20 de diciembre de 2010
Español
Original: inglés

Grupo de expertos en delitos cibernéticos
Viena, 17 a 21 de enero de 2011

Proyecto 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. La Comisión de Prevención del Delito y Justicia Penal aprobó esa recomendación y el Consejo Económico y Social hizo lo propio en su resolución 2010/18.

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 y proponer otras nuevas).

V.10-58680 (S) 130111 130111

4. Con miras a esbozar una estructura del estudio, estas tres dimensiones (aspectos sustantivos, perspectiva y enfoque) se han plasmado en 13 temas que siguen el mandato de la Declaración. A continuación se agrupan esos 13 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) Delitos cibernéticos (tema 1);

b) Estadísticas (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 cinco esferas concretas de respuestas jurídicas, a saber:

a) Armonización de la legislación (tema 4);

b) Derecho penal sustantivo (tema 5);

c) Instrumentos de investigación (tema 6);

d) Cooperación internacional (tema 7);

e) Pruebas electrónicas (tema 8);

f) Responsabilidad (tema 9).

Respuestas de índole no jurídica al 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.

Respuesta de la comunidad internacional (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.

Respuesta del sector privado (tema 13)

10. Como ya se observó, en la Declaración de Salvador también se recomienda que el estudio exhaustivo contenga un análisis de la respuesta del sector privado.

II. Descripción detallada de los temas

Tema 1. El fenómeno del delito cibernético

Antecedentes

11. El delito informático y, más concretamente, el delito cibernético, son términos utilizados para describir una categoría concreta de conducta delictiva. Los delitos varían desde el contenido ilícito hasta determinadas formas de delitos económicos. 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

12. En la década de 1960, cuando aparecieron los equipos informáticos de transistores y se extendió el uso de las computadoras[1], la tipificación de delitos se centró en los daños físicos a los sistemas informáticos y los datos almacenados[2]. El decenio de 1970 se caracterizó por un giro de los tradicionales delitos contra la propiedad cometidos contra equipos informáticos[3], y que asumieron nuevas formas de delincuencia[4], como el uso ilícito de equipos informáticos[5] y la manipulación[6] de datos electrónicos[7]. El giro en la modalidad de las transacciones, de las operaciones manuales a las informatizadas, llevó a una nueva forma de delito, el fraude

---

[1] En relación con los desafíos conexos, véase: Slivka/Darrow; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, págs. 217 y ss.

[2] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, 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 to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, págs. 217y ss.

[5] Freed, Materials and cases on computer and law, 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 Crimes, XII Conferencia de Directores de Institutos de Investigación Criminológica, Consejo de Europa, Estrasburgo, 1976, págs. 225 y ss.; Staff Study of Computer Security in Federal Programs; Comité de Operaciones Gubernamentales, 95º Congreso, primer período de sesiones, Senado de los Estados Unidos de América, febrero de 1977.

informático[8]. 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 informática[9]. 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 patentes[10]. Además, el comienzo de la interconexión de equipos informáticos permitió a los infractores entrar en un equipo de computación sin estar presente en el lugar del delito[11]. 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 pornografía infantil pasó del intercambio de libros y películas a la distribución en línea por medio de sitios web y servicios de Internet[12]. 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 personales[13] 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].

---

[8] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, vol. 2, págs. 217 y ss.; Bequai, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, vol. 6, 1977, pág. 22.

[9] Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, pág. 73.

[10] Bloombecker, The Trial of Computer Crime, Jurimetrics Journal, vol. 21, 1981, pág. 428; Schmidt, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, vol. 21, 1981, 345 y ss. Denning, Some Aspects of Theft of Computer Software, Auckland University Law Review, vol. 4, 1980, 273 y ss.; Weiss, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, vol. 11, 1983, págs. 1 y ss.; Bigelow, The Challenge of Computer Law, Western England Law Review, vol. 7, 1985, pág. 401; Thackeray, Computer-Related Crimes, Jurimetrics Journal, 1984, 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.; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review, vol. 33, 1984, págs. 777 y ss.

