marzo de 1999, que causó más de 10 millones de dólares en daños directos solamente en los Estados Unidos, y del virus *“I love you”*, en mayo de 2000, cuyos daños se estiman entre 7.000 millones y 10.000 millones de dólares, y que infectó hasta 45 millones de computadoras en todo el mundo. En otro incidente, una serie de ataques de denegación de servicios, se bombardearon sitios web con grandes volúmenes de datos sin sentido, lo que provocó el colapso de 1.200 sitios, incluidos los de nuevas organizaciones y los de comercio electrónico, en menos de dos horas. Las pérdidas causadas por esos incidentes, en particular los que entrañan virus, se combinan en la mayoría de los casos, cuando otros delincuentes copian el virus, lo alteran para ocultar su carácter a los usuarios o los programas de filtrado, y vuelven a propagarlos[20].

32. Las pérdidas reales son difíciles de cuantificar, pero incluyen los costos directos de reparar sistemas y programas, la pérdida de acceso o servicios para los usuarios con los daños consiguientes, la pérdida de datos valiosos y la pérdida de ingresos procedentes de la explotación de sitios. Esos delitos necesitan también la preparación y mantenimiento de medidas de

seguridad y de otras medidas preventivas, como factor de costo añadido. Los aumentos generales de esos delitos y el carácter espectacular de algunos de ellos generan también presiones políticas considerables pero imprevisibles para mejorar los controles de derecho penal, sanciones más severas, y precauciones técnicas por parte de los productores de programas y equipos electrónicos y de las compañías que proporcionan acceso a la Internet a sus clientes. Otro costo oculto de esos incidentes es el miedo al delito cibernético, que puede perjudicar a la utilización de las tecnologías o disuadir a los gobiernos y poblaciones de los países en desarrollo de hacer un uso más eficaz de ellas.

33. La búsqueda de análisis fiables de la naturaleza y el ámbito de los delitos mismos es también difícil. Quedan todavía cuestiones abiertas con respecto a sí algunas formas de comportamiento deben penalizarse en absoluto y, en caso afirmativo, cómo deben definirse y clasificarse. Todo sistema de clasificación depende también en parte, de las tecnologías de que se trate lo que plantea además problemas de definición. Tecnologías como las de redes informáticas, sistemas de radiodifusión por cable y teléfonos celulares y tradicionales se están haciendo rápidamente indistinguibles a medida que aumenta la utilización de las redes informáticas y que sistemas más tradicionales adoptan tecnologías digitales. Un ejemplo actual es el del llamado *palm-pilot*, que combina aspectos de la telefonía celular, la radiodifusión por red y el acceso a las redes informáticas. Ello será un desafío para los investigadores, analistas de políticas y redactores de textos legales en un futuro previsible, y ha llevado a que se hagan llamamientos para la utilización de conceptos tecnológicamente neutrales y de un lenguaje que garantice que se evitarán lagunas e incoherencias.

34. La reunión de estadísticas exactas presenta también problemas aunque los delitos se tipifiquen claramente. La mayoría de los expertos creen que formas comunes de delitos relacionados con las redes informáticas no son suficientemente denunciadas, porque las víctimas no comprenden que lo han sido, quizá no comprenden que el comportamiento de que se trata es un delito, o bien pueden decidir no querellarse para evitar molestias o no perjudicar a la solvencia de la empresa. Otros problemas se derivan de la victimización masiva causada por delitos como la propagación de virus, porque el número de las víctimas es sencillamente demasiado grande para poder ser determinado y contado, y porque esos programas pueden seguir creando nuevas víctimas mucho tiempo después de haber sido capturados y castigados los delincuentes. Otro factor que complica la reunión y comparación de estadísticas nacionales del delito es el hecho de que los delitos transnacionales relacionados con las redes informáticas se cometan, por definición, o surtan efectos en dos Estados al menos y, en algunos casos, en muchos, lo que presenta el riesgo de denuncias múltiples o de la falta total de denuncias.

III. Conclusiones y recomendaciones: elaboración de políticas mundiales para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas

A. Necesidad de tratar los delitos de alta tecnología y relacionados con las redes informáticas como tema distinto

35. Las actividades delictivas examinadas en el presente informe están vinculadas por tecnologías subyacentes que comparten muchas características. Algunas son actividades nuevas, creadas y definidas por las propias tecnologías, mientras que otras son formas de delito más tradicionales que han sido considerablemente influidas por esas tecnologías. Muchas cuestiones fundamentales de políticas, como la de lograr un equilibrio adecuado entre los derechos humanos y las facultades de investigación, y entre los intereses nacionales e internacionales, son comunes a todas las formas de delitos de alta tecnología y relacionados con las redes informáticas. En un nivel más práctico, los problemas con que se enfrentan investigadores y fiscales, como localizar e identificar a los delincuentes e incautar, preservar, autenticar y utilizar pruebas informáticas o electrónicas ante los tribunales, son sustancialmente los mismos cualquiera que sea la naturaleza de los delitos. Por ello, se recomienda que esta esfera se trate como un tema distinto a efectos de investigación y de cualesquiera deliberaciones multilaterales futuras. Hay que señalar, sin embargo, que muchas preocupaciones que están surgiendo, como la difusión de pornografía infantil, el fraude y otros delitos financieros, requerirán también la aportación de expertos familiarizados con los

delincuentes de que se trate y con sus métodos específicos.

