Distr. general
21 de febrero de 2017
Español
Original: inglés

[Start1]

Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético

Viena, 10 a 13 de abril de 2017

Deliberaciones de la primera reunión del Grupo de expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético, celebrada en Viena del 17 al 21 de enero de 2011

Resumen del Relator

I. Introducción

1. En su resolución 65/230, la Asamblea General solicitó a la Comisión de Prevención del Delito y Justicia Penal que estableciera, con arreglo a lo dispuesto en 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, un grupo intergubernamental de expertos de composición abierta, que se reuniría con antelación al 20º período de sesiones de la Comisión, para que realizara 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.

2. La primera reunión del Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético se celebró en Viena del 17 al 21 de enero de 2011. (Véase el informe sobre esa reunión en el documento UNODC/CCPCJ/EG.4/2011/3.) La reunión tuvo ante sí un proyecto de programa provisional (UNODC/CCPCJ/EG.4/2011/1) y un proyecto de temas para su examen en un estudio exhaustivo de las consecuencias del delito cibernético y la respuesta ante ese fenómeno (UNODC/CCPCJ/EG.4/2011/2), preparado por la Secretaría. El Grupo de Expertos examinó y aprobó un informe breve de procedimiento, un conjunto de temas sustantivos para examinarlo en el estudio y una metodología y plazos indicativos del estudio. Se presentó un informe de todo ello a la Comisión de Prevención del Delito y Justicia Penal en su 20º período de sesiones (véase el documento E/CN.15/2011/19, anexos I y II).

3. Se inició la elaboración de un resumen de las deliberaciones sustantivas, que no se pudo finalizar debido a la falta de recursos. En su resolución 22/7, de 26 de abril

de 2013, la Comisión invitó al Grupo de Expertos a que finalizara y aprobara los informes resumidos de sus reuniones primera y segunda, celebradas en Viena del 17 al 21 de enero de 2011 y del 25 al 28 de febrero de 2013, respectivamente. En la reunión de la Mesa ampliada del Grupo de Expertos, celebrada el 1 de diciembre de 2016, el Presidente pidió al Relator que ultimara los informes resumidos para finales de enero de 2017 y mantuviera informados a la Secretaría y el Presidente sobre el progreso de su labor. En consecuencia, el Relator, Sr. Christopher D. Ram (Canadá), examinó las notas originales, los elementos del proyecto de resumen y las grabaciones de la reunión a fin de preparar y ultimar el presente resumen.

4. Las deliberaciones del Grupo de expertos se basaron en el programa aprobado, el proyecto de lista de temas sustantivos y una metodología de estudio propuesta, que se elaboró durante la reunión. El presente resumen de las deliberaciones complementa las decisiones relativas al alcance sustantivo o la metodología del estudio, mediante el examen de las cuestiones sustantivas planteadas y la información aportada por los expertos en la primera reunión. Contiene las opiniones expresadas por expertos intergubernamentales y otros expertos sobre diversas cuestiones, incluidas cuestiones sustantivas de interés para los Estados Miembros, el proyecto de lista de temas sustantivos y otros temas propuestos para su inclusión en el estudio, y cuestiones de procedimiento y metodológicas relacionadas con la realización del propio estudio. Refleja el programa de la reunión, pero como muchas cuestiones se plantearon en más de una ocasión, se ajusta en la medida de lo posible a un enfoque temático.

II. Resumen de las deliberaciones

A. El problema del delito cibernético (tema 2 del programa)

5. Los expertos examinaron la prevalencia y el papel que desempeñaban las tecnologías de la información y las comunicaciones en sus países y cómo esos factores estaban vinculados con la ciberdelincuencia. La mayoría de los expertos señalaron que el delito cibernético iba en aumento. También señalaron que existían vínculos concretos y complejos entre a) la prevalencia y el uso de las tecnologías, tanto en los Estados Miembros como a nivel regional y b) la evolución de la ciberdelincuencia. La ciberdelincuencia se consideraba un problema universal, pero no era necesariamente un fenómeno uniforme. Muchos oradores coincidieron en que el problema era motivo de preocupación mundial. Algunos expertos señalaron que la complejidad de las formas de delincuencia y victimización, así como el flujo de datos y de productos del delito, además de otros factores, producían efectos que variaban de un Estado Miembro a otro. Se señaló que la difusión de las tecnologías y el problema conexo de la ciberdelincuencia también planteaban cuestiones relacionadas con la soberanía nacional, la independencia, la gobernanza, los derechos humanos y la cultura. Varios expertos mencionaron la necesidad de respetar la independencia soberana y la diversidad cultural, tanto al elaborar las definiciones de ciberdelincuencia como al estudiar las respuestas nacionales, transnacionales y mundiales ante ella.

6. A lo largo de la reunión se repitieron varios aspectos del problema del delito cibernético, a saber:

a) *Las tecnologías de la información y las redes de computadoras*. Los expertos señalaron que las tecnologías de la información y las redes de computadoras representaban para las actividades internas e internacionales de desarrollo tanto una oportunidad como un objetivo, y que se consideraban también un medio para prestar asistencia para el desarrollo y asistencia técnica y aumentar al máximo su eficacia. Desde ese punto de vista, la ciberdelincuencia se consideraba también un factor que podía poner en peligro las oportunidades de desarrollo. Por tanto, para todos los Estados Miembros era fundamental disponer de medios y arbitrios para hacerle frente. Los expertos también señalaron que, si bien la ciberdelincuencia y las actividades conexas podían tener efectos diferentes en los países desarrollados y en desarrollo, todos los Estados Miembros compartían los incentivos para promover el desarrollo y