[12] Child Pornography, CSEC World Congress Yokohama Conference, 2001, pág. 17; Sexual Exploitation of Children over the Internet, informe para su utilización por el Comité de Energía y Comercio de la Cámara de Representantes de los Estados Unidos, 109º Congreso, 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: El ciberdelito: Guía para los países en desarrollo, Unión Internacional de Telecomunicaciones (UIT), 2009, capítulo 2.8.4.

[14] Una red zombi o "botnet" es un grupo de computadoras manipuladas subrepticiamente en que se ejecuta un programa informático bajo control externo. Para más información, véase Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, pág. 4.

[15] Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006.

Alcance del estudio

13. 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 delitos que aún no se han tipificado;

c) Sinopsis de delitos combinados (como el robo de identidad o "peska") y tendencias futuras;

d) Inventario de casos pertinentes;

e) Definición y tipología del delito cibernético;

f) Mecanismos (técnicos) de prevención del delito;

g) Examen de la importancia de la definición del delito cibernético;

h) Reflexiones acerca de la posibilidad de la despenalización como una solución de determinados delitos cibernéticos.

Tema 2. Información estadística

Antecedentes

14. Las estadísticas sobre delito constituyen la base del examen y los procesos de adopción de decisiones por los encargados de la formulación de políticas y los especialistas[17]. 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 el delito cibernético, evitar posibles ataques y garantizar la promulgación de legislación más apropiada y eficaz.

Situación actual de las estadísticas sobre el delito cibernético

15. Por lo general, la información sobre el alcance del delito se extrae de estadísticas y estudios sobre la delincuencia[18]. 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

---

[16] Velasco San Martín, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, págs. 499 y ss.

[17] Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, pág. 308, puede consultarse en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620& rep=rep1&type=pdf.

[18] En lo que respecta a la importancia creciente de las estadísticas sobre delincuencia, véase: Osborne/Wernicke, Introduction to Crime Analysis, 2003, págs.1 y ss., que puede consultarse en: www.crim.umontreal.ca/cours/ cri3013/osborne.pdf.

información fiable debido a las diferencias de legislación y prácticas de registro[19]. Combinar y comparar las estadísticas nacionales de delincuencia exige cierto grado de compatibilidad[20] del que se carece cuando se trata del delito cibernético. Aunque los delitos cibernéticos se registren, no necesariamente se enumeran por separado[21].

16. En segundo lugar, las estadísticas solo pueden incluir los delitos que se han detectado y denunciado[22]. Especialmente en lo que se refiere al delito cibernético, preocupa el hecho de que el número de casos no denunciados parece ser importante[23]. Las empresas tal vez teman que la publicidad negativa dañe su reputación[24]. Si una empresa anuncia que su servidor ha sido objeto de actos de intrusismo informático, los clientes pueden perder la confianza, y el costo podrían ser aún mayores que las pérdidas causadas por la intrusión. Sin embargo, si los delitos no se denuncian y no se enjuicia a los delincuentes, estos probablemente reincidan. Además, las víctimas tal vez no confíen en que los organismos de represión sean capaces de identificar a los delincuentes[25] y crean que no tiene sentido denunciar los delitos[26]. Dado que la automatización permite que los

---

[19] En este contexto véase: Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009, pág. 9, puede consultarse en: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

[20] Alvazzi del Frate, Crime and criminal justice statistics challenges en Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 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 informáticos 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 Heise News, 27 de octubre de 2007, puede consultarse en: www.heise-security.co.uk/news/80152. Véase también: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, pág. 660.

[24] Véanse Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, que puede consultarse en: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, pág. 310, puede consultarse en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[25] Véanse Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, vol. 2, pág., 310, puede consultarse en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, pág. 2, que puede consultarse en: www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

[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

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 de comisiones por adelantado[27], las posibles consecuencias de delitos no denunciados podrían ser importantes. Tratándose de pequeñas cantidades, las víctimas de dichos ataques probablemente no recurran a procedimientos de denuncia engorrosos. En la práctica, suelen denunciarse únicamente los casos que entrañan comisiones muy elevadas[28].

Alcance del estudio

17. El estudio de este 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

18. 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.