B. Necesidad de ayudar a los países en desarrollo

36. Una gran parte del debate de políticas sobre los sistemas informáticos y los delitos relacionados con las redes informáticas se ha desarrollado hasta ahora en países con sectores de alta tecnología bien desarrollados, y entre esos países. Los países desarrollados tienen intereses considerables que pueden verse perjudicados por los delitos relacionados con las redes informáticas. Cuentan con amplias inversiones del sector público y del sector privado en las tecnologías, y con poblaciones que dependen cada vez más de la utilización de las redes informáticas. Sin embargo, también están en juego los intereses de los países en desarrollo. Las nuevas tecnologías representan una importante oportunidad de promover los intereses sociales, económicos y de otra índole de los países en desarrollo[21], pero podrían agravar también las disparidades existentes, si esos países no aprovecharan plenamente la oportunidad. A este respecto, tanto los delitos relacionados con las redes informáticas como los esfuerzos de los países desarrollados y de las industrias de alta tecnología para luchar contra esos delitos pueden convertirse en un obstáculo para el desarrollo si los países en desarrollo no pueden participar eficazmente en los debates. Su aportación es necesaria para definir y articular plenamente sus intereses, determinar las necesidades de asistencia técnica y de otra índole en las distintas etapas del proceso, elaborar medidas de prevención y lucha contra el delito que sean viables en todas las sociedades, y garantizar la aplicación plena y eficaz de esas medidas.

37. La aplicación casi universal de medidas eficaces de lucha contra el delito será necesaria porque las nuevas tecnologías pueden ser explotadas por delincuentes casi sin ninguna de las restricciones que imponen a los delincuentes tradicionales las fronteras nacionales. Mientras que los delincuentes tradicionales se ven limitados por factores como la distancia geográfica, los controles aduaneros y la necesidad de tener acceso físico a sus víctimas, los delincuentes electrónicos pueden operar remotamente y con una impunidad real desde cualquier jurisdicción que carezca de legislación suficiente o de la voluntad o la capacidad de aplicarla, o a través de una de esas jurisdicciones. Una amplia representación y una participación efectiva serán esenciales a fin de que las políticas y las medidas elaboradas resulten viables para todos los países y todos ellos estén dispuestos a aplicarlas eficazmente y puedan hacerlo.

38. Garantizar la participación efectiva exigirá la asistencia de los países desarrollados en las distintas etapas del proceso. Al principio, se necesitará la aportación de los países en desarrollo para evaluar sus intereses en las propias tecnologías y la forma en que esos intereses pueden ser afectados por la delincuencia relacionada con las redes informáticas y los esfuerzos para combatirla. Eso hace que la asistencia en las primeras etapas sea especialmente importante. Algunos países llevan cierto tiempo activamente dedicados, pero para muchos las tecnologías son todavía poco conocidas y no han examinado a fondo los problemas técnicos, jurídicos y de políticas que pueden surgir. Incluso con asistencia, el desarrollo de esos conocimientos especializados requiere tiempo. Por ello, es importante que esa asistencia comience tan pronto como sea posible y continúe el tiempo suficiente para garantizar una participación efectiva mientras se delibera. A la larga, necesitará también asistencia técnica continuada para mantener la eficacia operativa. El hecho de que las tecnologías y los delitos que dependen de ellas sigan evolucionando requerirá un esfuerzo mundial para seguir los nuevos acontecimientos, elaborar respuestas eficaces y difundirlas con suficiente rapidez para que los organismos encargados de aplicar la ley y los fiscales se mantengan a la altura de los delincuentes o se les anticipen.

39. En consecuencia, se recomienda que se realicen esfuerzos inmediatos para evaluar las necesidades de asistencia técnica de los países en desarrollo que la requieran y satisfacerlas tan rápidamente como sea posible. Esa evaluación debe hacerse en el contexto de las estrategias de desarrollo electrónico de esos países y del aumento de la utilización mundial de tecnologías para sistemas informáticos y de telecomunicaciones y para la prevención del delito. Debería hacerse también en consulta con empresas del sector privado dedicadas a esas tecnologías y, cuando fuera posible, con su asistencia. Entre los elementos importantes de la evaluación en términos mundiales estará la

identificación de tecnologías de importancia crítica y la fijación de prioridades.

C. Necesidad de examinar medidas internacionales, nacionales y del sector privado

40. Los expertos reconocen universalmente que el carácter internacional de las modernas tecnologías informáticas y de telecomunicaciones ha llevado a nuevas formas de delincuencia transnacional y multinacional. El concepto de espacio cibernético y la facilidad con que actos delictivos realizados en un lugar geográfico pueden tener efectos en otros lugares hace esencial la integración de las medidas nacionales e internacionales. Sin esa integración, las contramedidas pueden ser ineficaces contra el delito, y tener consecuencias perjudiciales no pretendidas, cómo disuadir a las poblaciones de la utilización de nuevas tecnologías, el menoscabo de los derechos humanos o la creación de discrepancias en competitividad o desarrollo industriales.

41. El papel destacado desempeñado por la industria en la elaboración y mantenimiento de las tecnologías hace también importante la integración de las medidas públicas y del sector privado. Los intereses del sector privado apoyan en general la lucha eficaz contra el delito, pero sus motivaciones, que suelen ser comerciales y no políticas, y sus métodos, que son de naturaleza técnica más que jurídica, deben armonizarse y, cuando sea posible, integrarse en los esfuerzos nacionales e internacionales de los gobiernos.

D. Función de las Naciones Unidas

42. Como parte de la preparación para la Asamblea de las Naciones Unidas dedicada al Milenio, se pidió al Consejo Económico y Social que examinara la función de la tecnología de la información en las esferas del desarrollo y la cooperación internacional. El Consejo llegó a la conclusión de que el desarrollo y la difusión de las nuevas tecnologías de información eran en gran parte autosostenidos, pero las Naciones Unidas podrían ayudar en ese proceso de formas importantes[22]. Entre ellas estaban ayudar a los países en desarrollo a mantenerse a la par de los nuevos acontecimientos, en particular en regiones o esferas en que no era probable que la evolución dirigida por el mercado satisficiera sus necesidades, y ayudando a desarrollar tecnologías específicas que pudieran producir beneficios sociales pero no fueran necesariamente viables desde el punto de vista comercial. Con carácter más general, llegó a la conclusión de que la función esencial de las Naciones Unidas era crear consenso y asociaciones entre los participantes en el proceso, incluidos gobiernos, instituciones académicas y empresas del sector privado. La finalidad de ese consenso era reunir los conocimientos especializados y recursos necesarios para que todo el mundo tuviera acceso a las nuevas tecnologías de la información y oportunidad de beneficiarse de ellas.