protegerlo de la ciberdelincuencia. En términos más generales, observaron que, dado que las redes de computadoras permitían a los delincuentes de un Estado explotar la infraestructura y atacar a víctimas de otro Estado, existían intereses comunes para prevenir y luchar contra la ciberdelincuencia al margen del contexto del desarrollo;

b) *La rapidez y el alcance de la evolución de las tecnologías y el delito cibernético*. Esos factores suponían un reto para los legisladores y los sistemas de aplicación de la ley y de justicia penal, en particular en los países en desarrollo. Se expresó preocupación por la necesidad de velar por que se mantuvieran actualizados las leyes nacionales, los instrumentos internacionales y los programas de asistencia técnica y que esta se ofreciera de manera permanente;

c) *El carácter transnacional de las redes de computadoras y la ciberdelincuencia*. Los expertos observaron que las entidades oficiales encargadas de responder a la ciberdelincuencia y proteger a las víctimas y las infraestructuras estaban sujetas a las restricciones de la soberanía, la cortesía y la jurisdicción territorial, mientras que los delincuentes no lo estaban. Este asunto se planteó con frecuencia, no solo en el contexto de las cuestiones relativas a la aplicación de la ley y la cooperación internacional, sino también en relación con esferas de políticas más generales, la influencia de los derechos humanos en las formas que debía adoptar la tipificación como delito de la ciberconducta y la reglamentación nacional o mundial de las tecnologías por razones no necesariamente relacionadas con la delincuencia;

d) *La complejidad del delito cibernético, la rapidez con que se comete y los problemas que plantean esos factores para la investigación y el enjuiciamiento penales, tanto desde el punto de vista de la capacidad interna de investigación como de la existencia de marcos jurídicos o de otro tipo para la cooperación internacional*. Se señaló que la necesidad de establecer facultades de investigación rápida o acelerada y conciliarlas con las salvaguardias del estado de derecho planteaba dificultades a los legisladores e investigadores nacionales;

e) *Los problemas planteados por la rapidez y el carácter transnacional de la ciberdelincuencia*. Esos factores creaban cada vez más problemas de rapidez a la hora de hacer frente al delito cibernético. En los casos de delitos transnacionales, se necesitaba un acceso rápido a los datos. Sin embargo, el uso necesario de los canales oficiales de asistencia judicial recíproca y las salvaguardias del estado de derecho de los Estados afectados aumentaban considerablemente el tiempo necesario para obtener los datos;

f) *La creciente ubicuidad de las tecnologías y los problemas que generan esas tecnologías en casi todos los aspectos de la vida*. La prevalencia de las tecnologías tenía efectos que alcanzaban desde la aldea más pequeña hasta las relaciones estratégicas e internacionales de ámbito mundial de más alto nivel, tanto en las actividades del sector público como del sector privado. Los expertos destacaron la labor de sus propios Gobiernos y las iniciativas a nivel regional y subregional. También acogieron con beneplácito y subrayaron la necesidad de dar respuestas mundiales y de la participación de las Naciones Unidas en la preparación y la coordinación de esas respuestas.

7. Se plantearon dos cuestiones generales con respecto a las respuestas al delito cibernético, a saber:

a) *La necesidad de disponer de datos mundiales fiables y exhaustivos sobre la naturaleza y la extensión del problema*. Esa cuestión se reflejó en el mandato de realizar un estudio y en los materiales convenidos sobre los temas sustantivos y la metodología del estudio, aprobados por la primera reunión del Grupo de Expertos. Entre las dificultades más importantes a ese respecto figuraban el muy amplio alcance del problema, la gama de fuentes de información que debían tenerse en cuenta y la necesidad de actualizar constantemente los datos y los análisis para reflejar su evolución dinámica;

b) *La cuestión de los marcos jurídicos o de otro tipo para reglamentar y coordinar las respuestas internacionales al delito cibernético*. Se expresaron

opiniones divergentes. Algunos expertos sostuvieron que se necesitaba un nuevo instrumento jurídico internacional amplio y universal sobre el delito cibernético para establecer un consenso mundial sobre respuestas eficaces y proporcionar una base jurídica internacional clara para esas respuestas. Otros opinaron que sería más eficaz el uso de los regímenes jurídicos nacionales e internacionales existentes y enfoques más a medida para la cooperación caso por caso y la prestación de asistencia técnica.

8. Con relación al significado de la expresión “delito cibernético”, varios expertos destacaron que una única definición jurídica no resultaba factible. Sin embargo, hubo un acuerdo general sobre la necesidad de adoptar un enfoque descriptivo o tipológico como base para el estudio y otras investigaciones y como fundamento para una cooperación internacional eficaz. La mayoría de los expertos coincidieron en que la tipología elaborada en el decenio de 1990 y recogida en el Convenio del Consejo de Europa sobre la Ciberdelincuencia era un buen punto de partida, independientemente de que apoyaran o no el propio Convenio como instrumento jurídico viable. Esa tipología incluía la consideración de nuevos tipos de delitos, cuya comisión solo era posible gracias a las nuevas tecnologías; el uso de tecnologías para cometer delitos ya tipificados o análogos, a veces de nuevas maneras; y el hecho de que los grupos delictivos organizados, los grupos terroristas u otros también utilizaran con frecuencia las tecnologías para facilitar la comisión de delitos, evitar la detección u ocultar pruebas o el producto del delito.