---

como la información suministrada en el sitio web de la INTERPOL, que puede consultarse en: www.interpol.int/Public/THB/vico/Default.asp.

[27] Véase Organismo contra la Delincuencia Organizada Grave “International crackdown on mass marketing fraud revealed, 2007”, que puede consultarse en: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[28] Según el informe del National White Collar Crime Center sobre delitos de Internet 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.

Desafíos de la lucha contra el delito cibernético

19. 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 programas informáticos[29] destinados a localizar vías de acceso abiertas o descifrar códigos de acceso, es solo un ejemplo de ello[30]. 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 militar[31] 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 este entorno[32].

Alcance del estudio

20. El estudios 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. Armonización de la legislación

Antecedentes

21. 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.

---

[29] "Websense Security Trends Report 2004", pág. 11; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, pág. 3; Sieber, Consejo de Europa, Organised Crime Report 2004, pág. 143.

[30] Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", pág. 9.

[31] Véase una breve historia de Internet, incluidos sus orígenes militares Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff, "A Brief History of the Internet", que puede consultarse en: www.isoc.org/internet/history/brief.shtml.

[32] Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

Diferencias nacionales y regionales

22. 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, como lo demuestra la lucha contra la correo basura[33]. El correo 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 recursos[34]. 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 palabra[35] en otros[36].

23. Habida cuenta de que el delito cibernético es realmente un delito transnacional[37], la cooperación internacional es un requisito indispensable para que la investigación y el enjuiciamiento prosperen[38]. La cooperación internacional eficaz exige un grado de armonía de criterios y la armonización de la legislación a fin de prevenir la creación de refugios[39].

---

[33] El ciberdelito: Guía para los países en desarrollo, UIT, 2009, capítulo 2.5.7.

[34] Véase Spam Issue in Developing Countries, pág. 4, puede consultarse en: www.oecd.org/dataoecd/5/47/34935342.pdf.

[35] En lo que respecta al principio de la libertad de palabra, véanse: Tedford/HerbeckHaiman, Freedom of Speech in the United States, 2005; Barendt, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; Emord, Freedom, Technology and the First Amendment, 1991; en relación con la importancia del principio respecto de la vigilancia electrónica, véanse: Woo/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.; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; 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; Cohen, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, que puede consultarse en: www.fas.org/sgp/crs/misc/95-815.pdf.

[36] La preocupación por la libertad de expresión explica por qué determinados actos de racismo no se consideraron ilícitos en el Convenio sobre la Ciberdelincuencia, aunque se tipificaron en el primer Protocolo Adicional. Véase Explanatory Report to the First Additional Protocol, Núm. 4.

[37] En lo que respecta al alcance de los ataques transnacionales en los ataques cibernéticos que más daño causan, véase: Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension, en Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 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: Putnam/Elliott, International Responses to Cyber Crime, en Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, págs. 35 y ss., que puede consultarse en: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, págs. 1 y ss., que puede consultarse en: http://media.hoover.org/documents/0817999825_1.pdf.

[39] En lo que respecta al principio de la doble incriminación en las investigaciones internacionales, véanse el Manual de las Naciones Unidas sobre prevención y control de delitos informáticos, párr 269, que puede consultarse en: www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard: "Harmonizing national legal approaches on cybercrime", pág. 5, que puede consultarse en: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

Alcance del estudio

24. El estudio de este tema consistirá en:

a) El análisis de los éxitos y las limitaciones de las iniciativas existentes para armonizar la legislación en materia de delito cibernético;

b) 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;

c) El análisis del grado en que las diferencias en las normas jurídicas afectan a la cooperación internacional;

d) La determinación de las técnicas de la redacción de leyes que garanticen la flexibilidad necesaria para mantener las tradiciones jurídicas fundamentales dentro del proceso de armonización.

Tema 5. Tipificación de los delitos cibernéticos

Antecedentes

25. 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 describe *supra*.