43. Los delitos de alta tecnología y relacionados con las redes informáticas constituyen un obstáculo importante tanto para el acceso como para los posibles beneficios de lo que el Consejo denominó una economía mundial basada en el conocimiento, y la tarea de formar un consenso será igualmente importante en la esfera del control de la delincuencia. Existe ya acuerdo general en la necesidad de medidas eficaces de lucha contra el delito entre los Estados con inversiones y confianza importantes en las tecnologías, pero se trata sólo del comienzo del proceso. La elaboración de medidas específicas requerirá la evaluación y conciliación de numerosas cuestiones económicas, sociales, culturales y jurídicas. La elaboración y la aplicación de muchas medidas de lucha contra el delito tendrá que ser apoyada por un consenso casi universal y por niveles suficientes de capacidad técnica en casi todos los países, para que sean efectivas. El consenso debería extenderse no sólo a los países y sus gobiernos sino también a los intereses amplios y multinacionales del sector privado.

44. En un futuro inmediato, es importante que se reúna y difunda información exacta sobre la naturaleza y el alcance del problema y las opiniones de los Estados Miembros sobre lo que habría que hacer, a fin de que los Estados puedan examinar opciones y dar instrucciones a las Naciones Unidas sobre la forma de actuar. Las organizaciones intergubernamentales mencionadas en el presente informe, así como algunos gobiernos individuales, han comenzado ya el proceso de compartir con otros Estados los conocimientos legislativos, judiciales, técnicos y de aplicación de la ley que han elaborado, tanto en general como en el contexto de casos individuales de delitos transnacionales importantes. Esa actividad debe ampliarse, tanto en alcance como en el número de

países participantes, pero para ello hará falta una evaluación exacta de las necesidades existentes y de los recursos disponibles para atender esas necesidades.

45. Por ello se recomienda que el Centro de las Naciones Unidas para la Prevención Internacional del Delito, de la Oficina de Fiscalización de Drogas y Prevención del Delito de la Secretaría, reciba instrucciones de realizar un estudio más detenido del problema, para su presentación a la Comisión de Prevención del Delito y Justicia Penal en su 11º período de sesiones. A continuación se examinarán posibles temas para ese estudio, que debería incluir al menos una encuesta de las necesidades básicas de los Estados Miembros, su disposición para ayudar mediante la aportación de recursos financieros y de conocimientos técnicos, y su opinión sobre la forma de dar una respuesta mundial al problema y la forma que esa respuesta debería adoptar.

46. Se recomienda además que se cree un grupo de expertos intergubernamental de composición abierta para que examine ese estudio y prepare opciones y recomendaciones para nuevo examen y adopción de medidas por la Comisión en su 11º período de sesiones. Como se señala *supra*, la participación de una gama completa de países es importante en todas las etapas del proceso. Es importante que el grupo sea de base tan amplia como se pueda y, en particular, que incluya representantes de los países en desarrollo. Por ello, se recomienda que esa participación sea apoyada por contribuciones voluntarias de otros Estados en la mayor medida posible.

47. Se recomienda además que se establezca un programa mundial contra los delitos de alta tecnología y relacionados con las redes informáticas, una vez que se haya terminado el estudio y se conozcan las opiniones del grupo de expertos, y que los Estados interesados aporten contribuciones voluntarias para establecer y apoyar ese programa. La recomendación se examina detenidamente en la sección F *infra*.

48. A la larga, muchos expertos opinan que nada que no sea un instrumento jurídico amplio y mundial contra los delitos de alta tecnología y relacionados con las redes informáticas bastará para establecer las políticas, facultades, procedimientos y mecanismos de cooperación internacional necesarios para tratar eficazmente los delitos transnacionales relacionados con las redes informáticas. Sin embargo, las opiniones son diversas con respecto a la rapidez con que podrá elaborarse un instrumento de esa índole. Como se señala en la sección B *supra*, hace falta que una gama más amplia de países participe pronto en el proceso. Hay también importantes cuestiones que habría que resolver al elaborar ese instrumento, por ejemplo, las relativas a la soberanía nacional, la aplicación de salvaguardias judiciales y de otras salvaguardias de derechos humanos y el papel de los intereses del sector privado en las medidas para promover la seguridad y la lucha contra los delitos informáticos. Esas cuestiones pueden examinarse al evaluar opciones, tanto para el proceso de elaboración de un instrumento como para su posible forma y contenido. En general, un instrumento que contenga disposiciones más amplias y vinculantes sería más eficaz, pero sería más largo de negociar y resultaría más difícil y engorroso de aplicar para muchos Estados. En la etapa actual no se puede llegar a conclusiones, pero se recomienda al grupo de expertos que examine opciones procesales y sustantivas con respecto a un instrumento internacional y formule recomendaciones como parte de su informe a la Comisión en su 11º período de sesiones.

49. Otro factor que debe considerarse es el hecho de que los delitos de alta tecnología y relacionados con las redes informáticas parecen estar aumentando rápidamente de frecuencia, ámbito geográfico y complejidad técnica, proceso que parece probable continúe, en paralelo con el rápido desarrollo y la proliferación de nuevos medios informáticos, de redes y de telecomunicaciones. Esa perspectiva indica que, aunque un instrumento jurídico mundial puede constituir una importante respuesta a largo plazo, quizá sean necesarias también medidas eficaces en un futuro más inmediato. Por ello, se recomienda que se pida asimismo al grupo de expertos que elabore otras opciones para una estrategia mundial a corto plazo contra los delitos de alta tecnología y relacionados con las redes informáticas, centrándose en esferas como la asistencia jurídica y técnica en general y en casos específicos; la fijación de normas técnicas para cuestiones como la reunión, preservación, autenticación y revelación de pruebas electrónicas; y el establecimiento de centros o puntos de contacto para las solicitudes de asistencia. A este respecto, debería tomarse en consideración la labor que se está realizando ya en las organizaciones mencionadas en la subsección A de la sección II del presente informe.

