12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

Salvador (Brasil), 12 a 19 de abril de 2010

Distr. limitada
14 de abril de 2010
Español
Original: inglés

Informe de la Comisión II: tema 8 del programa y seminario 2

Adición

Tema 8 del programa. Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético

1. En sus sesiones primera a tercera, celebradas los días 12 y 13 de abril de 2010, la Comisión II celebró un debate general sobre el tema 8 del programa, titulado "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético". Para su examen de ese tema, la Comisión tuvo ante sí los documentos siguientes:

a) Documento de trabajo preparado por la Secretaría sobre las novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético (A/CONF. 213/9);

b) Guía para las deliberaciones (A/CONF.213/PM.1);

c) Informes de las reuniones preparatorias regionales del 12º Congreso (A/CONF.213/RPM.1/1, A/CONF.213/RPM.2/1, A/CONF.213/RPM.3/1 y A/CONF.213/RPM.4/1).

2. En la primera sesión, celebrada el 12 de abril, el Presidente de la Comisión II hizo una declaración introductoria. Un representante de la Secretaría presentó el tema. Formularon declaraciones los representantes de China, Argelia, el Canadá, la Argentina, los Estados Unidos de América, la Arabia Saudita, la Federación de Rusia, Alemania, Bostwana, Cuba y Chile. Hicieron igualmente declaraciones los observadores de la Red Iberoamericana de Cooperación Jurídica Internacional (IberRed), el Consejo de Europa y la Sociedad Mundial de Victimología. También formuló una declaración a título personal un experto de Noruega.

V.10-52736 (S) 150410 150410

3. En la segunda sesión, celebrada el 13 de abril, hicieron declaraciones los representantes de España (en nombre de la Unión Europea), Polonia, la República de Corea, Azerbaiyán, México, Indonesia, Angola y la Argentina.

4. En la tercera sesión, celebrada el 13 de abril, hicieron declaraciones los representantes de Colombia, Sudáfrica, la India, el Perú, Zimbabwe, Omán y el Brasil. También hizo una declaración un observador de la Asociación Internacional de Fiscales.

Debate general

5. Al iniciar el debate, el Presidente puso de relieve los problemas que planteaban el delito cibernético y la capacidad de los grupos delictivos organizados de aprovechar indebidamente las posibilidades que brindaba la rápida evolución de la tecnología. Destacó el carácter transfronterizo del delito cibernético, la falta de conocimientos sobre el alcance del problema y las diferencias entre los sistemas nacionales.

6. En su declaración introductoria, la representante de la Secretaría dijo que el delito cibernético era uno de los mayores problemas que afrontaban los órganos de aplicación de la ley y señaló que los Estados Miembros, miembros de los círculos académicos y otros interesados habían exhortado a que se elaborara una convención internacional sobre la materia. Los Estados debían desarrollar su capacidad, y la UNODC podía prestar asistencia en ese sentido aportando conocimientos técnicos especializados y apoyo operacional. Un medio eficaz para que los Estados fortalecieran su capacidad de manera sostenible e integral con miras a eliminar el delito cibernético podría ser un plan de acción para la creación de capacidad a nivel mundial, en cuya ejecución participaran las instituciones y los asociados principales.

7. Durante el debate se reconocieron los numerosos e innegables beneficios de los rápidos adelantos tecnológicos. Sin embargo, esos mismos adelantos posibilitaban nuevas modalidades de delitos tradicionales, como el fraude y la distribución de pornografía en que se utilizaran niños, y delitos nuevos, como la penetración en redes informáticas, el envío de correo basura, la pesca de datos (“phishing”), (la utilización de sitios web ficticios, o de mensajes en que se invite a los usuarios a visitarlos, con fines fraudulentos) la piratería digital, la propagación maliciosa de virus y otros ataques contra infraestructuras de información esenciales. Se señaló que las organizaciones terroristas y los grupos delictivos organizados utilizaban tecnologías en rápida evolución para facilitar sus actividades. Hubo consenso respecto de que el delito cibernético amenazaba las economías, las infraestructuras esenciales, el prestigio de las instituciones y el bienestar social y cultural.