Derecho penal sustantivo

26. La mayoría de los marcos regionales amplios establecidos para abordar el problema del delito cibernético contienen un conjunto de disposiciones de derecho penal sustantivo que están destinadas a suplir las deficiencias de la legislación nacional. Por lo general, las disposiciones de estos 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. Sin embargo, algunos enfoques van más lejos y penalizan delitos como la producción y distribución de herramientas (como los programas o el equipo informáticos) que pueden utilizarse para cometer delitos informáticos, actos relacionados con la pornografía infantil, la seducción de menores o discursos de incitación al odio.

Alcance del estudio

27. El estudio de este tema se basará en las conclusiones del estudio sobre el tema 1 acerca del fenómeno del delito cibernético y consistirá en:

a) El inventario de enfoques nacionales y regionales sobre la tipificación del delito cibernético;

b) La evaluación de las mejores prácticas en relación con la tipificación del delito cibernético;

c) El análisis de las diferencias de enfoque entre los países de tradición jurídica romanista y los inspirados por el *common law* respecto de la tipificación del delito cibernético.

Tema 6. Procedimientos de investigación

Antecedentes

28. Para realizar investigaciones eficaces, los organismos encargados de hacer cumplir 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 penales[40]. Estas medidas tal vez sean las mismas que las utilizadas en las investigaciones tradicionales que no guardan relación con el delito cibernético. No obstante, en vista de que los delincuentes no tienen por qué encontrarse en el lugar del delito, o cerca de este, es muy probable que las investigaciones deban realizarse de forma muy distinta de la tradicional[41].

Medidas de investigación

29. Además de las disposiciones relativas a los delitos cibernéticos sustantivos, la mayoría de los marcos regionales amplios establecidos para responder al problema del delito cibernético también contienen un conjunto de disposiciones concebido concretamente para facilitar las investigaciones sobre el delito cibernético. Estas disposiciones por lo general incluyen procedimientos concretos de inspección e incautación, la conservación rápida de datos informáticos, la revelación de datos almacenados, la interceptación de datos relativos al contenido y la recopilación de datos relativos al tráfico.

30. Algunos Estados han adoptado medidas que trascienden estas disposiciones tipo para abordar problemas concretos, como la interceptación de las comunicaciones por protocolo de voz a través de Internet (VoIP)[42]. Aunque la mayoría de los Estados han dispuesto medidas de investigación, como las escuchas

---

[40] En relación con los enfoques que tienen en cuenta a los usuarios en la lucha contra el delito cibernético, véase: Görling, The Myth Of User Education, 2006 en www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. Véase también la observación formulada por Jean-Pierre Chevenement, Ministro del Interior de Francia, en la Conferencia del Grupo de los Ocho celebrada en París en 2000: “En términos más generales, debemos educar a los usuarios. Todos ellos deben comprender qué pueden hacer y qué no pueden hacer en Internet, y debemos advertirles de sus posibles peligros. A medida que aumenta el uso de Internet, naturalmente deberemos intensificar nuestras iniciativas al respecto”.

[41] Debido a los protocolos usados en la comunicación por medio de Internet y la accesibilidad en todo el mundo, hay muy poca necesidad de una presencia física en el lugar en que se ofrece un servicio. Como consecuencia de esta independencia entre el lugar en que transcurre la acción y el escenario del delito, muchos delitos penales relacionados con Internet son de carácter transnacional. En lo que respecta a la independencia respecto del lugar del delito y el resultado de este, véase: El ciberdelito: Guía para los países en desarrollo, UIT, 2009, cap. 3.2.7.

[42] Por “protocolo de voz a través de Internet (VoIP)” se entiende la tecnología para transmitir comunicaciones de voz mediante la utilización de una red de conmutación de paquetes y protocolos conexos. Véase más información en: Swale, Voice Over IP: Systems and Solutions, 2001; Black, “Voice Over IP”, 2001.

telefónicas, que permiten interceptar comunicaciones de telefonía fija y móvil[43], estas medidas suelen no ser suficientes para interceptar las comunicaciones de VoIP. La interceptación de llamadas telefónicas tradicionales por lo general se realiza a través de los proveedores de servicios de telecomunicaciones[44]. Mediante la aplicación del mismo principio al VoIP, los organismos encargados de hacer cumplir la ley suelen operar por medio de los proveedores de acceso a Internet y los proveedores de servicios (VoIP). Sin embargo, si esos servicios se basan en la tecnología interpares, los proveedores pueden no estar en condiciones de interceptar las comunicaciones[45].

