



Consejo Económico y Social

Distr. general
2 de marzo de 2011
Español
Original: inglés

Comisión de Prevención del Delito y Justicia Penal

20º período de sesiones

Viena, 11 a 15 de abril de 2011

Tema 6 del programa provisional*

**Tendencias de la delincuencia a nivel mundial y nuevas
cuestiones y respuestas relativas a la prevención del
delito y la justicia penal**

Informe del Grupo intergubernamental de expertos de composición abierta encargado de realizar un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno

Nota de la Secretaría

1. De conformidad con lo dispuesto en el párrafo 9 de la resolución 65/230 de la Asamblea General, el Grupo intergubernamental de expertos de composición abierta establecido por la Comisión con arreglo al párrafo 42 de la Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución (resolución 65/230 de la Asamblea General, anexo) celebró su reunión en Viena del 17 al 21 de enero de 2011. De acuerdo con su mandato, el Grupo de expertos deliberó sobre la cuestión de la realización de

un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas.

* E/CN.15/2011/1.



2. En el párrafo 11 de la resolución 65/230, la Asamblea General solicitó al Grupo intergubernamental de expertos de composición abierta que informara a la Comisión sobre los avances de su labor. En consecuencia, el Grupo de expertos examinó y aprobó los documentos finales adjuntos, titulados “Conjunto de temas para su examen en un estudio exhaustivo de las consecuencias del delito cibernético y la respuesta ante ese fenómeno” (anexo I) y “Metodología del estudio” (anexo II), que se transmitieron a la Comisión en su 20º período de sesiones para su examen.

3. Tras la aprobación del conjunto de temas para su examen en un estudio exhaustivo de las consecuencias del delito cibernético y la respuesta ante ese fenómeno (anexo I), el representante de Colombia formuló la siguiente declaración y solicitó que se la incluyera en el informe del Grupo intergubernamental de expertos de composición abierta:

1. Durante la reunión del Grupo intergubernamental de expertos de composición abierta, muchas delegaciones expresaron su preocupación acerca del frecuente uso indebido de las nuevas tecnologías de la información y las comunicaciones con fines terroristas. En este contexto, un representante de la Secretaría realizó una exposición sobre la labor de la Oficina de las Naciones Unidas contra la Droga y el Delito en relación con ese problema y, en particular, el uso indebido de Internet. Teniendo en cuenta que el estudio del delito cibernético debe ser completo y exhaustivo, sería necesario abordar todas las preocupaciones expresadas. Por lo tanto, es esencial que se incluyan en el estudio todos los aspectos de las relaciones entre el terrorismo y el delito cibernético. Las organizaciones terroristas usan estas tecnologías de diferentes maneras, y en especial:

- a) Con fines propagandísticos;
- b) Para reunir información;
- c) Como instrumento de capacitación;
- d) Para organizar actividades ilícitas;
- e) Para difundir información con fines de reclutamiento e incitación;
- f) Con fines de almacenamiento y transmisión seguros de información;
- g) Para atacar las propias de redes de computadoras.

2. En interés del consenso, Colombia acepta las propuestas de la delegación de la Argentina relacionadas con esta cuestión, pero solicita que en el informe sobre la primera reunión del Grupo intergubernamental de expertos de composición abierta se tome nota de lo siguiente:

a) Con respecto al párrafo 12 del conjunto de temas para su examen en un estudio exhaustivo de las consecuencias del delito cibernético y la respuesta ante ese fenómeno (véase el anexo I), Colombia entiende que la referencia a un inventario de conductas que han sido tipificadas como delito incluye el tema del terrorismo;

b) Con respecto al título que precede al párrafo 18 de ese documento, Colombia entiende que los desafíos del delito cibernético incluyen también el tema del terrorismo;

c) Colombia expresa asimismo la esperanza de que el estudio incluya el examen del posible uso indebido por los terroristas de instrumentos que pueden utilizarse para cometer delitos cibernéticos, como los mencionados en el párrafo 25 de ese documento.

Anexo I

Conjunto de temas para su examen en un estudio exhaustivo de las consecuencias del delito cibernético y la respuesta ante ese fenómeno

I. Introducción

1. Durante el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en 2010, los Estados Miembros examinaron con cierto detalle la cuestión del delito cibernético y decidieron invitar a la Comisión de Prevención del Delito y Justicia Penal a que convocara a un grupo intergubernamental de expertos de composición abierta para que realizara un estudio exhaustivo del problema del delito cibernético y la respuesta ante ese fenómeno. Esa recomendación fue aprobada por la Comisión de Prevención del Delito y Justicia Penal, y posteriormente por el Consejo Económico y Social, en su resolución 2010/18, y por la Asamblea General, en su resolución 65/230.

2. De conformidad con el párrafo 42 de la Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución, en el estudio exhaustivo ha de examinarse:

[El] problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas.

3. Así pues, en el párrafo 42 de la Declaración de Salvador se indican los distintos aspectos sustantivos que el estudio debería investigar (el problema del delito cibernético, la legislación nacional, las mejores prácticas, la asistencia técnica y la cooperación internacional), así como la perspectiva (las respuestas de los Estados Miembros, la comunidad internacional y el sector privado), y el enfoque (examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas).

4. Con miras a esbozar una estructura del estudio, estas tres dimensiones (aspectos sustantivos, perspectiva y enfoque) se han plasmado en 12 temas que siguen el mandato de la Declaración. A continuación se agrupan esos 12 temas en distintas categorías.

El problema del delito cibernético (temas 1 a 3)

5. La Declaración de Salvador destaca que el estudio debería investigar el problema del delito cibernético. Para abordar en toda su extensión los problemas que plantea el delito cibernético, se establecen tres ámbitos fundamentales que han de analizarse exhaustivamente, a saber:

- a) Fenómeno del delito cibernético (tema 1);
- b) Información estadística (tema 2);
- c) Desafíos del delito cibernético (tema 3).

Respuestas jurídicas al delito cibernético (temas 4 a 9)

6. En la Declaración de Salvador se formula un llamamiento a realizar un estudio de las respuestas jurídicas al delito cibernético, incluido el intercambio de información sobre legislación nacional, mejores prácticas y cooperación internacional. Además de los aspectos generales de armonización de la legislación, se establecen esferas concretas de respuestas jurídicas, a saber:

- a) Enfoques comunes de la legislación (tema 4);
- b) Tipificación de los delitos cibernéticos (tema 5);
- c) Facultades en materia de procedimiento (tema 6);
- d) Cooperación internacional (tema 7);
- e) Salvaguardias y condiciones, incluida la protección de los derechos humanos fundamentales y los datos personales;
- f) Respeto del principio de igualdad soberana de los Estados y no injerencia en los asuntos de otros Estados;
- g) Pruebas electrónicas (tema 8);
- h) Funciones y responsabilidades de los proveedores de servicios y el sector privado (tema 9).

Capacidades en materia de prevención del delito y justicia penal y otras respuestas ante delito cibernético (tema 10)

7. La Declaración de Salvador se refiere no solo al estudio de las respuestas jurídicas al delito cibernético sino también, en general, a respuestas de otra índole a dicho delito.

Organizaciones internacionales (tema 11)

8. En la Declaración de Salvador se invita a realizar un análisis de las respuestas de los Estados Miembros, la comunidad internacional y el sector privado. Aunque las cuestiones relativas a las respuestas jurídicas de la comunidad internacional se incluyen en el epígrafe de las respuestas jurídicas, otro epígrafe dedicado a las respuestas de la comunidad internacional facilitará el análisis de los aspectos más generales, como la relación entre los enfoques regional e internacional.

Asistencia técnica (tema 12)

9. Habida cuenta de las consecuencias del delito cibernético en los países en desarrollo y la necesidad de adoptar un enfoque uniforme y coordinado para combatirlo, la asistencia técnica se considera una esfera concreta que ha de ser objeto del estudio exhaustivo.

II. Descripción detallada de los temas

Tema 1. El fenómeno del delito cibernético

Antecedentes

10. El delito informático y, más concretamente, el delito cibernético, son términos utilizados para describir una categoría concreta de conducta delictiva. Los problemas relacionados con esta categoría de conducta delictiva incluyen tanto la amplia variedad de delitos de que se trata como el desarrollo dinámico de nuevos métodos de cometer esos delitos.