9. Varios expertos señalaron que la posibilidad de utilizar las tecnologías para cometer delitos ya tipificados era muy amplia, lo que impediría cualquier tipo de enfoque basado en listas, tanto de cara al estudio como a otras aplicaciones. No obstante, también se observó que había surgido con el tiempo una lista de facto de delitos específicos en esferas en las que había habido un consenso sobre el hecho de que las nuevas formas de delincuencia relacionadas con la tecnología constituían un problema grave o específico y podían requerir la cooperación internacional y la coordinación de respuestas internacionales. Los ejemplos más citados a ese respecto fueron la creación y difusión de pornografía infantil y los tipos nuevos o ampliados de fraude masivo.

10. También se destacaron varias dificultades en el ámbito normativo o político de cara a un posible consenso sobre el alcance de la ciberdelincuencia como problema mundial. Una de esas dificultades era la creciente dependencia de los Estados Miembros de las tecnologías y las redes como infraestructuras de trascendental importancia y el consiguiente surgimiento de la ciberdelincuencia y otras amenazas como cuestión de seguridad nacional o de ciberseguridad. Se señaló que era inevitable que las cuestiones de la ciberdelincuencia y la ciberseguridad se superpusieran. Otra dificultad que se mencionó fue el hecho de que, si bien no existía un consenso internacional sobre la definición exacta o el alcance del término “terrorismo”, era evidente que las organizaciones terroristas podían utilizar las tecnologías y las redes y de hecho las utilizaban, lo que planteaba problemas tanto en lo que se refiere al alcance del estudio como a la labor de prevención y lucha contra la ciberdelincuencia y el terrorismo en general. La mayoría de los expertos convino en que existían problemas relacionados con la ciberseguridad y el terrorismo y que requerían una respuesta, pero las opiniones difirieron respecto de si sería adecuado o factible elaborar respuestas a esas amenazas en el contexto del mandato y el proceso del Grupo de Expertos.

11. También se examinaron los problemas relativos a la medición y la evaluación de las tasas y las tendencias de la ciberdelincuencia. Hubo acuerdo sobre la necesidad de disponer de información nacional y mundial exacta como base de datos contrastados para la adopción de medidas futuras, tanto para el estudio como de forma general, y se plantearon algunos problemas concretos. Varios expertos indicaron que la información estadística solía derivarse de las denuncias y de los enjuiciamientos basados en las definiciones jurídicas de los delitos. Se señaló que esto no reflejaba las situaciones en las que el uso de las tecnologías era un elemento real, pero no un requisito legal, o los casos que no se investigaban o enjuiciaban con buenos resultados y no reflejaban necesariamente los diferentes enfoques de los Estados Miembros respecto de la

penalización. También se señaló que la delincuencia “oscura” o no denunciada era un problema importante, ya que muchos casos de delitos cibernéticos nunca se detectaban y, en algunos casos, las víctimas no los denunciaban. Se consideró que los proveedores de servicios y otras entidades del sector privado eran una fuente importante de información en esa esfera, ya que en ocasiones se denunciaban los delitos a esas entidades, en lugar de presentar denuncia a las autoridades públicas, y que la incidencia o prevalencia de algunos delitos podía evaluarse por medios técnicos. También se mencionó la falta de capacidad estadística y de infraestructura en los países en desarrollo, no solo como problema sino también como posible objetivo de la labor de ayuda para el desarrollo y las actividades de asistencia técnica. También se observó que las tecnologías se estaban propagando rápidamente, transformando así muchas actividades en los ámbitos de la gobernanza, lo social y lo económico, lo que planteaba mayores dificultades para evaluar los costos y la gravedad general del problema y para realizar comparaciones estadísticas a lo largo del tiempo.

B. Respuestas de los Estados Miembros, la comunidad internacional y el sector privado al delito cibernético y 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 (temas 3 y 4 del programa)

12. En el ámbito de las respuestas jurídicas y de otra índole que se estaban dando en el plano nacional, muchos expertos aportaron resúmenes de medidas legislativas adoptadas en sus países, algunas de las cuales se extendían a lo largo de varios decenios, a medida que la ciberdelincuencia se había ido extendiendo y evolucionando. La mayoría de los expertos indicaron que sus países habían reconocido la gravedad del problema y que se habían adoptado medidas legislativas y de otra índole. Se mencionaron diferentes enfoques, pero se observó que, en general, reflejaban la combinación en cierto grado de la modificación o modernización de las disposiciones vigentes en la legislación nacional relativas a la penalización y las facultades de investigación, y el establecimiento de disposiciones completamente nuevas, cuando fuera necesario. La mayoría de los expertos coincidieron en la necesidad de proteger la integridad de las redes de computadoras y sus usuarios ante nuevas amenazas delictivas específicas, como los programas maliciosos, las “botnets” (redes de computadoras “zombis”) y el acceso a datos almacenados o a comunicaciones en tránsito que invadían la intimidad personal o la soberanía nacional. También hubo acuerdo sobre la necesidad de tipificar los delitos o modernizar su penalización, de manera que se trataran problemas específicos, como el fraude y el abuso de menores. Entre los asuntos que se plantearon en repetidas ocasiones con respecto a las respuestas legislativas figuraban la cuestión de si las reformas legislativas debían centrarse en la modificación de los delitos y facultades existentes o en la adopción de enfoques completamente nuevos, y la necesidad de redactar disposiciones legislativas de manera “neutral desde el punto de vista tecnológico”, a fin de que no quedaran obsoletas o resultaran inejecutables a medida que evolucionaran las tecnologías.