Alcance del estudio

31. El estudio de este tema consistirá en:

a) Ejemplos de casos de investigaciones que pusieron de relieve la necesidad de adoptar medidas de investigación especiales para delitos cibernéticos;

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

c) Reseña de las necesidades actuales de los organismos de represión en relación con disposiciones concretas relativas al delito cibernético;

d) Análisis de las diferencias de enfoque respecto de las disposiciones de investigación relativas al delito cibernético en los países de tradición jurídica romanista y los inspirados por el *common law*.

Tema 7. Cooperación internacional

Antecedentes

32. Un número cada vez mayor de delitos cibernéticos tienen una dimensión internacional[46], en particular debido al hecho de que los delincuentes, aprovechando

---

[43] En lo que respecta a la importancia de la interceptación y las soluciones técnicas, véase: Karpagavinayagam/State/Festor, "Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection", ICIMP 2007. En lo que se refiere a los desafíos relativos a la interceptación de la comunicación de datos, véase: SwaleChochliouros/Spiliopoulou/Chochliouros, "Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response", en Janczewski/Colarik, "Cyber Warfare and Cyber Terrorism", 2007, pág. 424.

[44] En lo que respecta a las diferencias entre la red telefónica pública conmutada y las comunicaciones por protocolo de voz a través de Internet (VoIP), véase: Seedorf, "Lawful Interception in P2P-Based VoIP Systems", en Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, págs. 217 y ss.

[45] En lo que respecta a la interceptación de comunicaciones por VoIP por los organismos encargados de hacer cumplir la ley, véanse Bellovin y otros, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP"; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006; Seedorf, "Lawful Interception in P2P-Based VoIP Systems", en Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, págs. 217 y ss.

[46] En lo que respecta a la dimensión transnacional del delito cibernético, véanse: Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, vol. 12,

el carácter transnacional de Internet, con frecuencia no tienen la necesidad de estar presentes en el mismo lugar que la víctima. Esta separación entre la ubicación de las víctimas y los 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 en asistencia al Estado que haya asumido la jurisdicción[47]. La cooperación internacional eficaz plantea uno de los principales desafíos 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[48], pueden hacer que la cooperación internacional sea difícil.

Instrumentos de cooperación internacional

33. Hay cuatro principales fuentes de bases jurídicas necesarias para la cooperación internacional oficial en esferas como la extradición, la asistencia judicial recíproca en asuntos penales y la cooperación con fines de decomiso.

34. En primer lugar, las disposiciones sobre cooperación internacional tal vez formen parte de acuerdos internacionales y regionales que tratan de un delito internacional en particular, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional[49,50] y el Convenio sobre Cibercriminalidad del Consejo de Europa[51]. En segundo lugar, hay tratados regionales sobre cooperación internacional como los convenios del Consejo de Europa, interamericanos o de la Comunidad de África Meridional para el Desarrollo sobre extradición o asistencia judicial recíproca. En tercer lugar, hay acuerdos bilaterales sobre extradición y asistencia judicial recíproca. En general esos acuerdos contienen información relativa a los tipos de solicitud que pueden presentarse, definen los procedimientos y las formas de contacto pertinentes, así como los derechos y

---

núm. 2, pág. 289, que puede consultarse en: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, págs. 1 y ss., que puede consultarse en: http://media.hoover.org/documents/0817999825_1.pdf.

47 Véase en este contexto: Guías legislativas para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos, 2004, pág. 220, que puede consultarse en: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

48 Gabuardi, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, vol. I, núm. 2, pág. 156, que puede consultarse en: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

49 En lo que respecta a la Convención, véase: Smith, An International Hit Job: Prosecuting Organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, vol. 97, pág. 1118, que puede consultarse en: www.georgetownlawjournal.org/issues/pdf/97- Smith.PDF.