La evolución del delito informático y el delito cibernético

11. En la década de 1960, cuando aparecieron los equipos informáticos de transistores y se extendió el uso de las computadoras¹, la tipificación de delitos se centró en los daños físicos a los sistemas informáticos y los datos almacenados². El decenio de 1970 se caracterizó por un giro de los tradicionales delitos contra la propiedad cometidos contra equipos informáticos³, y que asumieron nuevas formas de delincuencia⁴, como el uso ilícito de equipos informáticos⁵ y la manipulación⁶ de datos electrónicos⁷. El giro en la modalidad de las transacciones, de las operaciones manuales a las informatizadas, llevó a una nueva forma de delito, el fraude informático⁸. En el decenio de 1980 se extendió cada vez más el uso de las computadoras personales y por primera vez una gran variedad de infraestructura crítica pasó a depender de la tecnología informática⁹. Uno de los efectos colaterales de la distribución de sistemas informáticos fue el interés creciente en los programas informáticos y la aparición de las primeras formas de piratería informática y delitos relacionados con las patentes¹⁰. Además, el comienzo de la interconexión de

-
- ¹ En relación con los desafíos conexos, véase R. T. Slivka y J. W. Darrow; *Methods and Problems in Computer Security*, *Rutgers Journal of Computers and the Law*, vol. 5, núm. 2 (1976), págs. 217 a 269.
- ² McLaughlin, "Computer crime: the Ribicoff Amendment to United States Code, Title 18", *Criminal Justice Journal*, vol. 2, 1978, págs. 217 y ss.
- ³ Gemignani, "Computer Crime: The Law in '80", *Indiana Law Review*, vol. 13, 1980, pág. 681.
- ⁴ McLaughlin, "Computer crime: the Ribicoff Amendment".
- ⁵ Freed, *Materials and Cases on Computer and Law*, (n.p., 1971), pág. 65.
- ⁶ Bequai, "The electronic criminals: how and why computer crime pays", *Barrister*, vol. 4, 1977, págs. 8 y ss.
- ⁷ *Criminological Aspects of Economic Crime: Proceedings of the 12th European Conference of Directors of Criminological Research Institutes (November 1976)*, vol. XV, *Collected Studies in Criminological Research (Estrasburgo, Consejo de Europa, 1977)*, págs. 225 y ss.; *Estados Unidos de América, Staff Study of Computer Security in Federal Programs: Committee on Government Operations — United States Senate (Washington, D.C., United States Government Printing Office, 1977)*.
- ⁸ McLaughlin, "Computer crime: the Ribicoff Amendment" (véase la nota 2 *supra*); Bequai, "Computer crime: a growing and serious problem", *Police Law Quarterly*, vol. 6, 1977, pág. 22.
- ⁹ E. A. Glynn, "Computer abuse: the emerging crime and the need for legislation", *Fordham Urban Law Journal*, vol. 12, núm. 1 (1983-1984), pág. 73.
- ¹⁰ Bloombecker, "The Trial of computer crime", *Jurimetrics Journal*, vol. 21, 1981, pág. 428; W. Schmidt, "Legal proprietary interests in computer programs: the American experience", *Jurimetrics Journal*, vol. 21, 1981, 345 y ss.; M. Dunning, "Some aspects of theft of computer software", *Auckland University Law Review*, vol. 4, núm. 3 (1982), págs. 273 y ss.; Weiss,

equipos informáticos permitió a los infractores entrar en un equipo de computación sin estar presente en el lugar del delito¹¹. La introducción de la interfaz gráfica (www, o World Wide Web) en el decenio de 1990, seguida de un rápido aumento del número de usuarios de Internet, dio lugar a nuevos métodos de conducta delictiva. Por ejemplo, la distribución de materiales relativos al abuso de niños pasó del intercambio de libros y películas a la distribución en línea por medio de sitios web y servicios de Internet¹². Aunque los delitos informáticos solían ser delitos locales, Internet convirtió el delito electrónico en delito transnacional. El primer decenio del siglo XXI se caracterizó por métodos nuevos y sumamente complejos de cometer delitos, como la suplantación de identidad o robo de datos personales¹³ y los ataques con redes zombi o “botnets”¹⁴, y el uso de nuevas tecnologías que plantean dificultades a los cuerpos y fuerzas de seguridad, como el protocolo de voz a través de Internet (VoIP)¹⁵ y la “informática en las nubes”¹⁶.

“Pirates and prizes: the difficulties of protecting computer software”, *Western State University Law Review*, vol. 11, 1983, pp. 1 y ss.; R. P. Bigelow, “The challenge of computer law”, *Western England Law Review*, vol. 7, núm. 3 (1985), pág. 401; G. Thackeray, “Computer-related crimes: an outline”, *Jurimetrics Journal*, vol. 25, núm. 3 (1985), págs. 300 y ss.

- ¹¹ Yee, “Juvenile computer crime: hacking — criminal and civil liability”, *Comm/Ent Law Journal*, vol. 7, 1984, págs. 336 y ss.; “Who is calling your computer next? Hacker!”, *Criminal Justice Journal*, vol. 8, 1985, págs. 89 y ss.; A. M. Wagner, “The challenge of computer-crime legislation: how should New York respond?”, *Buffalo Law Review*, vol. 33, núm. 3 (1984), págs. 777 y ss.
- ¹² “Child pornography”, documento temático preparado para el Segundo Congreso Mundial contra la Explotación Sexual Comercial de los Niños, Yokohama (Japón), 12 a 20 de diciembre de 2001, pág. 17; “Sexual exploitation of children over the Internet”, informe preparado para su utilización por la Comisión de Energía y Comercio, Cámara de Representantes de los Estados Unidos, 109º Congreso, enero de 2007, pág. 9.
- ¹³ Por suplantación de identidad o robo de datos personales (“peska”) se entiende un acto que tiene por objeto lograr que la víctima revele información personal o confidencial. Se empleó inicialmente para describir la utilización de los correos electrónicos para “peskar” contraseñas y datos financieros en un mar de usuarios de Internet. El empleo de la grafía “k” se relaciona con las convenciones terminológicas de uso común en la piratería informática. Para más información véase: Unión Internacional de Telecomunicaciones (UIT), *El ciberdelito: Guía para los países en desarrollo*, (Ginebra, 2009), capítulo 2.8.4.
- ¹⁴ Una red zombi o “botnet” es un grupo de computadoras manipuladas subrepticamente en que se ejecuta un programa informático bajo control externo. Para más información, véase Clay Wilson, “Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress”, Congressional Research Service Report RL32114, 2007, pág. 4.
- ¹⁵ M. Simon y J. Slay, “Voice over IP: forensic computing implications”, documento preparado para la Cuarta Conferencia Australiana sobre técnicas forenses digitales, Perth, 4 de diciembre de 2006.
- ¹⁶ Cristos Velasco San Martín, “Jurisdictional aspects of cloud computing”, documento presentado en la Conferencia Octopus Interfaz del Consejo de Europa: Cooperación contra el delito cibernético, Estrasburgo, 10 y 11 de marzo de 2009; M. Gercke, “Die Auswirkungen von Cloud Storage auf die Tätigkeit der Strafverfolgungsbehörden”, en *Inside the Cloud: Neue Herausforderungen für das Informationsrecht*, J. Taeger y A. Wiebe, eds., Oldenburger Tagungsbände (Edewecht, Alemania, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2009), pág. 499 y ss.

Alcance del estudio

12. El alcance del estudio en relación con este tema se centrará en el fenómeno del delito cibernético propiamente dicho y no incluirá las respuestas al delito cibernético.

- a) Análisis del fenómeno del delito cibernético teniendo en cuenta los actos que están previstos en los marcos jurídicos existentes;
- b) Inventario de actos tipificados como delitos;
- c) Inventario de conductas que aún no han sido tipificadas como delito;
- d) Sinopsis de delitos combinados (como el robo de identidad o “peska”) y tendencias futuras;
- e) Inventario de casos pertinentes;
- f) Examen de la importancia de la definición del delito cibernético.