13. Muchos expertos señalaron que era conveniente un cierto grado de armonización o la adopción de enfoques comunes respecto de la penalización a los efectos de sentar las bases para la cooperación internacional, aunque algunos también observaron que no habría necesariamente consenso sobre cada posible delito y subrayaron la necesidad de respetar la soberanía nacional y la diversidad cultural. Se expresaron diversas opiniones sobre si el mejor enfoque de la armonización y la cooperación internacional era la elaboración de alcance variable de un nuevo instrumento jurídico internacional, el uso del Convenio del Consejo de Europa sobre la Ciberdelincuencia como base jurídica u orientación de derecho no vinculante, el uso de otros instrumentos o directrices existentes o un enfoque más adaptado a las circunstancias de cada caso de cooperación, intercambio de información y asistencia técnica. No obstante, algunos expertos señalaron que la armonización tenía sus límites, dado que

muchos Estados ya tenían leyes, y sería necesario intercambiar información para que cada Estado pudiera elegir el enfoque que más le conviniera.

14. Varios expertos señalaron que la armonización de los delitos y las leyes en materia de investigación también estaría vinculada en cierta medida a la legislación sobre derechos humanos que afectara al acceso a las tecnologías y las redes y su uso y al alcance de los delitos, así como a las leyes relacionadas con otros ámbitos, por ejemplo, los diferentes enfoques de la reglamentación de los usos no delictivos de las tecnologías, los proveedores de servicios y el establecimiento de normas técnicas. Por ejemplo, se observó que algunas formas de contenidos en línea estaban tipificadas como delito en algunas jurisdicciones, mientras que en otras estaban protegidas por el derecho a la información o la libertad de expresión. Algunos expertos mencionaron la existencia de discrepancias en delitos generales o en delitos cibernéticos específicos, como las diferencias en la edad de las víctimas que se utilizaban como base de los delitos contra menores. También se planteó como un problema para los legisladores y los investigadores las diferencias en la comisión efectiva de los delitos y la aparición de la “delincuencia distribuida”, en la que grupos de delincuentes ubicados en diferentes lugares cometían delitos complejos.

15. Algunos expertos expusieron en líneas generales sus regímenes legislativos nacionales en materia de investigación de la ciberdelincuencia. En la mayoría de los casos, las facultades de investigación incluían atribuciones generales por las que se regían técnicas como el registro y la incautación, la interceptación de comunicaciones y normas y prácticas forenses y probatorias. También se mencionaron disposiciones o variaciones más especializadas concebidas específicamente para dar solución a problemas que se planteaban en la investigación de los delitos cibernéticos. Entre esos problemas y medidas figuraban las obligaciones jurídicas de los proveedores de servicios de conservar los datos y ayudar a los investigadores recuperando y presentando datos pertinentes a partir de sistemas complejos, y la agilización de las facultades de investigación en respuesta a la rapidez con la que podían cometerse los delitos y trasladarse o eliminarse las pruebas digitales si los infractores se percataban de que estaban siendo investigados. Se señaló que se habían adaptado algunas técnicas de investigación ya existentes para utilizarlas en la localización, incautación y conservación de las pruebas digitales en dispositivos y redes. Varios expertos también mencionaron el problema de mantenerse al día respecto de la constante evolución de las tecnologías y las técnicas de los delincuentes para evitar la detección o la vigilancia y la necesidad de incorporar nuevas facultades y técnicas de investigación. En ese contexto, se señaló que los servicios encargados de hacer cumplir la ley podían utilizar algunas formas de programas maliciosos de manera muy similar a los delincuentes, pero que esos usos podían plantear problemas importantes relacionados con el estado de derecho, los derechos humanos o la jurisdicción, dependiendo de las circunstancias.

16. Si bien el alcance del estudio y el mandato del Grupo de Expertos se centraban en las respuestas nacionales e internacionales al delito cibernético como una cuestión de derecho penal o de justicia penal, algunos expertos indicaron que las esferas no penales del derecho eran fundamentales para entender las respuestas nacionales al problema y crear un consenso internacional sobre la manera de responder a él. Uno de las esferas que se plantearon fue la de los derechos humanos nacionales e internacionales, sobre la que algunos expertos indicaron que tenía efectos directos en el alcance de la penalización y en las facultades y prácticas de investigación nacionales y transnacionales. A ese respecto, se puso de relieve que la voluntad y la capacidad jurídica de muchos Estados para cooperar dependerían de que hubiera salvaguardias del estado de derecho y de los derechos humanos mutuamente satisfactorias. También se planteó el grado en que las medidas más generales o proactivas de protección de los derechos humanos, como las leyes o normas de protección de datos, eran un factor que había que tener en cuenta. Los expertos también mencionaron varias leyes nacionales no penales que se aplicaban a diversas actividades del sector privado o de particulares que afectaban tanto a la infraestructura en la que se cometían los delitos cibernéticos como a la capacidad o la obligación de

las empresas de cooperar en la prevención y la investigación. Algunos ejemplos habituales que se mencionaron fueron las leyes o normas técnicas relativas a la infraestructura de privacidad y protección de datos, la obligación legal de denunciar los delitos o de colaborar de diversas maneras con los encargados de aplicar la ley y las obligaciones legales o las prácticas voluntarias en relación con cuestiones como el cifrado y la seguridad técnica.