50 Convención Interamericana sobre Asistencia Mutua en Materia Penal, 1992, Treaty Series, Organización de los Estados Americanos, núm. 75. El texto de la Convención y una lista de firmas y ratificaciones pueden consultarse en: http://www.oas.org/juridico/spanish/firmas/a-55.html.

51 Consejo de Europa, Convenio sobre la Cibercriminalidad, ETS 185.

obligaciones de los Estados requirentes y los Estados requeridos[52]. En cuarto lugar, la cooperación internacional puede permitirse en virtud del derecho interno sobre la base de la reciprocidad o caso por caso.

Alcance del estudio

35. El estudio de este tema consistirá en:

a) Desafíos en relación con la cooperación internacional en casos de delito cibernético;

b) Inventario de disposiciones sobre cooperación internacional pertinentes a la investigación y el enjuiciamiento del delito cibernético;

c) Inventario de ejemplos de mejores prácticas extraídos de acuerdos bilaterales;

d) Inventario de casos de delito cibernético que entrañan cooperación internacional;

e) Función de los medios no oficiales de cooperación como el intercambio de información de inteligencia;

f) Reseña de las necesidades actuales de las autoridades competentes respecto de la cooperación internacional.

Tema 8. Pruebas electrónicas

Antecedentes

36. Habida cuenta de que 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 computadoras y redes ya es parte de la vida cotidiana en los países desarrollados y lo mismo está sucediendo también en los países en desarrollo. La mayor capacidad de los discos duros[53] y el costo relativamente bajo[54] del almacenamiento de documentos digitales, en comparación con el almacenamiento de documentos en papel ha llevado a un número creciente de documentos digitales[55]. Actualmente, una cantidad importante

---

[52] En este contexto véanse el Tratado modelo de asistencia recíproca en asuntos penales, 1990, resolución 45/117 de la Asamblea General; Guías legislativas para la aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos, 2004, págs. 219-220, que puede consultarse en: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[53] Véanse Abramovitch, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, vol. 22, núm. 3, págs. 28 y ss.; Coughlin/Waid/Porter, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, puede consultarse en: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%200505 4.pdf

[54] Giordano, Electronic Evidence and the Law, Information Systems Frontiers, vol. 6, núm. 2, 2006, pág. 161; Willinger/Wilson, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, vol. X, núm. 5.

[55] Lange/Minster, Electronic Evidence and Discovery, 2004, 6.

de datos se almacena únicamente en formato digital[56]. Como consecuencia de este aumento, la documentación electrónica, como los documentos de texto, los vídeos digitales y las fotografías digitales[57] cumplen una función en las investigaciones del delito cibernético y las actuaciones judiciales conexas[58].

Normas relativas a las pruebas electrónicas

37. Las pruebas electrónicas plantean una serie de desafíos, tanto en la etapa en que se recogen como en la de su admisión como prueba[59]. Durante el proceso de reunión de pruebas, los investigadores deben cumplir con 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 llevar a cabo investigaciones que den buenos resultados. Estas 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 capacidad de identificar y enjuiciar con éxito a un delincuente se basa en la reunión y evaluación correctas de pruebas digitales[60].

38. La digitalización también influye en la forma en que los organismos de represión y los tribunales utilizan las pruebas[61]. 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, copias impresas de archivos[62].

---

[56] Homer, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, vol. 1, núm. 1, pág. 1, puede consultarse en: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[57] En lo que respecta a la admisibilidad y fiabilidad de las imágenes digitales, véase: Kwiatkowski, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy, págs. 267y ss.

[58] Harrington, A Methodology for Digital Forensics, T.M. Cooley J. Pac. & Clinical L., 2004, vol. 7, págs. 71 y ss.; Casey, Digital Evidence and Computer Crime, 2004, pág. 14. En lo que respecta a los marcos jurídicos en los distintos países, véanse: Rohrmann/Neto, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, núm. 5; Wang, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, núm. 5; Bazin, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, núm. 5; Makulilo, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, núm. 5. Winick, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, vol. 8, núm. 1, pág. 76; 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.