Tema 2. Información estadística

Antecedentes

13. Las estadísticas sobre el delito constituyen la base del examen y los procesos de adopción de decisiones por los encargados de la formulación de políticas y los especialistas¹⁷. Además, el acceso a información precisa sobre el verdadero alcance del delito cibernético puede permitir a los organismos de represión mejorar las estrategias de lucha contra ese delito, evitar posibles ataques y garantizar la promulgación de legislación más apropiada y eficaz.

Situación actual de las estadísticas sobre el delito cibernético

14. Por lo general, la información sobre el alcance del delito se extrae de estadísticas y estudios sobre la delincuencia¹⁸. Ambas fuentes plantean problemas cuando se utilizan para elaborar recomendaciones en materia de políticas. En primer lugar, las estadísticas sobre delincuencia suelen generarse a nivel nacional y no reflejan el alcance internacional de la cuestión. Aunque teóricamente sería posible combinar los datos de los diferentes Estados, este enfoque no produciría información fiable debido a las diferencias de legislación y prácticas de registro¹⁹. Combinar y comparar las estadísticas nacionales de delincuencia exige cierto grado de compatibilidad²⁰ del que se carece cuando se trata del delito cibernético. Aunque los delitos cibernéticos se registren, no necesariamente se enumeran por separado²¹.

¹⁷ P. A. Collier and B. J. Spaul, “Problems in policing computer crime”, *Policing and Society*, vol. 2, núm. 4 (1992), pág. 308.

¹⁸ En lo que respecta a la importancia creciente de las estadísticas sobre delincuencia, véase: *Introduction to Crime Analysis: Basic Resources for Criminal Justice Practice* (Binghamton, Nueva York, Haworth Press, 2003), págs. 1 y ss.

¹⁹ En este contexto véase: *Overcoming Barriers to Trust in Crimes Statistics: England and Wales*, Monitoring Report No. 5, interim report (Londres, United Kingdom Statistics Authority, diciembre de 2009), pág. 9, puede consultarse en www.statisticsauthority.gov.uk.

²⁰ Alvazzi del Frate, “Crime and criminal justice statistics challenges”, en *International Statistics on Crime and Justice*, S. Harrendorf, M. Heiskanen y Malby, editores Serie de publicaciones

15. En segundo lugar, las estadísticas solo pueden incluir los delitos que se han detectado y denunciado²². Especialmente en lo que se refiere al delito cibernético, preocupa el hecho de que el número de casos no denunciados parece ser significativo²³. Las empresas tal vez temen que la publicidad negativa lesione su reputación²⁴. Si una empresa anuncia que su servidor ha sido objeto de actos de intrusismo informático, los clientes pueden perder la confianza, y los costos podrían ser aún mayores que las pérdidas causadas por la intrusión. Sin embargo, si los delitos no se denuncian y no se enjuicia a quienes los cometen, estos probablemente reincidan. Además, las víctimas tal vez no confían en que los organismos de represión sean capaces de identificar a los delincuentes²⁵ y crean que no tiene sentido denunciar los delitos²⁶. Dado que la automatización permite que los delincuentes cibernéticos adopten una estrategia consistente en obtener grandes beneficios realizando un gran número de ataques con el fin de obtener una reducida cantidad de dinero de cada víctima, como sucede con el fraude que entraña el cobro

HEUNI núm. 64, (Helsinki, Instituto Europeo de Prevención del Delito y Lucha contra la Delincuencia afiliado a las Naciones Unidas, 2010), pág. 168. Puede consultarse en: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

- ²¹ “Computer Crime”, Parliamentary Office of Science and Technology, *Postnote* núm. 271, octubre de 2006, pág. 3.
- ²² En relación con los problemas conexos, véase Kabay, “Understanding Studies and Surveys of Computer Crime”, 2009, que puede consultarse en: www.mekabay.com/methodology/crime_stats_methods.pdf.
- ²³ La Oficina Federal de Investigación (FBI) de los Estados Unidos ha pedido a las empresas que denuncien los ataques de “phishing” o los ataques contra los sistemas de tecnología de la información de las empresas, y que informen a las autoridades al respecto de manera que estas estén al tanto de las actividades delictivas en Internet. “Para nosotros es un problema que algunas empresas estén claramente más preocupadas por la mala publicidad que por las consecuencias de un ataque de piratería informática que ha tenido éxito”, explicó Mark Mershon, jefe interino de la oficina de la FBI en Nueva York.” Véase “FBI wants to know more about hacker attacks”, *Heise News*, 27 de octubre de 2006, que puede consultarse en: www.h-online.com/security/news/item/FBI-wants-to-know-more-about-hacker-attacks-731717.html. Véase también “Comments on Computer Crime – Senate Bill S. 240”, *Memphis State University Law Review*, 1980, pág. 660.
- ²⁴ Véanse N. Mitchison y R. Urry, “Crime and Abuse in e-Business”, en *IPTS Report*, núm. 57, 2001, págs. 18 a 22; Collier y Spaul, “Problems in Policing Computer Crime”, (véase la nota 17 *supra*), 310,
- ²⁵ Véanse Collier y Spaul, “Problems in Policing Computer Crime”, (véase la nota 17 *supra*), R. G. Smith, “Investigating Cybercrime: Barriers and Solutions”, documento preparado para la Asociación de examinadores certificados del fraude, Conferencia de la Cuencia del Pacífico sobre el Fraude, Sidney, 11 de septiembre de 2003, pág. 2, que puede consultarse en: www.aic.gov.au/about_aic/research_programs/staff/smith_russell.aspx.
- ²⁶ Lo cierto es que los diarios, así como las estaciones de televisión, limitan su cobertura de las investigaciones en Internet que han tenido éxito a casos espectaculares como el descubrimiento de un pedófilo al deshacer las modificaciones realizadas en una fotografía y reconstruir el rostro del sospechoso. Para más información sobre el caso y la cobertura, véase: “Interpol in appeal to find paedophile suspect”, *The New York Times*, 9 de octubre de 2007, puede consultarse en: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin, así como la información suministrada en el sitio web de la Organización Internacional de Policía Criminal (INTERPOL), que puede consultarse en: www.interpol.int/Public/THB/vico/Default.asp.

de comisiones por adelantado²⁷, las posibles consecuencias de delitos no denunciados podrían ser importantes. Tratándose de pequeñas cantidades, las víctimas de dichos ataques probablemente opten por no recurrir a procedimientos de denuncia que llevan mucho tiempo. En la práctica, suelen denunciarse únicamente los casos que entrañan comisiones muy elevadas²⁸.

Alcance del estudio

16. El estudio del tema consistirá en:

- a) Reunir las estadísticas, los estudios y los análisis más recientes sobre la prevalencia y el alcance del delito cibernético;
- b) Estimar el valor de las estadísticas para las recomendaciones normativas;
- c) Determinar los obstáculos posibles a la reunión de estadísticas exactas;
- d) Identificar los países que reúnen estadísticas específicas sobre delitos cibernéticos;
- e) Evaluar la necesidad y las ventajas de reunir información estadística sobre el delito cibernético;
- f) Examinar las técnicas posibles que podrían utilizarse para reunir esta información;
- g) Analizar un modelo posible de autoridad central depositaria de información estadística.

Tema 3. Desafíos del delito cibernético

Antecedentes

17. Actualmente se está prestando mucha atención a la elaboración de estrategias para abordar los desafíos concretos del delito cibernético. Esto obedece a dos razones: en primer lugar, que algunos de los instrumentos necesarios para investigar el delito cibernético son nuevos y por ello requieren investigación intensiva, y en segundo lugar, que la investigación de los delitos que entrañan tecnología de redes está acompañada de varios desafíos singulares en comparación con las investigaciones tradicionales.