E. Elementos de un estudio detallado

50. En el estado actual de los conocimientos, el campo de la delincuencia relacionada con las redes informáticas sigue planteando más preguntas que respuestas, y se necesitan más estudios para definir la materia, determinar los intereses afectados y la forma en que lo son, y definir opciones políticas para el futuro. El estudio abarcaría al menos los siguientes elementos:

a) Se debería conocer las opiniones de los Estados sobre el carácter y el ámbito del problema y las posibles respuestas nacionales e internacionales;

b) Se debería consultar a Estados que representaran una gama completa de características industriales, jurídicas, sociales y económicas;

c) Se debería examinar tanto los delitos internacionales como los transnacionales. Aunque muchos Estados consideran también algunas cuestiones como problemas puramente nacionales, la naturaleza de las tecnologías rompe las distinciones tradicionales entre delincuencia nacional y transnacional. Los investigadores, encargados de formular políticas y negociadores encontrarán con frecuencia difícil distinguir entre los delitos nacionales y los transnacionales, lo que aboga por un enfoque integrado, en particular en las etapas preliminares del proceso;

d) Se deberían incluir las opiniones y la asistencia de elementos del sector privado, destacando los siguientes aspectos:

i) El estudio debería examinar y considerar opiniones y aportaciones de las industrias que se ocupan de desarrollar y explotar las tecnologías pertinentes, incluidos el equipo y los programas informáticos y las redes informáticas y de telecomunicaciones;

ii) El estudio debería examinar también las opiniones de las organizaciones no gubernamentales pertinentes. Las organizaciones dedicadas a causas como la libertad de expresión y la protección de la intimidad de la persona han criticado intentos anteriores de establecer facultades de investigación eficaces y han dado origen a una oposición política a los esfuerzos del Grupo de los Ocho y del Consejo Europa en esa esfera;

e) El estudio debería examinar cuestiones situadas al margen de la lucha contra el delito, como el desarrollo sostenible, la protección de la intimidad, la libertad de expresión y otros derechos fundamentales, así como intereses comerciales y de otra índole. Esos intereses fundamentales y otros están estrechamente relacionados con el desarrollo tecnológico, y es probable que resulten afectados tanto por el aumento de la delincuencia relacionada con las redes informáticas como por los esfuerzos de los gobiernos y de la comunidad internacional para impedir y esa delincuencia y luchar contra ella;

f) El estudio debería evaluar también la importancia de esos delitos, tanto en general como en el contexto de factores estadísticamente pertinentes, como las formas concretas de delincuencia, la geografía y otras condiciones sociales o económicas. Ya se han examinado las dificultades para reunir y analizar una información estadística exacta. Sin embargo, a medida que surja una comprensión común del ámbito técnico de la materia y de la tipología de los delitos, debería disponerse de datos más fiables. Además, al aumentar la conciencia popular de los tipos de comportamiento de que se trata y el hecho de que son o deberían ser tratados como delitos, debería disminuir también su denuncia insuficiente. Es igualmente importante la reunión de datos preliminares para lograr el apoyo político a medidas nacionales e internacionales eficaces contra esos delitos;

g) El estudio debería examinar la definición y clasificación de los delitos de alta tecnología y relacionados con las redes informáticas. La clasificación utilizada en el presente informe es coherente con otros trabajos en la materia y puede servir de base para exámenes ulteriores, pero hace falta un examen más completo y riguroso para preparar un marco que cuente con el consenso de los gobiernos, los grupos de intereses y los expertos en esa esfera. Se trata de una primera prioridad, ya que se necesitan definiciones y clasificaciones para dar coherencia a la reunión de estadísticas y la investigación en que deberá basarse la elaboración ulterior de políticas. Una tipología viable requerirá el examen de factores de diversas esferas importantes, entre ellas las siguientes:

i) *Las tecnologías pertinentes*. El campo de la delincuencia de alta tecnología y relacionada con las redes informáticas está determinado en gran parte por la naturaleza y el ámbito de las

tecnologías de que se trata, las cuales evolucionan y convergen rápidamente. Por esa razón, en el presente informe y en otros trabajos sobre el tema se ha utilizado la frase genérica "delitos de alta tecnología y relacionados con las redes informáticas". Hacen falta investigaciones para examinar toda la gama de tecnologías que intervienen y proponer opciones para una clasificación general que las incluya a todas. Se necesita también un examen más detenido de acontecimientos tecnológicos específicos y de los tipos de actividad delictiva que dependen de ellos. Dada la rápida evolución de las tecnologías, deben examinarse no sólo las tecnologías actuales sino también su posible evolución;

ii) *La naturaleza y motivación de los delincuentes*. Los delincuentes que cometen delitos creados por las nuevas tecnologías constituyen una esfera de estudio relativamente nueva. Se conocen bien las motivaciones de delincuentes más tradicionales como los pedófilos, autores de fraudes o traficantes de drogas internacionales. La adaptación de esos delincuentes a las nuevas tecnologías requiere un examen desde la perspectiva de la delincuencia relacionada con las redes informáticas;

iii) *Los aspectos geográficos de los delitos.* Serán distintos de los aspectos de los delitos más tradicionales, al menos en dos puntos importantes. El primero es que hay dos "geografías" principales que se superponen. La ubicación física real de los delincuentes y sus factores de situación específicos, como las condiciones sociales, económicas o culturales, serán importantes. Sin embargo, será importante también la geografía electrónica -las consideraciones tantas veces citadas del espacio cibernético- que influyen en los modelos de delincuencia.