[59] Casey, Digital Evidence and Computer Crime, 2004, pág. 9.

[60] En lo que respecta a la necesidad de formalización de la informática forense, véase: Leigland/Krings, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, vol. 3, núm. 2.

[61] En lo que respecta a las dificultades de utilizar las pruebas digitales sobre la base de los procedimientos y las doctrinas tradicionales, véase: 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, págs. 57 y ss.

[62] Véase Vacca, Computer Forensics, Computer Crime Scene Investigation, 2ª edición, 2005, pág. 3. En lo que respecta al análisis anterior sobre el uso de copias impresas. Véase: Robinson,

Alcance del estudio

39. El estudio de este tema consistirá en:

a) Inventario de las disposiciones que se ocupan de la utilización y admisibilidad de las pruebas electrónicas;

b) Análisis de las diferencias de enfoque y de determinación de principios comunes en relación con las pruebas electrónicas en los países de tradición jurídica romanista y los inspirados por el *common law*.

Tema 9. Responsabilidad de los proveedores de servicios de Internet

Antecedentes

40. Aunque el delincuente actúe solo, la comisión de un delito cibernético automáticamente supone que entran en juego otras personas y empresas. Debido a la estructura de Internet, la trasmisión de un simple correo electrónico exige el servicio de varios proveedores, a saber: el proveedor de correo electrónico, los proveedores de acceso y los enrutadores que envían el correo electrónico al destinatario[63]. La situación es parecida en el caso de la descarga de películas que contienen pornografía infantil. En el proceso 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 acceder a Internet.

Papel del proveedor de servicios de Internet

41. El hecho de que un delito cibernético no pueda cometerse sin la intervención de los proveedores, sumado al hecho de que estos proveedores a menudo no pueden prevenir que se cometan delitos cibernéticos, plantea la pregunta de si debería limitarse la responsabilidad de los proveedores de servicios de Internet[64]. La respuesta a esta pregunta es fundamental para el desarrollo económico de la infraestructura de la tecnología de la información y las comunicaciones.

42. Las iniciativas de los organismos policiales suelen depender de la cooperación de los proveedores de servicios de Internet. Esto plantea cierta preocupación, ya que limitar la responsabilidad de los proveedores de Internet respecto de los actos cometidos por sus usuarios podría influir en la cooperación y el apoyo de los

---

The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, vol. 12, 1970, págs. 291y ss.

[63] En lo que respecta a la estructura de redes y las consecuencias en lo que se refiere a la participación de los proveedores de servicios, véanse: Black, Internet Architecture: An Introduction to IP Protocols, 2000; Zuckerman/McLaughlin, Introduction to Internet Architecture and Institutions, 2003, que puede consultarse en: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[64] Véase una introducción al análisis en: Elkin-Koren, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Vol. 9, 2005, págs. 15 y ss., que puede consultarse en: www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

proveedores de servicios de Internet en las investigaciones de delitos cibernéticos, así como en la propia prevención del delito cibernético.

Alcance del estudio

43. El estudio de este tema consistirá en:

a) Inventario de enfoques para reglamentar la responsabilidad de los proveedores de servicios de Internet diferenciando entre los distintos tipos de proveedores;

b) Concepto de la limitación de responsabilidad de los proveedores de servicios de Internet;

c) Aptitud de los proveedores de los servicios de Internet para prestar asistencia a los organismos encargados de hacer cumplir la ley y prevenir los delitos cibernéticos.

Tema 10. Respuestas de índole no jurídica al 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.

Respuestas de índole no jurídica

45. Las respuestas de índole no jurídica al delito cibernético incluyen, por ejemplo, el establecimiento de la infraestructura necesaria para investigar y enjuiciar los delitos (por ejemplo, equipo y personal), la capacitación de expertos que participan en la lucha contra el delito cibernético, 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) Reseña de diferentes enfoques de índole no jurídica utilizados para responder al delito cibernético;

b) Determinación de los medios para medir los resultados de esos enfoques;

c) Análisis de las relaciones entre las diferentes respuestas de índole no jurídica y las posibilidades de adoptarlas en conjunto.