Desafíos de la lucha contra el delito cibernético y amenazas conexas

18. La lista de desafíos técnicos y jurídicos singulares del delito cibernético es larga. El hecho de que los delincuentes puedan cometer delitos cibernéticos por medio de aparatos que no exigen conocimientos técnicos profundos, como

²⁷ Véase Organismo del Reino Unido contra la Delincuencia Organizada Grave, “International crackdown on mass marketing fraud revealed, 2007”

²⁸ Según el informe del National White Collar Crime Center sobre delitos de Internet en 2006, solo el 1,7% de la cifra total denunciada de pérdidas en dólares de los EE.UU. guardaba relación con el fraude de las cartas nigerianas, pero en los casos denunciados en promedio la pérdida fue de 5.100 dólares cada uno. El número de delitos denunciados es muy bajo, mientras que la pérdida promedio a causa de esos delitos es elevada.

programas informáticos²⁹ destinados a localizar vías de acceso abiertas o descifrar códigos de acceso, es solo un ejemplo de ello³⁰. Otro desafío es la dificultad de rastrear a los delincuentes. Aunque los usuarios dejen múltiples rastros al utilizar los servicios de Internet, los delincuentes pueden obstaculizar las investigaciones al ocultar su identidad. Por ejemplo, si los delincuentes cometen delitos utilizando terminales de Internet públicas o redes inalámbricas abiertas puede ser difícil encontrarlos. Un problema de carácter más general al investigar el delito cibernético surge del hecho de que, desde una perspectiva tecnológica, Internet ofrece pocos instrumentos de control que puedan utilizar las autoridades de represión. Internet se concibió inicialmente como una red militar³¹ basada en una arquitectura de red descentralizada que procuraba mantener su funcionalidad principal intacta, aunque se atacaran los componentes de la red. Este enfoque descentralizado no se concibió inicialmente para facilitar las investigaciones penales ni para prevenir los ataques desde dentro de la red, y las medidas de investigación que requieren un medio de control plantean desafíos singulares en ese entorno³².

Alcance del estudio

19. El estudio de este tema consistirá en:

- a) Hacer un inventario amplio de problemas relacionados con la lucha contra el delito cibernético;
- b) Preparar un resumen de las mejores prácticas, tanto técnicas como jurídicas, para hacer frente a esos problemas.

Tema 4. Enfoques comunes de la legislación

Antecedentes

20. En los últimos 20 años, distintos países y organizaciones regionales han elaborado legislación y marcos jurídicos para abordar el delito cibernético. Pese a que se han establecido algunas tendencias comunes, las diferencias entre las leyes nacionales siguen siendo importantes.

Diferencias nacionales y regionales

21. Una razón de las diferencias nacionales y regionales en los marcos legislativos es que las consecuencias del delito cibernético no son las mismas en todo el mundo,

²⁹ Websense, “*Security Trends Report 2004*”, pág. 11; Estados Unidos de América, Oficina General de Cuentas, *Information Security I: Computer Controls over Key Treasury Internet Payment System*, GAO-03.837, (Washington, D.C., 2003), pág. 3; U. Sieber, “The threat of cybercrime”, en *Organised Crime in Europe: The Threat of Cybercrime — Situation Report 2004* (Strasburgo, publicación del Consejo de Europa, 2005), pág. 143.

³⁰ Ealy, “A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention”, SANS Institute, 2003, pág. 9.

³¹ Para una breve historia de Internet, incluidos sus orígenes militares, véase Leiner, y col. “A Brief History of the Internet”, que puede consultarse en: www.isoc.org/internet/history/brief.shtml.

³² H. F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Pittsburgh, Carnegie Mellon University, Software Engineering Institute, 2002).

como lo demuestra la lucha contra el correo basura³³. El correo-e basura ha resultado ser un problema mucho más serio en los países en desarrollo que en los países occidentales como consecuencia de la escasez y el costo de los recursos³⁴. En lo que se refiere al contenido ilícito, algunos países y regiones tal vez penalicen la difusión de material que podría considerarse protegido por el principio de la libertad de palabra³⁵ en otros³⁶.

22. Habida cuenta de que el delito cibernético es realmente un delito transnacional³⁷, la cooperación internacional es un requisito indispensable para que la investigación y el enjuiciamiento prosperen³⁸. La cooperación internacional eficaz exige un grado de armonía de criterios y la armonización de la legislación a fin de prevenir la creación de refugios³⁹.

³³ El ciberdelito: Guía para los países en desarrollo, (véase la nota 13 *supra*).

³⁴ Véase Organización de Cooperación y Desarrollo Económicos, “Spam Issue in Developing Countries”, document DSTI/CP/ICCP/SPAM(2005)6/FINAL, de 26 de mayo de 2005, pág. 4, que puede consultarse en: www.oecd.org/dataoecd/5/47/34935342.pdf.

³⁵ En lo que respecta al principio de la libertad de palabra, véanse: T. L. Tedford y D. A. Herbeck, *Freedom of Speech in the United States*, (State College, Pennsylvania, Strata, 5ª ed. 2005); Barendt, *Freedom of Speech*, (Oxford, Oxford University Press, 2007); C. E. Baker; *Human Liberty and Freedom of Speech*; (Nueva York, Oxford University Press, 1989); C. E. Emord, *Freedom, Technology and the First Amendment*, (San Francisco, Pacific Research Institute for Public Policy, 1991); en relación con la importancia del principio respecto de la vigilancia electrónica, véanse C. Woo y M. So, “The case for Magic Lantern: September 11 Highlights the need for increasing surveillance”, *Harvard Journal of Law & Technology*, vol. 15, núm. 2, 2002, págs. 530 y ss.; C. M. Vhesterman, *Freedom of Speech in Australian Law; A Delicate Plant*, (Aldershot, Hampshire, Ashgate, 2000); E. Volokh, “Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law”, *Loyola University Chicago Law Journal*, vol. 33, 2001, págs. 57 y ss., que puede consultarse en: www.law.ucla.edu/volokh/harass/religion.pdf; H. Cohen, “Freedom of Speech and Press: Exceptions to the First Amendment”, Congressional Research Service Report 95-815, 2009, que puede consultarse en: www.fas.org/sgp/crs/misc/95-815.pdf.

³⁶ La preocupación por la libertad de expresión (por ejemplo, la Primera Enmienda de la Constitución de los Estados Unidos) explica por qué determinados actos de racismo no se consideraron ilícitos en el Convenio sobre la Ciberdelincuencia, (Consejo de Europa, núm. 185) aunque se tipificaron en el Protocolo Adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de indole racista y xenófoba cometidos por medio de sistemas informáticos (Consejo de Europa, Serie de tratados europeos, núm. 189). Véase también el informe explicativo al protocolo adicional, que se puede consultar en <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

³⁷ En lo que respecta al alcance de los ataques transnacionales en los ataques cibernéticos que más daño causan, véase: A. D. Sofaer y S. E. Goodman, “Cyber Crime and Security – The Transnational Dimension”, en *The Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer y S. E. Goodman edit., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), pág. 7, que puede consultarse en: http://media.hoover.org/documents/0817999825_1.pdf.

³⁸ En lo que respecta a la necesidad de cooperación internacional en la lucha contra el delito cibernético, véanse: T. L. Putnam y D. D. Elliott, “International Responses to Cyber Crime”, en *Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer y S. E. Goodman, edit., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), págs. 35 y ss., que puede consultarse en: http://media.hoover.org/documents/0817999825_35.pdf; y Sofaer y Goodman, “Cyber Crime and Security – The Transnational Dimension”.

³⁹ En lo que respecta al principio de la doble incriminación en las investigaciones internacionales, véanse “Manual de las Naciones Unidas sobre prevención y control de delitos informáticos”,

Alcance del estudio

23. El estudio de este tema consistirá en:

- a) El análisis de las iniciativas encaminadas a adoptar enfoques comunes de la legislación en materia de delito cibernético;
- b) Otros elementos pertinentes a la adopción de enfoques comunes de la legislación en materia de delito cibernético, incluida la gravedad percibida de la conducta delictiva y la repercusión de las normas de derechos humanos;
- c) La recopilación de un inventario sobre la forma en que los países aplican las normas jurídicas de las organizaciones regionales y un análisis de las técnicas que pueden contribuir a garantizar la coherencia de los enfoques;
- d) El análisis del grado en que las diferencias en las normas jurídicas afectan a la cooperación internacional.

Tema 5. Tipificación de los delitos cibernéticos**Antecedentes**

24. La investigación y enjuiciamiento eficaces del delito cibernético exigirán la tipificación de nuevos delitos si una conducta determinada aún no está incluida en la legislación vigente. La existencia de legislación adecuada es no solo pertinente para las investigaciones nacionales sino que también puede influir en la cooperación internacional, como se describió anteriormente.