F. Opciones y recomendaciones específicas para trabajos futuros sobre la delincuencia de alta tecnología y relacionada con las redes informáticas

1. Un posible instrumento internacional contra la delincuencia de alta tecnología y relacionada con las redes informáticas

51. Una vez que se haya terminado el estudio, se recomienda que el grupo de expertos asesore a la Comisión sobre las cuestiones y opciones relativas a si resulta viable y conveniente elaborar un instrumento internacional contra la delincuencia de alta tecnología y relacionada con las redes informáticas. Esas cuestiones incluirán las siguientes:

a) La determinación de si el instrumento, en su caso, debería ser normativo o legalmente vinculante. El instrumento podría tratar de establecer requisitos obligatorios para delitos, facultades de investigación y mecanismos de cooperación internacional, o limitarse simplemente a dar directrices para ayudar a los Estados a elaborar medidas eficaces y promover la uniformidad internacional de leyes y procedimientos. Una transacción entre esas dos opciones, que ilustra la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, incluiría un instrumento en el que algunas disposiciones crearan obligaciones vinculantes, mientras que otras contuvieran directrices más generales o dejaran su cumplimiento a la discreción de los Estados partes;

b) La relación que tendría, en su caso, el nuevo instrumento con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. En general, esa Convención podría servir de precedente para algunas disposiciones, mientras que otras quizás no fueran apropiadas para la delincuencia de alta tecnología y relacionada con las redes informáticas. Por ejemplo, la limitación del ámbito de

la Convención a las actividades de “grupos delictivos organizados”, excluiría un porcentaje importante de delitos de alta tecnología y relacionados con las redes informáticas que se cometen por personas o grupos que no quedan comprendidos en la definición dada en la Convención[23]. La posibilidad de elaborar otro protocolo a la Convención para los delitos de este tipo parece, por ello, excluida[24];

c) La forma en que el instrumento, una vez terminado, podría mantenerse al día. Como se señala en la introducción del presente informe, la esfera que se examina se caracteriza por la evolución dinámica de las tecnologías y de las actividades delictivas conexas, y será importante lograr que todo marco para integrar las medidas nacionales e internacionales pueda mantenerse a la altura de los cambios. Entre las opciones puede estar la delegación de algunas facultades legislativas en un grupo de expertos que represente a los Estados partes y se establezca con ese fin, la utilización de protocolos para tratar nuevas cuestiones específicas a medida que surjan, la utilización de una redacción relativamente amplia y tecnológicamente neutral, u otras medidas;

d) La forma de incorporar intereses conexos como el derecho a la intimidad, la libertad de expresión y otros derechos humanos e intereses comerciales en un instrumento internacional. Aunque la materia requiere que el centro del instrumento esté en la prevención de la delincuencia y la lucha contra ella, también deben considerarse esos otros intereses, tanto en el proceso de redacción del instrumento como en su contenido sustantivo.

2. Una estrategia a corto plazo para hacer frente a la delincuencia de alta tecnología y relacionada con las redes informáticas

52. Como se ha señalado *supra*, la delincuencia de alta tecnología y relacionada con las redes informáticas es un problema acuciante que puede requerir una respuesta internacional concertada, tanto a corto como a largo plazo. Se recomienda que el estudio examine posibles medidas que pudieran adoptarse en un futuro inmediato, y que el grupo de expertos formule recomendaciones sobre una estrategia a corto plazo para su examen por la Comisión en su 11º período de sesiones. Los elementos de esa estrategia podrían incluir los siguientes:

a) La recopilación y difusión a todos los Estados Miembros de información sobre la delincuencia de alta tecnología y relacionada con las redes informáticas y las posibles respuestas a ella, a fin de informar, tan rápidamente como sea posible, a los que no hayan participado ya en las deliberaciones. El estudio propuesto sería un elemento esencial de conjuntos de información, pero se dispone también de otros materiales, entre ellos los siguientes:

i) Podría actualizarse y publicarse de nuevo *el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos*, publicado en 1994;

ii) Se podría publicar y difundir la documentación y los materiales 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 Delincuente[25];

iii) Se podría difundir más ampliamente materiales de otras organizaciones intergubernamentales, en particular el Consejo de Europa, la Interpol y el Grupo de Lyon creado por el Grupo de los Ocho;

iv) Se podrían organizar cursos prácticos, seminarios o períodos de sesiones informativos con funcionarios de los Estados interesados y con la posible participación de representantes del sector privado;

b) Se podría aumentar la disponibilidad de materiales relativos a la formación de investigadores y fiscales. Las Naciones Unidas no han producido esa clase de materiales, pero algunos Estados Miembros lo han hecho para la formación de sus propios funcionarios, y en algunos casos para su uso en proyectos de asistencia técnica en que han participado otros Estados;

c) En algunos Estados se necesitará asistencia técnica directa. Esa asistencia puede incluir la formación de jueces, fiscales, investigadores y expertos técnicos o forenses, muchos de los cuales estarían así en condiciones de capacitar a otros. En algunos casos, esos proyectos pueden integrarse en proyectos de desarrollo más generales orientados a ayudar a los Estados a adquirir y utilizar las nuevas tecnologías de desarrollo. Como se ha señalado *supra*, será importante que la prevención del delito y la lucha contra él se conviertan en parte integrante de esos proyectos, si se

quiere evitar los efectos perjudiciales de la delincuencia relacionada con las redes informáticas en el desarrollo;

d) Debería fomentarse el establecimiento de centros o puntos de contacto en cada Estado Miembro. Ello incluiría puntos de contacto para la asistencia inmediata en las investigaciones de delitos relacionados con las redes informáticas[26], pero también contactos más generales reunir información sobre la evolución en cada Estado y para recibir y difundir información procedente de la comunidad internacional;