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 cibernético[65], el Commonwealth (Ley modelo sobre el delito cibernético), el Consejo de Europa (Convenio sobre la Cibercriminalidad) y la Unión Europea (Decisión marco relativa a los ataques contra los sistemas de información).

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 conflictos entre diferentes enfoques internacionales[66]. El Convenio la Cibercriminalidad del Consejo de Europa y la Decisión marco relativa a los ataques contra los sistemas de información de la Unión Europea 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) Inventario de mejores prácticas de las organizaciones regionales e internacionales;

b) Fortalezas y debilidades de los enfoques existentes;

c) Análisis de deficiencias de los enfoques jurídicos internacionales.

Tema 12. Asistencia técnica

Antecedentes

50. Contrariamente a 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 industrializadas[67]. 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 de correo-e basura en los países en desarrollo[68] y llegó a la conclusión de que los países en desarrollo a menudo

---

[65] Véanse, por ejemplo, las resoluciones 45/121, 55/63, 56/121 y 60/177 de la Asamblea General.

[66] Para más información véase Gercke, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, págs. 7 y ss.

[67] Véase “Development Gateway’s Special Report, Information Society – Next Steps?”, 2005, que puede consultarse en: http://topics.developmentgateway.org/special/informationsociety.

[68] “Spam Issue in Developing Countries”, que puede consultarse en: www.oecd.org/dataoecd/5/47/34935342.pdf.

informan de que sus usuarios de Internet sufren más a causa de los efectos del correo-e basura y el uso indebido de Internet.

Asistencia técnica

51. La dimensión transnacional del delito cibernético exige que todos los países actúen de manera coordinada. Evitar el establecimiento de refugios seguros para los delincuentes cibernéticos es uno de los principales desafíos de la lucha contra ese delito[69]. Por consiguiente, el 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. Esto 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. Este se elaboraría con todos los interlocutores pertinentes.

Alcance del estudio

52. 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) Determinación de las mejores prácticas para suministrar asistencia técnica relativa el delito cibernético.

Tema 13. El sector privado

Antecedentes

53. La prevención e investigación del delito cibernético dependen de distintos elementos. Aunque a menudo se hace hincapié en la promulgación de legislación adecuada, el sector privado sigue desempeñando un papel importante tanto para prevenir como para ayudar en la investigación del delito cibernético. No obstante, su participación en la investigación del delito cibernético entraña una serie de desafíos.

El papel del sector

54. El papel del sector en relación con el delito cibernético es complejo y puede abarcar desde la elaboración y aplicación de soluciones para proteger sus propios servicios del abuso de los delincuentes hasta la protección de los usuarios y el apoyo

---

[69] Esta cuestión se trató en distintas organizaciones internacionales. En la resolución 55/63 de la Asamblea General se señala: “Los Estados deben velar para que en su legislación y en la 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 el plan de acción de 10 principios del Grupo de los Ocho se destaca la necesidad de eliminar los refugios seguros para quienes utilicen indebidamente las tecnologías de la información.

a las investigaciones. Las medidas de protección adoptadas por el sector suelen ser un componente lógico de las estrategias empresariales amplias y por lo general no requieren una base jurídica concreta en tanto las medidas no supongan contramedidas activas ilícitas. Las 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 del sector en las investigaciones penales ha planteado desafíos en muchos países y se han adoptado diferentes enfoques al respecto. En algunos países, el sector participa exclusivamente con carácter voluntario y se han elaborado directrices para facilitar la cooperación de la industria y los cuerpos y fuerzas de seguridad. Otros países han adoptado un enfoque diferente en virtud del cual han impuesto obligaciones jurídicas al sector para que coopere con los organismos encargados de cooperar con los cuerpos y fuerzas de seguridad en las investigaciones penales.

Alcance del estudio

55. El estudio de este tema consistirá en:

a) Inventario de las mejores prácticas de prevención e investigación del delito cibernético por el sector privado;

b) Análisis de las necesidades del sector y de los cuerpos y fuerzas de seguridad;

c) Evaluación de las fortalezas y debilidades de los enfoque existentes.