Derecho penal sustantivo

25. La mayoría de los marcos regionales amplios establecidos para abordar el problema del delito cibernético contienen un conjunto de disposiciones de derecho penal sustantivo destinadas a suplir las deficiencias de la legislación nacional. Por lo general, las disposiciones de esos marcos incluyen la penalización del acceso ilícito, la interceptación ilícita, la interferencia ilícita en la integridad de los datos, la interferencia ilícita en la integridad de los sistemas, el fraude informático y la falsificación informática. Algunos marcos nacionales pueden ir más lejos y penalizar delitos como la producción y distribución de instrumentos (como los programas o el equipo informático) que pueden utilizarse para cometer delitos informáticos, o con fines terroristas, actos relacionados con la materiales relativos al abuso de niños, la seducción de menores o discursos de incitación al odio.

Alcance del estudio

26. El estudio se basará en las conclusiones del estudio sobre el tema 1 acerca del fenómeno del delito cibernético:

Revista Internacional de Política Criminal, núms. 43 y 44, 1994 (publicación de las Naciones Unidas, núm. de venta S.94.IV.5), párr. 269, que puede consultarse en: www.uncjin.org/Documents/EighthCongress.html; juez Stein Schjolberg y Amanda M. Hubbard, "Harmonizing national legal approaches on cybercrime", documento preparado para la Unión Internacional de Telecomunicaciones, reunión temática sobre ciberseguridad en la Cumbre Mundial sobre la Sociedad de la Información, Ginebra, 28 de junio a 1 de julio de 2005, pág. 5,

- a) Un inventario de enfoques nacionales y regionales sobre la tipificación del delito cibernético, incluso en relación con la participación en él y la tentativa de cometerlo;
- b) Una evaluación de las mejores prácticas con respecto a la tipificación del delito cibernético;
- c) El análisis de las diferencias de enfoque entre los distintos ordenamientos y tradiciones jurídicos respecto de la tipificación del delito cibernético.

Tema 6. Facultades en materia de procedimiento

Antecedentes

27. Para realizar investigaciones eficaces, los organismos encargados del cumplimiento de la ley deben tener acceso a procedimientos de investigación que les permitan adoptar las medidas necesarias para encontrar al delincuente y reunir las pruebas requeridas para las actuaciones penales⁴⁰. Esas medidas pueden ser las mismas que las utilizadas en las investigaciones tradicionales no relacionadas con el delito cibernético. No obstante, por el hecho de que los delincuentes no tienen que estar presentes en el lugar del delito o cerca de este, es muy probable que las investigaciones deban realizarse de manera muy distinta de la tradicional⁴¹.

Medidas de investigación

28. Además de las disposiciones relativas a los delitos cibernéticos sustantivos, la mayoría de los marcos regionales amplios establecidos para hacer frente a ese problema contienen también un conjunto de disposiciones concebido concretamente para facilitar las investigaciones sobre él. Esas disposiciones comprenden por lo general procedimientos concretos de inspección e incautación, la conservación rápida de datos informáticos, la revelación de los datos almacenados, la interceptación de datos relativos al contenido y la recopilación de datos relativos al tráfico.

⁴⁰ Por lo que atañe a los enfoques basados en las necesidades de los usuarios en la lucha contra el ciberdelito, véase S. Görling, “The myth of user education”, documento preparado para la *Virus Bulletin Conference*, celebrada en Montreal del 11 al 13 de octubre de 2006, que puede consultarse en el sitio www.virusbtn.com/conference/vb2006/abstracts/Gorling.xml.

Véase también la observación formulada por Jean-Pierre Chevènement, Ministro del Interior de Francia, durante una conferencia sobre la seguridad y la confianza en el ciberespacio del Grupo de los Ocho celebrada en París en 2000, en el sentido de que en términos generales, se debía educar a los usuarios, y de que estos debían comprender lo que podían y no podían hacer en Internet y estar advertidos de los posibles peligros, a medida que aumentaba la utilización de Internet, se debería, naturalmente, intensificar las iniciativas a ese respecto.

⁴¹ Por los protocolos que se utilizan en las comunicaciones por Internet y la posibilidad de acceso mundial a ella, es muy poco necesaria la presencia física en el lugar en que se ofrece un servicio. Por esa independencia entre el lugar en que transcurre la acción y el lugar en que se comete el delito, muchos de los relacionados con Internet son de carácter transnacional. Con respecto a la independencia del lugar del delito y el resultado de este véase la publicación titulada “El ciberdelito: Guía para los países en desarrollo” (véase la nota de pie de página 13 *supra*), cap. 3.2.7.

29. En la actualidad, los organismos de aplicación de la ley se ven enfrentados a tecnologías nuevas que repercuten negativamente en los métodos de investigación clásicos. Muchos de esos problemas siguen por resolver.

Alcance del estudio

30. El estudio de este tema consistirá en lo siguiente:

a) Un inventario de ejemplos de casos de investigaciones en que se haya puesto de relieve la necesidad de medidas de investigación especiales para los delitos cibernéticos;

b) Un inventario de diferentes disposiciones en materia de investigación contenidas en los marcos jurídicos regionales y nacionales;

c) Una reseña de las necesidades actuales de los organismos de aplicación de la ley en relación con las disposiciones concretas relativas al delito cibernético, a fin de hacer frente a los problemas creados por las nuevas tecnologías;

d) Un análisis de las diferencias de enfoque respecto de las disposiciones en materia de investigación relativas al delito cibernético en distintos ordenamientos y tradiciones jurídicas.

Tema 7. Cooperación internacional

Antecedentes

31. Un número cada vez mayor de delitos cibernéticos tiene una dimensión internacional⁴², en particular debido a que los delincuentes, aprovechando el carácter transnacional de Internet, con frecuencia no tienen necesidad de estar presentes en el mismo lugar que la víctima. Esta separación entre la ubicación de víctimas y delincuentes y la movilidad de estos últimos determinan la necesidad de que las autoridades judiciales y las de represión cooperen a nivel internacional y presten asistencia al Estado que haya asumido la jurisdicción⁴³. La cooperación internacional eficaz plantea uno de los principales problemas para combatir el delito, cada vez más globalizado, tanto en sus formas tradicionales como en el plano cibernético. Las diferencias de legislación y de prácticas entre los Estados, así como el número relativamente limitado de tratados y acuerdos sobre cooperación internacional entre Estados, pueden hacer que la cooperación internacional sea

⁴² Con respecto a la dimensión transnacional del delito cibernético, véase Mike Keyser, "The Council of Europe Convention on Cybercrime", *Journal of Transnational Law and Policy*, vol. 12, núm. 2 (2003), pág. 289, que puede consultarse en el sitio www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. Sofaer y Goodman, "Cyber crime and security: the transnational dimension" (véase la nota de pie de página 37 *supra*), págs. 1 y ss.

⁴³ En este contexto, véanse las Guías legislativas para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos (publicación de las Naciones Unidas, núm. de venta S.05.V.2), pág. 217. Ese texto puede consultarse en el sitio www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

difícil⁴⁴. Además, se debería discutir y llegar a un acuerdo sobre qué es lo que debe considerarse una cuestión internacional en los casos de delitos cibernéticos.

Instrumentos de cooperación internacional

32. Hay distintas fuentes de bases jurídicas necesarias para la cooperación internacional oficial en ámbitos como la extradición, la asistencia judicial recíproca en asuntos penales y la cooperación con fines de decomiso. Las disposiciones sobre cooperación internacional pueden formar parte de acuerdos internacionales y regionales, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional⁴⁵.