e) Hará falta un compromiso sustancial de recursos financieros y técnicos. Esa asistencia puede adaptar la forma de contribuciones voluntarias al Fondo de las Naciones Unidas para la Prevención del Delito y la Justicia Penal o la facilitación de expertos o materiales para apoyar un programa mundial contra la delincuencia de alta tecnología y relacionada con las redes informáticas, o proyectos específicos de las Naciones Unidas. La universalidad de las tecnologías y su vulnerabilidad a la explotación por los delincuentes en cualquier parte ofrece incentivos para que los Estados con recursos financieros o técnicos ayuden a otros Estados. Las industrias que desarrollan y explotan redes informáticas y de telecomunicaciones tienen también recursos financieros y técnicos a los que se puede acudir, así como incentivos para contribuir, porque muchas formas de delincuencia relacionadas con las redes informáticas amenazan la viabilidad comercial de sus productos.

3. Establecimiento de un programa mundial contra la delincuencia de alta tecnología y relacionada con las redes informáticas

53. Las pruebas de que se dispone indican que hay un volumen considerable de actividades de investigación y de elaboración de medidas de política, jurídicas y técnicas pero escasa coordinación general de esas actividades. La extensión de las actividades varía según los países. Esas actividades incluyen a cierto número de organizaciones intergubernamentales y no gubernamentales, así como a varios organismos y departamentos de las Naciones Unidas, y son una preocupación principal de empresas comerciales y de grupos de intereses no gubernamentales. La atención, lo mismo que la asignación de recursos, suelen centrarse en cuestiones específicas que preocupan a los gobiernos o las organizaciones directamente afectados, lo que produce posibles lagunas o incoherencias en la investigación. La naturaleza mundial de las Naciones Unidas las sitúan en una posición única para examinar y coordinar las actividades en esta esfera. Se recomienda que, una vez examinadas las necesidades y opiniones de los Estados Miembros, se establezca un programa mundial contra la delincuencia de alta tecnología y relacionada con las redes informáticas. Se recomienda también que los Estados interesados hagan contribuciones voluntarias para la creación y funcionamiento de ese programa mundial.

54. La Comisión debería examinar en su 11º período de sesiones el posible mandato de ese programa mundial, una vez obtenidos los resultados del estudio y conocidas las opiniones del grupo de expertos. El mandato del programa mundial podría incluir las actividades expuestas en el párrafo 52 *supra*, así como las siguientes:

a) La identificación de los Estados Miembros que soliciten asistencia y el análisis de sus necesidades específicas;

b) La elaboración de materiales para ayudar a los encargados de formular políticas, legisladores, organismos de aplicación de la ley, fiscales y otros funcionarios competentes a tratar los casos nacionales y transnacionales;

c) La reunión, recopilación y difusión de materiales preparados por otros;

d) La prestación de asistencia jurídica, técnica y de otra índole a los Estados que la soliciten, con sujeción a la disponibilidad de recursos suficientes;

e) La elaboración de un inventario de conocimientos técnicos disponibles de personas individuales y organismos dispuestos a prestar asistencia a los Estados solicitantes;

f) La coordinación de las actividades con otros organismos y departamentos de las Naciones Unidas, en particular en las esferas de los derechos humanos y el desarrollo, con miras a incluir el tema de la delincuencia relacionada con las redes informáticas en otros programas, cuando proceda, y a garantizar la incorporación de las aportaciones de otros programas en la elaboración de estrategias para la prevención y control del delito;

g) La coordinación de actividades con otras organizaciones internacionales y distintos gobiernos y organismos que trabajen en la esfera de la delincuencia de alta tecnología y relacionadas con las redes informáticas;

h) La coordinación de las actividades con los grupos de intereses no gubernamentales y las empresas del sector privado, y la organización de recursos monetarios y de expertos técnicos procedentes de empresas, como parte de una estrategia mundial contra la delincuencia de alta tecnología y relacionada con las redes informáticas.

4. Inventario preliminar de cuestiones sustantivas para examen

55. Como elementos de las estrategias tanto a corto como a largo plazo, habrá que abordar muchas de las mismas cuestiones sustantivas. Sobre la base de las deliberaciones previas en las Naciones Unidas y en otros foros mencionadas en el presente informe, requieren examen las siguientes cuestiones sustantivas:

a) La determinación de los comportamientos perjudiciales que impliquen a las nuevas tecnologías, y la tipificación de nuevos delitos o la modificación de la existente para penalizarlos;

b) La elaboración de principios para tratar el rastreo transnacional de las comunicaciones, incluidas las facultades para obtener, preservar y revelar datos del tráfico[27];

c) La elaboración de principios que regulen las investigaciones electrónicas transfronterizas voluntarias o involuntarias;

d) La elaboración de principios comunes para tratar de la intercepción de comunicaciones transmitidas por redes informáticas o medios similares;

e) La evaluación de los intereses de la confidencialidad o intimidad inherentes a diversas formas de almacenamiento y transmisión de datos, a fin de establecer controles procesales de la incautación e intercepción en línea de esos intereses. La mayoría de los Estados establecen restricciones escasas, si es que las establecen, sobre el acceso con fines de aplicación de la ley a sitios web abiertos o a comunicaciones por la web, por ejemplo, pero aplicarían restricciones a la incautación de datos procedentes de fuentes más privadas;

f) La elaboración de normas o prácticas comunes para identificar a los distintos usuarios de los servicios de redes informáticas o de telecomunicaciones, equilibrada con la necesidad de intimidad y anonimidad de la persona;

g) La elaboración de principios comunes para ajustar las prácticas forenses y las disposiciones legales sobre la prueba a fin de garantizar que las pruebas informáticas puedan preservarse, autenticarse y utilizarse en los procedimientos penales;