17. En cuanto a las respuestas nacionales propuestas o posibles en el futuro, de carácter jurídico o de otra índole, hubo acuerdo general en que se habían realizado considerables progresos, que se iniciaron en los decenios de 1980 y 1990 en un número reducido de Estados Miembros desarrollados, para luego extenderse de forma más general. La mayoría de los expertos describieron las medidas legislativas y de otra índole a lo largo de los últimos años, y muchos destacaron la implantación de iniciativas nacionales para crear capacidad, a fin de mantenerse al corriente de las novedades tecnológicas. Se puso de relieve la integración de la labor encaminada a prevenir y combatir la ciberdelincuencia en ámbitos no penales, como la gobernanza, el desarrollo comercial y las estrategias nacionales de desarrollo. También se llegó a un consenso general sobre la necesidad de la asistencia para el desarrollo y la asistencia técnica para que la ciberdelincuencia no contribuyera a crear una "brecha digital" entre los Estados Miembros o se convirtiera en un obstáculo para el desarrollo. También se convino en general que la labor dirigida a reprimir la ciberdelincuencia en los países con una gran capacidad jurídica y de aplicación de la ley no debería simplemente desplazar este problema transnacional y mundial a los países con menor capacidad. Varios expertos aportaron información sobre las actividades nacionales y regionales de asistencia técnica en curso. Tanto los expertos nacionales como los representantes del sector privado también destacaron que ese tipo de prevención de la delincuencia y creación de capacidad era un terreno en el que el sector privado tenía el incentivo y la capacidad para hacer una contribución sustancial.

18. En lo tocante a las respuestas jurídicas internacionales existentes y propuestas o posibles, se expresaron diversas opiniones y se plantearon algunas diferencias importantes con respecto a los posibles enfoques. Se expresaron opiniones diferentes acerca de la penalización de determinadas formas de conducta y las facultades o métodos de investigación, y muchos expertos señalaron que, en la medida de lo posible, sería conveniente armonizar las leyes y emplear enfoques comunes sobre la penalización como base para la cooperación internacional y la asistencia técnica. Se observó que la ciberdelincuencia planteaba problemas similares en todas partes y que existía un interés común en intercambiar conocimientos jurídicos especializados y en determinar y subsanar las lagunas en materia de penalización y de aplicación de la ley de las que podían aprovecharse los delincuentes.

19. Algunos expertos y varias organizaciones formularon observaciones sobre las funciones actuales y potenciales de las organizaciones internacionales. Se señaló que varias organizaciones regionales y subregionales participaban activamente en la elaboración o el mantenimiento de marcos o normas jurídicos, entre ellos el Convenio del Consejo de Europa sobre la Ciberdelincuencia, el Acuerdo sobre la Cooperación entre los países de la CEI para luchar contra el delito en la esfera de la información computadorizada (2001), el Acuerdo Intergubernamental sobre Cooperación en el Ámbito de la Seguridad de la Información a Nivel Internacional y las normas y reglamentos pertinentes de la Unión Europea. También se mencionaron diversas actividades de investigación, desarrollo y asistencia técnica y creación de capacidad. Se observó que era necesario coordinar los mandatos y las actividades entre las entidades y las actividades centradas en la ciberdelincuencia y esferas conexas, incluidos los derechos humanos, los ámbitos mercantiles y otras esferas no penales del derecho internacional público y privado y la regulación de la tecnología. Muchos expertos acogieron con satisfacción las iniciativas de las organizaciones regionales, pero varios pusieron de relieve el hecho de que el carácter mundial de las redes de computadoras y de la ciberdelincuencia hacía esencial la participación de las Naciones Unidas y, en particular, de la Comisión de Prevención del Delito y Justicia Penal y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). Algunos

expertos se mostraron complacidos por el presente estudio como primera iniciativa importante sobre ese tema bajo los auspicios de la Comisión, mientras que otros hicieron notar la labor previa de examen de la ciberdelincuencia o del delito informático por la Comisión, la Asamblea General y otros órganos[1]. Varios expertos mencionaron el Manual de las Naciones Unidas sobre prevención y control de delitos informáticos, elaborado en 1994, y sugirieron que podría actualizarse y volver a publicarse[2].

20. En cuanto a la posible elaboración de un nuevo instrumento jurídico o convenio internacional sobre el delito cibernético, algunos expertos no expresaron opiniones, mientras que otros intercambiaron diferentes puntos de vista sobre cuál sería el mejor enfoque. Se señaló que la cuestión había sido objeto de debates políticos y había conducido finalmente a una solución de transacción en el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Los resultados de esos debates, que figuraban en la Declaración de Salvador, constituyeron la base del mandato del propio Grupo de Expertos. En ese contexto, algunos expertos manifestaron su preocupación por el hecho de que centrarse en la naturaleza de un posible marco jurídico para la adopción de medidas internacionales contra la ciberdelincuencia podría hacer que los Estados Miembros o los expertos pasaran por alto o subestimaran la dificultad de buscar soluciones a muchos de los problemas concretos que entrañaban esas respuestas, ya fuera en el contexto de un instrumento jurídico o al margen de ello. También se puso de relieve que en la Declaración de Salvador se pedía un estudio en el que se examinaran las posibles opciones para fortalecer las medidas existentes y proponer otras nuevas, que incluían las de índole jurídica y de otro tipo para dar respuesta a la ciberdelincuencia, tanto de alcance nacional como internacional, y se señaló que era necesario un resultado equilibrado para examinar equitativamente todas las posibles respuestas.