Alcance del estudio

33. El estudio de este tema consistirá en lo siguiente:

a) Un inventario de los enfoques jurídicos nacionales adoptados para determinar el carácter internacional en materia de represión de los delitos relacionados con Internet;

b) El examen de opciones con respecto a bases jurídicas eficaces, incluso de carácter internacional y universal, y el de otras formas de combatir el delito cibernético;

c) Las dificultades para establecer una cooperación internacional eficaz, en particular en materia de extradición y asistencia judicial recíproca, en casos de delito cibernético, incluida la aplicación de la doble incriminación y las diferencias entre las medidas de investigación;

d) Un inventario de las disposiciones nacionales e internacionales sobre cooperación internacional pertinentes a la investigación y el enjuiciamiento del delito cibernético;

e) Un inventario de ejemplos de las mejores prácticas extraídas de tratados y arreglos bilaterales y multilaterales, por ejemplo, entre otras cosas, las enseñanzas obtenidas del funcionamiento de la red de coordinadores 24/7;

f) Un inventario de los casos de delito cibernético que requirieron cooperación internacional;

g) La función de los mecanismos oficiosos de cooperación internacional, por ejemplo para el intercambio de información, y los problemas a ese respecto;

h) Una reseña de las necesidades actuales de las autoridades correspondientes en materia de la cooperación internacional;

⁴⁴ Carlos A. Gabuardi, "Institutional framework for international judicial cooperation: opportunities and challenges for North America", *Mexican Law Review*, vol. 1, núm. 2 (2009), pág. 156, que puede consultarse en el sitio <http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf>.

⁴⁵ Naciones Unidas, *Treaty Series*, vol. 2225. núm. 39574; con respecto a esa Convención, véase Jennifer M. Smith, "An international hit job: prosecuting organized crime acts as crimes against humanity", *Georgetown Law Journal*, vol. 97, 2009, pág. 1.118, que puede consultarse en el sitio www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

i) La determinación de los programas de capacitación en curso y las ideas para los previstos en el futuro, el intercambio de experiencias, la creación de capacidad y las actividades de asistencia técnica para reforzar las capacidades de la justicia penal y posibilitar la cooperación internacional.

Tema 8. Pruebas electrónicas

Antecedentes

34. Como se guarda cada vez más información en formato digital, las pruebas electrónicas son pertinentes tanto para las investigaciones de delitos cibernéticos como para las tradicionales. La tecnología de computadora y redes ya forma parte de la vida cotidiana en los países desarrollados, y lo mismo está sucediendo en los países en desarrollo. El aumento de la capacidad de los discos duros⁴⁶ y el costo relativamente bajo⁴⁷ del almacenamiento de documentos digitales en comparación con el almacenamiento de los impresos, ha hecho aumentar cada vez más el número de documentos digitales⁴⁸. En la actualidad, se almacena una cantidad considerable de datos únicamente en formato digital⁴⁹. Debido a ese aumento, la documentación electrónica, como los documentos de texto, los vídeos digitales y las fotografías digitales⁵⁰ resultan importantes en las investigaciones del delito cibernético y las actuaciones judiciales conexas⁵¹.

⁴⁶ Véase D. Abramovitch, “A brief history of hard drive control”, *IEEE Control Systems Magazine*, vol. 22, núm. 3 (2002), pág. 28 y ss.; T. Coughlin, D. Waid y J. Porter, “The disk drive: 50 years of progress and technology innovation — the road to two billion drives”, *Computer Technology Review*, abril de 2005, que pueden consultarse en el sitio www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

⁴⁷ S. M. Giordano, “Electronic evidence and the law”, *Information Systems Frontiers*, vol. 6, núm. 2 (2006), pág. 161; S. D. Willinger y R. M. Wilson, “Negotiating the minefields of electronic discovery”, *Richmond Journal of Law and Technology*, vol. 10, núm. 5 (2004).

⁴⁸ Lange/Minster, *Electronic Evidence and Discovery*, pág. 6.

⁴⁹ Chet Hosmer, “Proving the integrity of digital evidence with time”, *International Journal of Digital Evidence*, vol. 1, núm. 1 (2002), pág. 1, que puede consultarse en el sitio www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

⁵⁰ Con respecto a la admisibilidad y fiabilidad de las imágenes digitales, véase Jill Witkowski, “Can juries really believe what they see? New foundational requirements for the authentication of digital images”, *Washington University Journal of Law and Policy*, vol. 10, 2002, págs. 267 y ss.

⁵¹ Michael Harrington, “A methodology for digital forensics”, *Thomas M. Cooley Journal of Practical and Clinical Law*, vol. 7, 2004, págs. 71 y ss.; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 2ª edición (Londres, Academic Press, 2004), pág. 14. con respecto a los marcos jurídicos de los distintos países, véanse C. A. Rohrmann y J.S.A. Neto, “Digital evidence in Brazil”, *Digital Evidence and Electronic Signature Law Review*, núm. 5, 2008; M. Wang, “Electronic evidence in China”, *Digital Evidence and Electronic Signature Law Review*, núm. 5, 2008; P. Bazin, “An outline of the French law on digital evidence”, *Digital Evidence and Electronic Signature Law Review*, núm. 5, 2008; A. B. Makulilo, “Admissibility of computer evidence in Tanzania”, *Digital Evidence and Electronic Signature Law Review*, núm. 4, 2007; R. Winick, “Search and seizures of computers and computer data”, *Harvard Journal of Law and Technology*, vol. 8, núm. 1 (1994), pág. 76; F. Insa, “Situation report on the admissibility of electronic evidence in Europe”, en *Syllabus to the European Certificate on Cybercrime and E-Evidence*, 2008, pág. 213.

Normas relativas a las pruebas electrónicas

35. Las pruebas electrónicas plantean una serie de desafíos, tanto en la etapa en que se recogen como en la de su admisión como pruebas⁵². Durante el trámite de reunión de pruebas, los investigadores deben cumplir determinados procedimientos y requisitos, como el trato especial que se requiere para la protección de la integridad de los datos. Los servicios policiales necesitan que se adopten medidas concretas para poder realizar investigaciones fructíferas. Esas medidas son especialmente pertinentes si no se dispone de las fuentes de pruebas tradicionales como las huellas dactilares o la identificación por testigos. En esos casos, la posibilidad de identificar y enjuiciar debidamente a un delincuente se basa en la reunión y evaluación correctas de pruebas digitales⁵³.

36. La digitalización también influye en la forma en que los organismos de represión y los tribunales utilizan las pruebas⁵⁴. Mientras que los documentos tradicionales simplemente se entregan en los tribunales, las pruebas digitales tal vez exijan procedimientos concretos que no son adecuados para su conversión en pruebas tradicionales, por ejemplo, ejemplares impresos de archivos⁵⁵.

Alcance del estudio

37. El estudio de este tema consistirá en lo siguiente:

a) Un inventario de las disposiciones, salvaguardias y normas relativas a la reunión, la conservación, el almacenamiento, el análisis y la admisibilidad de pruebas electrónicas;

b) El análisis de las diferencias de enfoque y para la determinación de principios comunes en relación con las pruebas electrónicas en los distintos ordenamientos y tradiciones jurídicas;

c) La recopilación de las mejores prácticas en materia de capacitación especializada, creación de capacidad e intercambio de tecnología;

d) El análisis del mecanismo para el intercambio transfronterizo de pruebas digitales.

⁵² Casey, *Digital Evidence and Computer Crime* (véase la nota de pie de página 51), pág. 9.

⁵³ Por lo que atañe a la necesidad de formalizar la informática forense, véase R. Leigland y A. W. Krings, "A formalization of digital forensics", *International Journal of Digital Evidence*, vol. 3, núm. 2 (2004).

⁵⁴ En lo que respecta a las dificultades de utilizar las pruebas digitales sobre la base de los procedimientos y las doctrinas tradicionales, véase R. Moore, "To view or not to view: examining the plain view doctrine and digital evidence", *American Journal of Criminal Justice*, vol. 29, núm. 1 (2004), pág. 57 y ss.

⁵⁵ Véase John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 2ª ed. (Hingham, Massachusetts, Charles River Media, 2005), pág. 3. Por lo que atañe al análisis anterior sobre el uso de ejemplares impresos, véase Robinson, "The admissibility of computer printouts under the business records exception in Texas", *South Texas Law Journal*, vol. 12, 1970, pág. 291 y ss.