h) La elaboración de principios comunes para la protección de derechos fundamentales, tanto al establecer políticas y medidas internacionales contra la delincuencia de alta tecnología y relacionada con las redes informáticas como al aplicar esas medidas en casos específicos;

i) La elaboración de principios comunes que regulen la confidencialidad y la integridad de los datos y el equilibrio o la armonización de esos principios con la necesidad de medidas eficaces de lucha contra la delincuencia;

j) La elaboración y financiación de programas y materiales de asistencia técnica para los Estados que soliciten esa asistencia. Esos programas y materiales se necesitarán tanto para ayudar a los Estados a participar eficazmente en la elaboración de políticas mundiales como para garantizar que las autoridades nacionales están debidamente capacitadas y equipadas para poder responder con eficacia y rapidez a las solicitudes de asistencia en la investigación de delitos transnacionales relacionados con las redes informáticas;

k) La reunión, análisis y comunicación de informaciones sobre nuevos acontecimientos tecnológicos, los delincuentes y sus técnicas, y sobre métodos eficaces de prevenir, investigar y enjuiciar los delitos;

l) La capacitación, equipamiento y prestación de recursos a los expertos en aplicación de la ley a fin de garantizar la capacidad de investigar y enjuiciar eficazmente en los casos nacionales, y de cooperar eficazmente con otros Estados en los casos transnacionales;

m) La necesidad de evaluar y aclarar la función del sector privado y sus relaciones con los gobiernos,

tanto en el nivel nacional como en el internacional. Entre los elementos o aspectos concretos de esas relaciones que deberán examinarse se encuentran los siguientes:

i) La necesidad de encontrar un equilibrio entre las medidas eficaces de lucha contra la delincuencia y las limitaciones técnicas y comerciales para la elaboración y aplicación de esas medidas. La lucha contra el delito debería tenerse en cuenta por las industrias en la etapa de diseño de nuevas tecnologías, pero las autoridades de aplicación de la ley deben reconocer que algunas medidas pueden no ser técnicamente viables o suponer cambios que harían las tecnologías improductivas o no competitivas. Las exigencias de la lucha contra la delincuencia no deben afectar a la viabilidad o la competitividad básicas de las nuevas tecnologías, pero los costos del delito y de su prevención deben convertirse en parte de las evaluaciones generales de costos-beneficios, tanto de los gobiernos como de las industrias, y esos costos deben sufragarse, cuando proceda, con los beneficios obtenidos por las tecnologías en que se basan los delitos;

ii) La necesidad de que los gobiernos e industrias cooperen eficazmente a fin de aumentar al máximo los beneficios y reducir al mínimo los costos de que se trate. Ello incluye señalar y elaborar técnicas eficaces de seguridad y otras técnicas de prevención del delito, su incorporación a las nuevas tecnologías en la etapa de desarrollo más temprana posible, y la capacitación y preparación de los organismos de aplicación de la ley y de enjuiciamiento con respecto a las nuevas tecnologías, antes de que los posibles delincuentes tengan acceso a ellas. El progreso tecnológico de las industrias pertinentes las hace importantes, si es que no esenciales, para el éxito de los programas de asistencia técnica, y los propios intereses comerciales de las industrias justificarán en muchos casos la participación de éstas en esos programas;

iii) La necesidad de establecer sistemas y realizar operaciones de forma que apoyen una investigación penal eficaz y la prevención del delito, teniendo en cuenta también la necesidad de proteger la intimidad y otros derechos de los usuarios de las tecnologías. Ejemplos son el funcionamiento de sistemas capaces de conservar pruebas de las comunicaciones durante períodos razonables, por si fueran necesarias para una investigación, y la necesidad de poder identificar a los clientes;

iv) La necesidad de hacer una evaluación mundial del papel potencial del sector privado en la lucha contra el delito. Se trata de una cuestión compleja con la que se enfrentan ya muchos proveedores de servicios, los cuales comparten el interés público por la lucha eficaz contra la delincuencia, pero reconocen los peligros y las dificultades que surgen si esos proveedores sustituyen o reemplazan a los organismos públicos de aplicación de la ley. Las industrias se encuentran con presiones conflictivas para que incorporen medidas de seguridad en las nuevas tecnologías que pueden no ser comercialmente viables o que afectan a los intereses fundamentales de sus clientes[28]. También se enfrentan con presiones oficiales para que controlen o excluyan contenidos que se consideran ilegales o inadecuados, o para que ayuden a los organismos públicos de aplicación de la ley en la realización de investigaciones penales. Esas presiones suscitan complejas cuestiones éticas, jurídicas y de políticas que deben estudiarse, tanto en el plano nacional como en el mundial, a fin de lograr la mayor coherencia mundial posible.

Notas

[1] Véase “La era de los puentes digitales” en el informe del Secretario General a la Asamblea de las Naciones Unidas dedicada al Milenio (A/54/2000, párrs. 150 a 167). Véase también el informe del Secretario General sobre desarrollo y cooperación internacional en el siglo XXI: el papel de la tecnología y la información en el contexto de una economía mundial basada en los conocimientos (E/2000/52, secs. III a V).

[2] Comité Europeo para los Problemas de Delincuencia, Comité de Expertos sobre la Delincuencia en el Espacio Cibernético, “Proyecto de Convención sobre la delincuencia cibernética” (PC-CY (2000), proyecto Nº 25, rev. 5), disponible en línea en http://conventions.coe.int/treaty/en/projets/cybercrime25.htm.

[3] Las conclusiones de los estudios figuran en las recomendaciones R (89) 9 y R (95) 13. Del Consejo de Europa. El Comité de Expertos fue establecido por el Comité de Ministros del Consejo de Europa en la 583ª reunión de Delegados de Ministros, celebrada el 4 de febrero de 1997.