21. Con respecto al presente estudio, algunos expertos sostuvieron que, a efectos de procedimiento y de metodología, debería incluir tanto la viabilidad como la conveniencia de un instrumento de ese tipo, así como su posible contenido o elementos. Otros expertos argumentaron que la finalidad de la primera parte del estudio era reunir y presentar información fidedigna y que el examen de las respuestas jurídicas sería un asunto que tendrían que examinar el Grupo de Expertos, la Comisión y otros órganos políticos una vez que se hubiera reunido la información. Hubo acuerdo general en que el examen futuro de esa cuestión era competencia del propio Grupo de Expertos y que en el estudio debían examinarse opciones con respecto a bases jurídicas eficaces, incluso de carácter internacional y universal, y otras formas de combatir el delito cibernético (véase E/CN.15/2011/19, anexo I, párrafo 33 b)). En ese contexto, también se debatió si las referencias a un “instrumento jurídico internacional” implicaban instrumentos de carácter universal o también incluían instrumentos elaborados o abiertos a la ratificación o adhesión únicamente sobre una

[1] Véase la resolución 1999/23 del Consejo Económico y Social, titulada “Labor del Programa de las Naciones Unidas en materia de prevención del delito y justicia penal”, E/CN.15/2001/4 y E/CN.15/2002/8; *Informe de la Junta Internacional de Fiscalización de Estupefacientes correspondiente a 2001* (publicación de las Naciones Unidas, núm. de venta: S.02.XI.1), párrs. 5 a 83; Resoluciones 55/63, de 4 de diciembre de 2000, y 56/121, de 19 de diciembre de 2001, de la Asamblea General; *Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, La Habana, 27 de agosto a 7 de septiembre de 1990: informe preparado por la Secretaría* (publicación de las Naciones Unidas, número de venta S.91.IV.2), cap. I, secc. C, *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Viena, 10 a 17 de abril de 2000: informe preparado por la Secretaría* (publicación de las Naciones Unidas, núm. de venta S.00.IV.8), párrs. 161 a 174 y *11° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Bangkok, 18 a 25 de abril de 2005: informe de la Secretaría (*publicación de las Naciones Unidas, núm. de venta S.05.IV.7), párrs. 323 a 340.

[2] *Revista Internacional de Política Criminal, núms. 43 y 44,* (publicación de las Naciones Unidas, núm. de venta S.94.IV.5). Los expertos mencionaron que la actualización y nueva publicación del Manual se había recomendado previamente en el estudio sobre ciberdelincuencia de 2000-2001 y el estudio sobre el fraude y el delito relacionado con la identidad de 2004-2007. Véanse E/CN.15/2001/4, párr. 52 a) i) y E/CN.15/2007/8, párr. 37 g).

base regional o no universal. Algunos expertos sostuvieron que los instrumentos no universales acordados entre dos o más Estados Miembros, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia, eran no obstante instrumentos jurídicos internacionales, mientras que otros manifestaron que ese concepto se refería únicamente a instrumentos de carácter universal.

22. Desde el punto de vista sustantivo, algunos expertos afirmaron que los arreglos o instrumentos jurídicos especiales elaborados a nivel regional, en particular el Convenio del Consejo de Europa sobre la Ciberdelincuencia, no eran una respuesta suficiente y que se necesitaba un instrumento jurídico elaborado mediante un proceso abierto y que estuviera abierto a la ratificación o adhesión universal bajo los auspicios de las Naciones Unidas. Sostuvieron que, dado el carácter mundial de las tecnologías de la información y las comunicaciones y del delito cibernético, resultaba esencial disponer de un instrumento jurídico universal, y señalaron que esos procesos e instrumentos no eran una novedad en la lucha contra las formas transnacionales de delincuencia. Esos expertos también destacaron la importancia del consenso implícito sobre las respuestas al delito cibernético como base para elaborar un instrumento de ese tipo y la importancia de las Naciones Unidas como único foro en el que podían tratarse eficazmente las cuestiones relativas a ese asunto. También se plantearon otras preocupaciones concretas, como la necesidad de que las negociaciones estuvieran abiertas a la participación general y de que se creara consenso, la falta de voluntad de algunos Estados Miembros de adherirse al Convenio del Consejo de Europa sobre la Ciberdelincuencia debido a que era un instrumento en cuya negociación no habían tenido voz y el hecho de que algunos Estados Miembros no podían adherirse al Convenio por razones de política o debido a problemas prácticos relacionados con disposiciones específicas del propio Convenio. Una de esas preocupaciones se refería a las disposiciones del Convenio que permitían algunas formas de investigación transfronteriza directa y, en particular, la posibilidad de acceder directamente a datos basándose en el consentimiento de las partes privadas que poseían o controlaban los datos, sin tener que notificarlo necesariamente al Estado en cuyo territorio estuvieran localizados físicamente los datos u obtener su consentimiento. Esos expertos también mencionaron problemas relacionados con la inexistencia de un marco jurídico o de derechos humanos común y con diferencias en las políticas, las tradiciones jurídicas o la cultura con respecto a los elementos de la penalización. Algunos de los expertos que apoyaban la elaboración abierta a la participación general de un instrumento jurídico internacional también alegaron que el Convenio del Consejo de Europa sobre la Ciberdelincuencia ya estaba obsoleto o no contemplaba otras cuestiones que, a su juicio, debían tenerse en cuenta o estar incluidas.