8. Los oradores subrayaron las dificultades que se afrontaban para combatir el delito cibernético. Las nuevas tecnologías evolucionaban y se generalizaban con tal rapidez que dejaban a las políticas y la legislación a la zaga. Las diferencias entre los ordenamientos jurídicos y la insuficiente cooperación internacional obstaculizaban la investigación de los delitos cibernéticos y el enjuiciamiento de sus responsables. La tecnología compleja se había convertido en un fenómeno de masas y el delito cibernético iba a la par de su utilización lícita. Un orador señaló que con frecuencia no se denunciaba por la falta de confianza en el proceso de investigación y, en el caso de las empresas afectadas, por el temor a la pérdida de prestigio.

9. Diversos oradores informaron de las medidas adoptadas por sus gobiernos para combatir el delito cibernético, como la promulgación de legislación penal y contra el blanqueo de dinero, la reglamentación de los cibercafés, iniciativas de creación de capacidad, campañas de sensibilización, el reforzamiento de los mecanismos para presentar denuncias y la protección de los grupos vulnerables. Los oradores se refirieron al establecimiento de equipos de reacción de emergencia, dependencias especializadas y plataformas interinstitucionales para los órganos de represión, las fuerzas armadas, las instituciones académicas y el sector privado. Aludieron también a las posibilidades que brindaba la tecnología de la información a los órganos de represión, como los sistemas de vigilancia electrónica y de inteligencia artificial y los instrumentos electrónicos para detectar transacciones financieras sospechosas y localizar direcciones del protocolo de Internet. Sin embargo, la investigación de los delitos cibernéticos y el enjuiciamiento de sus autores requerían nuevas competencias e instrumentos procesales, como la capacidad de reunir y analizar pruebas digitales y de utilizarlas en actuaciones penales. Los oradores subrayaron la importancia de proteger la privacidad y los derechos humanos en la lucha contra el delito cibernético.

10. Muchos oradores destacaron que el delito cibernético solo podía combatirse con éxito mediante la cooperación internacional. Varios de ellos exhortaron a los Estados a que imprimieran más eficiencia a la asistencia judicial recíproca y la cooperación en materia de aplicación de la ley. Muchos señalaron que el Convenio sobre el delito cibernético del Consejo de Europa (Convenio de Budapest) era el marco jurídico internacional de mayor alcance para la cooperación entre países en la lucha contra el delito cibernético. Se aludió también a la Agenda sobre Ciberseguridad Global, presentada por la Unión Internacional de Telecomunicaciones en 2007, y a las iniciativas de la Organización de los Estados Americanos, el Grupo de los Ocho, la INTERPOL y la Secretaría del Commonwealth. Se señaló que las redes de profesionales eran útiles para intercambiar información práctica y experiencias. Se debía reforzar las redes regionales existentes y estrechar los nexos entre ellas.

11. Se reconoció que los países en desarrollo eran los más vulnerables al delito cibernético. Los países desarrollados deberían aumentar urgentemente la asistencia para la creación de capacidad, en particular la destinada al personal de los organismos de aplicación de la ley, los fiscales y los jueces. El sector privado, especialmente los proveedores de servicios, debería asumir su responsabilidad. Se hizo referencia a varios instrumentos existentes, como un foro virtual para los países de Asia, establecido con la asistencia de la UNODC, un módulo de capacitación basado en la web preparado por la Asociación Internacional de Fiscales y un manual de capacitación sobre la legislación contra el delito cibernético elaborado por la Unión Internacional de Telecomunicaciones. Los oradores se refirieron a la labor de la UNODC en la esfera de los delitos relacionados con la identidad y a las recomendaciones de un grupo básico de expertos sobre esa cuestión. Varios oradores exhortaron a que se preparara un plan de acción para la creación de capacidad en el plano internacional, con la participación de todos los interesados internacionales.