[4] Véase el anexo del comunicado de la Reunión de Ministros de Justicia y del Interior del Grupo de los Ocho, celebrada en Washington, D.C., el 10 de diciembre de 1997.

[5] Véase el comunicado de la Conferencia Ministerial del Grupo de los Ocho sobre la lucha contra la delincuencia organizada transnacional, celebrada en Moscú del 19 al 20 de octubre de 1999, párr. 17 y anexo 1.

[6] Se celebraron reuniones en París, del 15 al 17 de mayo de 2000, y en Berlín, del 24 al 26 de octubre de 2000. Se prevé realizar otra reunión en Tokio, en mayo de 2001.

[7] En el párrafo 14 de su resolución 1999/23, el Consejo pide al Secretario General que efectúe 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, el cual incluiría un examen de la conveniencia de preparar manuales, directrices y recomendaciones, y que informe sobre las conclusiones de dicho estudio a la Comisión de Prevención del delito y Justicia Penal, en su décimo período de sesiones.

[8] Véase las resoluciones 45/109 y 45/121 de la Asamblea General, y *Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y tratamiento del Delincuente, La Habana, 27 de agosto a 7 de septiembre de 1990: informe preparado por la Secretaría* (publicación de las Naciones Unidas, Nº de venta S.91.IV.2), cap. I, sec. C, pág. 149.

[9] Véase A/CONF.169/16/Rev.1, párrs. 370 a 385.

[10] Véase la resolución 55/25 de la Asamblea General, de 15 de noviembre de 2000, anexo I, artículo 18, párrs. 8 y 18.

[11] Véase *Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente...*, cap. I, sec. C.

[12] *Revista Internacional de Política Criminal*, Nos. 43 y 44 (publicación de las Naciones Unidas, Nº de venta S.94.IV.5).

[13] Véanse las resoluciones de la Asamblea General 52/91, de 12 de diciembre de 1997, y 53/110, de 9 de diciembre de 1998. Véase también A/CONF.187/10 *y Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Viena, 10 a 17 de abril de 2000: informe preparado por la Secretaría* (publicación de las Naciones Unidas, Nº de venta E.00.IV.8), párrs. 161 a 174.

[14] Véase A/CONF.187/L.10, párr. 14.

[15] Véase *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente...*, cap. I.

[16] Véase los artículos 2 (Definiciones) y 3 (Ámbito de aplicación) de la Convención (resolución 55/25, anexo I).

[17] Esos delitos fueron examinados recientemente por el Grupo de Acción Financiera sobre el Blanqueo de Capitales (GAFI) de la Organización de Cooperación y Desarrollo Económicos (OCDE). Véase GAFI: *"Report on money laundering typologies for 2000-2001"* (París, OCDE, febrero de 2001), párrs. 5 a 18.

[18] A/54/2000, párr. 152.

[19] Por ejemplo, el Director de la Oficina Federal de Investigación (FBI), de los Estados Unidos, en una declaración sobre la delincuencia cibernética hecha ante el Comité Judicial del Senado de los Estados Unidos, el 28 de marzo de 2000, informó de que, de 1998 a 1999, el número de casos de que se había ocupado el FBI se había duplicado, de 547 a 1.154, aunque no resulta claro si ello se debió al aumento de la delincuencia, al de las denuncias, o a ambos. Véase también P. Graboski, *"Computer crime: a criminological overview"*, *Forum on Crime and Society*, vol. 1 (2001), pág. 40.

[20] Un programador de los Estados Unidos de 31 años admitió que había creado el virus "Melissa". Un joven canadiense de 15 años se confesó culpable de 56 infracciones penales en relación con ataques de denegación de servicios. En el caso del virus "*I love you*" no hubo acusación, pero se cree que el virus tuvo su origen en Filipinas. En relación con cada uno de esos incidentes se difundió una gran diversidad de estimaciones de daños, y probablemente nunca se determinarán los verdaderos costos. Se citan las cifras como indicio de la escala general de las pérdidas y del grado de preocupación política por la amenaza que suponen los delitos cometidos a esa escala.

[21] Véase E/2000/52, secs. III a V.

[22] Véase E/2000/52, párrs. 79 a 99.

[23] Véase los artículos 2 y 3 de la Convención (resolución 55/25, anexo I).

[24] Los tres protocolos existentes incorporan disposiciones relativas al ámbito y la aplicación de la Convención, haciendo las transposiciones necesarias. Muchas de las disposiciones de la Convención, al haberse redactado sobre la base de que se aplicarían sólo a los casos en que intervinieran grupos delictivos organizados, serían difíciles de aplicar a los delitos relacionados con las redes informáticas cometidos por personas individuales.

[25] El Instituto de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente, de las Naciones Unidas, que organizó el curso práctico, prepara actualmente esos materiales para su publicación.

[26] El proceso se ha iniciado ya por el Grupo de los Ocho y se ha continuado por la Interpol.

[27] La expresión “datos del tráfico” designa en general los datos almacenados por los proveedores de servicios, que indican la fuente y el destino de una comunicación electrónica. Pueden incluir tanto la fuente y el destino últimos como las fuentes o destinos provisionales dentro de una red informática. Un concepto conexo es el de datos de “suscriptor” o “usuario”, que se utiliza por los proveedores de servicios para identificar a los distintos clientes.

[28] Un ejemplo reciente fue un interdicto dictado por un tribunal francés que exigió a la empresa Yahoo! Inc. de la Internet que introdujera métodos técnicos para impedir el acceso a sus suscriptores de Francia a sitios web de subasta de objetos de recuerdo nazis. La venta de esos objetos está prohibida en Francia, pero es legal en las jurisdicciones en donde los sitios se encuentran. Los proveedores están dispuestos en general a adoptar medidas de esa índole -siempre que sean técnicamente viables- pero únicamente cuando un tribunal u otra autoridad pública competentes determinan que el contenido es ilegal.