23. Otros expertos sostuvieron que no era viable elaborar un nuevo instrumento jurídico internacional sobre una base abierta a la participación general, dada la urgencia del problema y la envergadura de algunas de las cuestiones que habrían de resolverse por consenso. Señalaron que la cuestión se había planteado en el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y en ocasiones anteriores, y alegaron que las posiciones con respecto a diversas cuestiones de soberanía nacional y derecho interno eran demasiado dispares como para que pudiera elaborarse un instrumento útil y eficaz en un plazo razonable. Expresaron la esperanza de que el estudio ayudaría a aclarar las similitudes y diferencias de enfoque en las leyes nacionales y la medida en que podría llegarse a un consenso. En su opinión, el mejor enfoque era centrarse en las necesidades más inmediatas de asistencia técnica y la creación de medios informales de cooperación que permitieran realizar investigaciones rápidas. Sostuvieron que, si bien la soberanía, la jurisdicción y los derechos humanos podían ser factores que había que tener en cuenta, no era necesario abordar esas difíciles cuestiones. También consideraron que el problema principal a que tenían que hacer frente los encargados de la aplicación de la ley era la falta de capacidad nacional y de canales informales adecuados, y que ese debía ser el centro de atención de la labor futura. Esos expertos también adujeron que la complejidad del delito cibernético y la rapidez con que podían cometerse las infracciones indicaban la necesidad de adoptar enfoques flexibles en función de cada caso, especialmente en lo que respecta a las técnicas de investigación permitidas en

algunas jurisdicciones, pero no en otras. A ese respecto, consideraron que era importante fomentar la confianza recíproca entre las autoridades encargadas de hacer cumplir la ley a través de los medios disponibles, como las redes "24/72". También expresaron su preocupación por el hecho de que los posibles intentos de elaborar un nuevo instrumento jurídico internacional amplio sobre el delito cibernético requerirían una cantidad de tiempo considerable y no se podría garantizar un resultado satisfactorio. Sobre esa base, argumentaron que, en la medida en que se necesitaba un marco jurídico internacional de esa índole, la mejor opción sería utilizar el Convenio del Consejo de Europa sobre la Ciberdelincuencia, que se había elaborado en el contexto del Consejo de Europa, pero que también estaba abierto a la adhesión de otros Estados. Algunos expertos también mencionaron que el Convenio del Consejo de Europa sobre la Ciberdelincuencia era igualmente valioso como una opción de "normas flexibles" para orientar a los Estados Miembros como base para las disposiciones sobre penalización, facultades de investigación o pruebas electrónicas, o para otras leyes, incluso si esos Estados no estuvieran dispuestos a adherirse al Convenio y aplicarlo plenamente o no pudieran hacerlo.

24. En general, el debate de un posible instrumento jurídico internacional universal y amplio se centró en la conveniencia o viabilidad de su elaboración, antes que en lo que ese instrumento podría contener o en las cuestiones específicas que podrían plantearse en las negociaciones. Varios expertos señalaron que, para ellos, eso último era un elemento importante del estudio, que permitiría determinar las cuestiones y los problemas e indicar enfoques para resolverlos. Un experto planteó cuestiones más concretas, y propuso que podría seguirse la forma básica de la Convención de las Naciones Unidas contra la Corrupción en materia de penalización, prevención, asistencia técnica, cooperación internacional y protección de la soberanía nacional. Otro experto indicó que, si bien podría resultar difícil el debate mundial sobre terrorismo, habría al menos alguna posibilidad de considerar la ampliación del instrumento en cuestión a delitos de terrorismo específicos o a delitos conexos, y que algunos de los usos de las tecnologías por los grupos terroristas probablemente estarían contemplados en disposiciones relativas al delito cibernético en general.

25. En ese contexto, también se mencionó la Convención contra la Delincuencia Organizada. Algunos expertos consideraron que la Convención era un instrumento útil, dado que la mayoría de los Estados Miembros lo habían ratificado o se habían adherido a él. Además, una cantidad importante de delitos cibernéticos parecían ser "de carácter transnacional" y entrañar la participación de "un grupo delictivo organizado", de manera que se cumplían los requisitos del artículo 3 para la aplicación de la Convención. Otros expertos observaron que no se extendía a situaciones de ciberdelincuencia en las que no participaban grupos delictivos organizados y que no abordaba plenamente las formas especializadas de cooperación internacional que podrían ser necesarias en los casos de ciberdelincuencia. También se mencionaron las incertidumbres acerca de la gravedad de algunas formas de ciberdelincuencia y si estas cumplirían el requisito mínimo de "delito grave" para poder aplicar la Convención, tal como se definía en su artículo 2 b). Se expresaron diversas opiniones similares con respecto a la aplicación y la utilidad de los instrumentos de lucha contra el terrorismo en situaciones en que los terroristas atentaban contra las tecnologías o las redes o utilizaban estas para otros fines.

26. También se mencionaron varias dificultades concretas en relación con los marcos jurídicos de cooperación internacional actuales o los posibles marcos futuros, incluida la necesidad de encontrar soluciones prácticas de algunos de los problemas generales expuestos en el párrafo 7 del presente informe. En lo que respecta a la cooperación internacional en general, se expresaron diversos puntos de vista sobre la forma en que podría prestarse esa cooperación a su debido tiempo, ya fuera en virtud de los instrumentos jurídicos internacionales y regionales vigentes, como la Convención contra la Delincuencia Organizada y el Convenio del Consejo de Europa sobre la Ciberdelincuencia, o sobre diversas bases bilaterales o informales. Algunos expertos expresaron su preocupación con respecto a la necesidad de un consenso sobre normas forenses para la reunión, conservación, transmisión, autenticación y utilización de

datos digitales como prueba en procedimientos penales o judiciales de otro tipo. Asimismo, algunos expertos indicaron que las diferencias en las legislaciones nacionales relativas a la admisibilidad de técnicas como la interceptación de las comunicaciones y la infiltración en actividades delictivas, o la suplantación de identidad o la inducción al delito por un órgano encargado de hacer cumplir la ley podrían suscitar preocupaciones en situaciones que entrañaban investigaciones en línea o cuando estas afectaban a otras jurisdicciones. Otros expertos también señalaron que podrían surgir diferencias en las leyes nacionales con respecto a los requisitos en materia de derechos humanos, y pusieron de ejemplo las diferencias en la protección de la privacidad que se aplicaban a los datos utilizados para dirigir y rastrear las comunicaciones y el contenido real de esas comunicaciones.