Tema 9. Funciones y responsabilidades de los proveedores de servicios y el sector privado

Antecedentes

38. La prevención e investigación del delito cibernético dependen de distintos elementos. Aunque el delincuente actúe solo, la comisión de un delito cibernético supone automáticamente que intervengan otras personas y empresas. Por la estructura de Internet, la transmisión de un simple correo electrónico exige el servicio de varios proveedores, como el proveedor de correo electrónico, los proveedores de acceso y los enrutadores que envían ese correo electrónico al destinatario. La situación es parecida en el caso de la descarga de material relativo a la explotación sexual de niños. En el procedimiento de descarga intervienen el proveedor de contenido que cargó las fotografías (por ejemplo, en un sitio web) el proveedor de hospedaje que proporcionó los medios de almacenamiento para el sitio web, los enrutadores que enviaron los archivos al usuario y, por último, el proveedor de acceso que permitió al usuario entrar en Internet.

39. Aunque con frecuencia se hace hincapié en promulgar legislación apropiada, el sector privado sigue cumpliendo una función importante, tanto para prevenir el delito cibernético como para contribuir a su investigación. No obstante, su participación en esas investigaciones entraña una serie de dificultades.

Cuestiones jurídicas

40. El hecho de que un delito cibernético no pueda cometerse sin la intervención de los proveedores, unido al hecho de que esos proveedores a menudo no pueden impedir que se cometan tales delitos, plantea la cuestión de si se debería limitar la responsabilidad de los proveedores de servicios. La respuesta a esa pregunta es fundamental para el desarrollo económico de la infraestructura de la tecnología de la información y las comunicaciones.

41. Las iniciativas de los organismos policiales dependen con gran frecuencia de la cooperación de los proveedores de servicios de Internet. Ello plantea cierta preocupación, porque imponer responsabilidades a esos prestadores de servicios o limitarlas con respecto a los actos realizados por sus usuarios podría repercutir en la cooperación y el apoyo de esos proveedores respecto de las investigaciones de delitos cibernéticos, así como en la propia prevención de ese tipo de delito.

La función de la industria

42. La función de la industria en la lucha contra el delito cibernético es compleja y puede abarcar desde la elaboración y aplicación de soluciones para proteger sus propios servicios de su uso indebido por los delincuentes hasta la protección de los usuarios y el apoyo a las investigaciones. Las medidas de protección adoptadas por ese sector suelen ser un componente lógico de las estrategias empresariales amplias, y por lo general no requieren una base jurídica concreta mientras esas medidas no supongan contramedidas activas ilícitas. Dichas medidas de protección adoptadas en nombre de los usuarios, siempre que se hayan adoptado con el consentimiento de estos, tampoco plantean problemas. Sin embargo, la participación de la industria en las investigaciones penales ha planteado dificultades en muchos países y se han adoptado diferentes enfoques a ese respecto. En algunos países, el sector participa

en esas investigaciones de manera exclusivamente voluntaria, y se han elaborado directrices para facilitar la cooperación de la industria y los organismos policiales. En otros países se ha adoptado un enfoque diferente, conforme al cual se ha impuesto a la industria la obligación legal de cooperar con los organismos de policía en las investigaciones penales.

Alcance del estudio

43. El estudio de este tema consistirá en:

- a) Enfoques y prácticas relacionados con la responsabilidad de los proveedores de los servicios, incluida la diferenciación entre los distintos tipos de proveedores;
- b) La planificación del papel, la naturaleza y las funciones del sector privado, incluidos los proveedores de servicios;
- c) Prácticas de prevención e investigación del delito cibernético por el sector privado;
- d) Prácticas relacionadas con la cooperación entre el sector privado y las fuerzas de seguridad en la prevención e investigación del delito cibernético;
- e) Capacidad de los proveedores de servicios nacionales y multinacionales para prestar asistencia a las fuerzas de seguridad en la prevención e investigación de los delitos cibernéticos;
- f) Asignación de los gastos relacionados con el delito cibernético;
- g) Evaluación de los aspectos fuertes y débiles de los enfoques existentes.

Tema 10: Capacidades en materia de prevención del delito y justicia penal y otras respuestas ante el delito cibernético

Antecedentes

44. El debate acerca de las respuestas al delito cibernético con frecuencia se centra en la respuesta jurídica, pero las estrategias contra el delito cibernético por lo general siguen un enfoque más amplio.

Otras respuestas

45. Además de las respuestas jurídicas al delito cibernético, otras respuestas incluyen la adopción de medidas de prevención del delito, el establecimiento de la infraestructura necesaria para investigar y enjuiciar los delitos (por ejemplo, equipo y personal), la capacitación de los expertos que participan en la lucha contra el delito cibernético, la formulación de mejores prácticas, la educación de los usuarios de Internet y las soluciones técnicas para prevenir o investigar el delito cibernético.

Alcance del estudio

46. El estudio de este tema consistirá en:
- a) Una reseña de otros métodos utilizados para dar respuesta al delito cibernético;
 - b) Medidas para prevenir el delito cibernético;
 - c) Determinación de los medios necesarios para medir el éxito de estos métodos;
 - d) Análisis de la relación entre las diferentes respuestas y las posibilidades de adoptarlas en conjunto;
 - e) Posible papel de los círculos académicos, particularmente por medio de la formulación de programas apropiados de estudio e investigación del fenómeno del delito cibernético.

Tema 11. Organizaciones internacionales**Antecedentes**

47. En los decenios de 1970 y 1980, los enfoques jurídicos del delito cibernético se adoptaron principalmente en el plano nacional. En el decenio de 1990, la cuestión del delito cibernético comenzó a abordarse en las organizaciones regionales e internacionales, en particular por conducto de la Asamblea General, que a lo largo de los años ha aprobado varias resoluciones sobre el delito cibernético⁵⁶, el Commonwealth (Ley Modelo sobre el delito cibernético y la posible ampliación del Plan de la Commonwealth para la asistencia mutua en materia penal (Plan de Harare), a fin de que abarque los datos electrónicos), el Consejo de Europa (Convenio sobre el delito cibernético), la Unión Europea (Decisión marco relativa a los ataques contra los sistemas de información y el Convenio celebrado por el Consejo de conformidad con el artículo 34 del Tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los Estados Miembros de la Unión Europea), la Comunidad de Estados Independientes (CEI) (Acuerdo sobre la Cooperación entre los países de la CEI para luchar contra el delito en la esfera de la información computadorizada, de 2001), la Organización de los Estados Americanos y la Organización de Cooperación de Shanghai. Las organizaciones internacionales, entre ellas la Unión Internacional de Telecomunicaciones, que ha emprendido actividades en el marco de la Agenda sobre Ciberseguridad Global, y la Oficina de las Naciones Unidas contra la Droga y el Delito, han reunido datos y preparado estudios.

Armonización de normas

48. Las normas unificadas relativas a los protocolos técnicos han dado buenos resultados y han planteado la cuestión de la forma en que pueden evitarse los

⁵⁶ Por ejemplo, resoluciones de la Asamblea General 45/12, 55/63, 56/121 y 60/177.

conflictos entre diferentes enfoques internacionales⁵⁷. El Convenio sobre el delito cibernético del Consejo de Europa y la Ley Modelo de la Commonwealth sobre el delito cibernético han adoptado el enfoque más amplio, ya que abarcan el derecho penal sustantivo, el derecho procesal y la cooperación internacional. En relación con este tema podría emprenderse un examen de los marcos existentes para determinar su alcance, fortalezas, debilidades y posibles deficiencias.

Alcance del estudio

49. El estudio de este tema consistirá en:

- a) Un inventario de las mejoras prácticas de las organizaciones regionales e internacionales, incluidas las Naciones Unidas;
- b) Fortalezas y debilidades de los enfoques existentes;
- c) Análisis de las lagunas en los enfoques jurídicos internacionales existentes.

Tema 12. Asistencia técnica

Antecedentes

50. Contrariamente de lo que a veces se cree, el delito cibernético no es un problema que afecte principalmente a los países desarrollados. En 2005, el número de usuarios de Internet en los países en desarrollo superó por primera vez el de las naciones industrializadas⁵⁸. Dado que uno de los objetivos fundamentales de las estrategias de la lucha contra el delito cibernético es impedir que los usuarios se conviertan en víctimas de dicho delito, no debe subestimarse la importancia de la lucha contra el delito cibernético en los países en desarrollo. También es fundamental tener en cuenta el hecho de que las consecuencias del delito cibernético tal vez sean distintas en los países en desarrollo y en los países desarrollados. En 2005, la Organización de Cooperación y Desarrollo Económicos publicó un informe en el que se analizó el efecto del correo-e basura en los países en desarrollo⁵⁹ y se llegó a la conclusión de que los países en desarrollo a menudo informan de que sus usuarios de Internet sufren más a causa de los efectos de ese tipo de correo y el uso indebido de Internet.