12. Se examinó la recomendación formulada en las reuniones preparatorias regionales del Congreso, en el sentido de que se considerara con atención y favorablemente la elaboración de una convención mundial contra el delito

cibernético. Algunos oradores se expresaron resueltamente a favor de que se iniciaran negociaciones sobre un nuevo instrumento internacional para armonizar los enfoques jurídicos nacionales y fomentar la cooperación internacional. Se sostuvo que las iniciativas existentes tenían un alcance bilateral o regional limitado. Un instrumento internacional, que podría ser un protocolo que complementara la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional o una convención independiente, reforzaría y enriquecería los tratados o acuerdos bilaterales y regionales sobre el delito cibernético, como el Convenio de Budapest. Un orador propuso que se negociara un nuevo instrumento en el marco de la Comisión de Derecho Internacional, de la que sería miembro la UNODC.

13. Otros oradores se opusieron a que se iniciaran negociaciones sobre un instrumento de esa índole. A su juicio, el Convenio de Budapest era un marco apropiado utilizado, no solo por los Estados que eran parte en él, como modelo para elaborar leyes que permitían a los Estados realizar investigaciones fructíferas. Se expresó inquietud en el sentido de que un instrumento mundial pudiera no establecer normas igualmente rigurosas y de que durante la negociación de un nuevo instrumento pudieran estancarse las iniciativas de modernización en curso. Se consideró que los problemas que dificultaban la lucha contra el delito cibernético eran principalmente de carácter práctico, y que para resolverlos se requería mejorar el intercambio de información y la creación de capacidad. Se señaló que la limitada capacidad técnica especializada de muchos países para reaccionar ante el delito cibernético debería concentrarse en la solución de esas cuestiones prácticas y no en la negociación de una nueva convención.

14. Varios oradores opinaron que era demasiado prematuro acoger la idea de preparar una nueva convención, porque antes debían examinarse varias cuestiones fundamentales. Algunos oradores exhortaron a que se aclarara el enfoque y el alcance de un instrumento nuevo de ese tipo, y uno de ellos recomendó que se realizara un análisis preliminar de las normas existentes. Entre las dificultades que se afrontarían en la negociación de una nueva convención figuraban cuestiones relativas a la jurisdicción extraterritorial así como las de soberanía nacional que ésta planteaba; asuntos relacionados con los derechos humanos, la privacidad y la seguridad nacional; y la necesaria participación del sector privado en un proceso de negociación intergubernamental.

Conclusiones y recomendaciones

15. Durante el debate sobre el delito cibernético se llegó a un acuerdo respecto de varias conclusiones y recomendaciones, así como sobre la necesidad de que los Estados y las organizaciones internacionales dieran seguimiento a esas recomendaciones adoptando medidas expeditas y concretas.

16. Se convino en que el desarrollo de la tecnología suponía tanto beneficios como riesgos para la sociedad, y en que la lucha contra el delito cibernético exigía una atención urgente. Se deberían analizar con especial atención los factores coadyuvantes y los nexos entre la tecnología y el delito, a fin de elaborar estrategias eficaces.

17. Los Estados deberían desarrollar una capacidad sostenible a largo plazo y fortalecerla. Los países en desarrollo requerían con urgencia asistencia técnica,

en particular para la creación de capacidad y la redacción de leyes, así como recursos materiales y expertos capacitados. La UNODC debería seguir cooperando con los asociados principales para prestar asistencia técnica a ese respecto, incluso con el Consejo de Europa como custodio del Convenio de Budapest. Se debería estudiar con especial atención la posibilidad de elaborar un plan de acción para la creación de capacidad en el plano internacional.

18. Los Estados deberían hacer todo lo posible por intensificar la cooperación entre las instituciones nacionales, así como entre ellos y con el sector privado. Para ello se requería el compromiso político pleno de los gobiernos. Era preciso aumentar el intercambio de información y mejores prácticas entre los Estados mediante, por ejemplo, el fortalecimiento de las redes pertinentes.