Asistencia técnica

51. La dimensión transnacional del delito cibernético exige que todos los países actúen de manera coordinada y eficaz. Los países desarrollados y los países en desarrollo tienen un interés similar en la prestación de asistencia técnica. Evitar el establecimiento de refugios seguros para los delincuentes cibernéticos es uno de los principales desafíos de la lucha contra ese tipo de delito⁶⁰. Por consiguiente, el

⁵⁷ Para más detalles, véase M. Gercke "National, Regional and International Legislative Approaches in the Fight Against Cybercrime", *Computer Law Review International*, 2008, págs. 7 y ss.

⁵⁸ Véase Development Gateway's Special Report, *Information Society - The Next Steps* (2005).

⁵⁹ "Spam issues in developing countries" (véase la nota 34).

⁶⁰ Esta cuestión se trató en distintas organizaciones internacionales. En la resolución 55/63 de la Asamblea General se señala que: "los Estados deben velar para que en su legislación y en la

fomento de la capacidad de los países en desarrollo para permitirles combatir el delito cibernético se ha convertido en una importante tarea de la comunidad internacional.

52. La importancia de la asistencia técnica se refleja en la Declaración de Salvador, aprobada por el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en 2010, en la que se recomendó que la Oficina de las Naciones Unidas contra la Droga y el Delito prestara asistencia técnica a los Estados que lo solicitaran para hacer frente al delito cibernético. También se propuso que se considerara la posibilidad de adoptar un plan de acción para el fomento de la capacidad a escala internacional, que se elaboraría con todos los interlocutores pertinentes. La asistencia técnica debería mantenerse actualizada y prestarse ininterrumpidamente.

Alcance del estudio

53. El estudio de este tema consistirá en:

- a) Determinación de los elementos y principios fundamentales de la asistencia técnica para abordar el delito cibernético;
- b) Inventario de los cursos de capacitación sobre delitos cibernéticos existentes a nivel nacional, regional e internacional;
- c) Determinación de las mejores prácticas para suministrar asistencia técnica relativa al delito cibernético.

práctica se eliminen los refugios seguros para quienes utilicen la tecnología de la información con fines delictivos”. El texto completo de la resolución puede consultarse en www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. En los principios y el plan de acción para convertir el delito de alta tecnología aprobados en la reunión de Ministros de Justicia y del Interior del Grupo de los 8, celebrada en Washington D.C. el 10 de diciembre de 1997, se destaca que deben eliminarse los refugios seguros para quienes utilicen indebidamente las tecnologías de la información.

Anexo II

Metodología para la realización del estudio

1. A fin de cumplir el mandato del Grupo de expertos en relación con el estudio, se ha elaborado la estructura expuesta más adelante con objeto de facilitar su realización, que se llevará a cabo bajo los auspicios del Grupo de expertos.
2. Cada país tendrá derecho a exponer sus opiniones, que deberán reflejarse en el estudio.
3. Se encargará a la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) la preparación del estudio, incluida la formulación de un cuestionario, la reunión y el análisis de los datos y la redacción de un proyecto de texto del estudio. Para cumplir esta tarea, la UNODC se apoyará en sus propios conocimientos especializados y capacidad recurriendo a sus diversas subdivisiones temáticas (División para Asuntos de Tratados, Subdivisión de Política e Investigaciones). A ese fin, deberán ponerse a disposición de la Oficina suficientes recursos extrapresupuestarios para que pueda cumplir estas funciones eficientemente. Con objeto de ayudar a la Secretaría a garantizar una adecuada representación de los principales conocimientos especializados tecnológicos, y de los sistemas y las necesidades existentes en este ámbito, cada grupo regional le proporcionará nombres de expertos gubernamentales (no más de seis), la información necesaria para establecer contacto con ellos y sus esferas de conocimientos. La Secretaría consultará con estos expertos en calidad de recursos que se utilizarán en cada caso según sea necesario.
4. La Secretaría informará y consultará regularmente a la Mesa del Grupo de expertos en relación con el proceso y distribuirá a los Estados Miembros las minutas de las consultas. La preparación de la lista de expertos no tiene por objeto crear un Grupo de expertos limitado ni cualquier otro órgano paralelo o subsidiario del Grupo de expertos.
5. En lo que respecta a la reunión de información, la UNODC preparará un cuestionario para su divulgación a los Estados Miembros, organizaciones internacionales y entidades del sector privado (véase el plazo indicativo que figura más adelante), el cual consistirá en un único instrumento de encuesta basado en las directrices contenidas en el documento conceptual y de trabajo de la primera reunión del Grupo de expertos, en su versión enmendada, y en las recomendaciones de la primera reunión del Grupo de expertos reflejadas en su informe.
6. De forma secundaria, y según sea preciso, la Secretaría, teniendo presente la necesidad de contar con una representación equilibrada de las diferentes regiones, celebrará consultas con representantes del sector privado, incluidos representantes de los proveedores de servicios de Internet, los usuarios de esos servicios y otros interlocutores pertinentes; representantes de los círculos académicos, tanto de los países desarrollados como de los países en desarrollo; y representantes de las organizaciones intergubernamentales pertinentes.

Plazos indicativos

Enero de 2011: Presentación de orientaciones normativas y directrices por la primera reunión del Grupo de expertos. Aprobación de los temas, la metodología y los plazos del estudio.

Febrero a abril de 2011: Determinación de los expertos que prestarán asistencia a la UNODC en la realización del estudio (véase *supra*). Presentación de los nombres a la Mesa del Grupo de expertos. Comunicación de los nombres de los expertos gubernamentales por conducto de los grupos regionales.

Abril de 2011: Celebración del 20º período de sesiones de la Comisión de Prevención del Delito y Justicia Penal. Distribución de un proyecto de cuestionario de la UNODC para reunir información. Solicitud de observaciones de los Estados Miembros al respecto. Consultas en línea para recibir observaciones de los miembros del Grupo de expertos. El reconocimiento por la Comisión de los resultados de la primera reunión del Grupo de expertos y la labor futura, propuesta en la primera reunión.

Mediados de junio de 2011: Plazo para la recepción de observaciones sobre el cuestionario.

Mediados de julio de 2011: Finalización del cuestionario y divulgación a los Estados Miembros. También se enviará el cuestionario, mediante cartas separadas, a las organizaciones intergubernamentales y los representantes del sector privado y las instituciones académicas, a quienes se invitará a que proporcionen información y respondan las preguntas que les resulten pertinentes. En especial para el sector privado, se brindarán garantías de que todos los datos recibidos mantendrán un carácter confidencial y, de publicarse éstas, serán anónimos.

Mediados de julio a fines de diciembre de 2011: Reunión y clasificación de datos (5,5 meses, con un recordatorio de mediados del período que enviará la Secretaría a principios de octubre de 2011).

Principios de diciembre de 2011: Segunda reunión del Grupo de expertos, conjuntamente con la continuación del 20º período de sesiones de la Comisión de Prevención del Delito y Justicia Penal. Presentación de información sobre los progresos efectuados. Informe provisional sobre la marcha de la realización del estudio para la Comisión de Prevención del Delito y Justicia Penal en su 21º período de sesiones (abril de 2012).

Abril de 2012: Presentación del informe provisional sobre la marcha de los trabajos a la Comisión de Prevención del Delito y Justicia Penal en su 21º período de sesiones.

Mediados de enero de 2012 a julio de 2012: Análisis de los datos y redacción del estudio. Finalización del proyecto de texto del estudio.

Agosto de 2012: Divulgación del proyecto de texto del estudio a los miembros del Grupo de expertos para asegurar su preparación a tiempo para la tercera reunión del Grupo.

Octubre de 2012: Tercera reunión del Grupo de expertos para examinar, revisar y aprobar el proyecto de estudio.

Abril de 2013: Presentación del estudio a la Comisión de Prevención del Delito y Justicia Penal en su 22º período de sesiones para su consideración.