27, En cuanto a los procedimientos de investigación transnacionales, varios expertos, en particular quienes tenían antecedentes profesionales en organismos encargados de hacer cumplir ley, afirmaron que, aunque los canales convencionales de asistencia judicial recíproca eran necesarios en los casos transnacionales, ya no eran suficientes en los casos de ciberdelincuencia. Hicieron hincapié en que la rapidez con que los delincuentes podían cometer delitos cibernéticos y después eliminar u ocultar las pruebas electrónicas exigían facultades y técnicas de investigación mucho más rápidas y directas. Hubo acuerdo general en que la cuestión de la rapidez suponía un grave y creciente problema, pero muchos expertos también destacaron la necesidad de respetar la soberanía nacional, la igualdad, la independencia y la jurisdicción territorial. Ese último grupo de expertos sostuvo que, si bien podía mejorarse la eficiencia de los mecanismos de asistencia judicial recíproca, su función básica era proteger la soberanía e impedir la elusión de los requisitos básicos del estado de derecho de cada Estado, incluidos los que daban aplicación a los derechos humanos y las garantías procesales. Esa también fue una de las preocupaciones específicas planteadas en relación con el Convenio del Consejo de Europa sobre la Ciberdelincuencia. Un experto afirmó que la Convención iba demasiado lejos al permitir el acceso extraterritorial a los datos, mientras que otro expresó la esperanza de que se modificaran las disposiciones pertinentes para ir aún más lejos en ese sentido. En general, los expertos encargados de hacer cumplir la ley opinaron que la brecha entre los plazos cortos de las investigaciones y los mucho más prolongados de la cooperación internacional era el problema más grave de cara a la investigación y enjuiciamiento de los casos transnacionales de delitos cibernéticos. Varios expertos también señalaron que los problemas eran cada vez más graves, ya que los avances como la “computación en la nube” aumentaban el número de jurisdicciones que podrían verse implicadas en tales casos, incrementaban la incertidumbre de la localización física y hacían que esta fuera más difícil de determinar en los breves plazos disponibles. Los expertos también manifestaron preocupaciones más generales acerca de la necesidad de fórmulas o entendimientos prácticos sobre la forma en que debería asignarse la responsabilidad de los elementos de investigación y enjuiciamiento entre diversos demandantes jurisdiccionales en situaciones que afectaban a varios Estados.

28. Varios expertos y representantes del sector privado destacaron la importancia de la prevención. Se mencionaron los medios técnicos, como el uso de aplicaciones de seguridad para proteger la integridad de los sistemas y los datos, y los medios sociales, como la educación de los usuarios de los sistemas y la inclusión de elementos relativos a la ciberdelincuencia en los programas escolares y universitarios pertinentes. Los expertos señalaron que debido al considerable alcance de algunas actividades de ciberdelincuencia y su carácter continuado, como el correo basura y la activación de redes de computadoras “zombis” (“botnets”), era importante disponer de capacidad para intervenir mientras se cometían delitos de manera continua contra nuevas víctimas, a menudo mediante dispositivos que funcionaban automáticamente. Se consideraba esencial disponer de capacidad para localizar y eliminar los programas maliciosos de los dispositivos infectados, tanto como medida de prevención del delito como medida de investigación reactiva. Una medida conexa que se mencionó fue la posibilidad de crear competencias y capacidad para bloquear o “desmantelar” los sitios web que se utilizaban para cometer delitos o propagar contenidos ilegales o

programas maliciosos. También se debatió sobre las cuestiones de derecho penal, de derechos humanos, de jurisdicción y de técnica que suscitaba una medida de ese tipo. Algunos expertos indicaron que una medida de ese tipo entrañaría tanto facultades jurídicas como capacidad técnica para localizar los programas maliciosos y eliminarlos. Otros señalaron que los operadores de infraestructura del sector privado podrían desempeñar un papel importante tanto en el desarrollo de sistemas resistentes a los programas maliciosos como en su eliminación. También se señaló que era importante la cooperación transfronteriza de los sectores público y privado, ya que las "botnets" eran de carácter transnacional.

29. Las importantes funciones del sector privado y la necesidad de una cooperación eficaz entre los sectores público y privado se plantearon en el contexto de la Declaración de Salvador y el mandato del estudio. Algunos expertos y representantes del sector privado plantearon cuestiones relacionadas con la cooperación entre ese sector y el público. Se señaló que el alcance y la evolución de las actividades del sector privado en diferentes entornos técnicos y normativos dificultaban la definición de términos fundamentales como "proveedor de servicios" a efectos jurídicos, pero que eso no era necesariamente un problema para establecer buenas prácticas de cooperación. Desde el punto de vista del sector privado, se señaló que el problema de cumplir con los requisitos legales de los diferentes países era un problema importante para las empresas con actividades internacionales. También se observó que, si bien los gobiernos tendían a considerar el sector privado como una sola entidad, en realidad consistía en una amplia variedad de entidades con funciones y capacidades diferentes, lo cual tenía importantes consecuencias a la hora de solicitar diversas formas de asistencia o cooperación.

30. Varios expertos pusieron de relieve que era necesario determinar las iniciativas que habían dado frutos y extraer las correspondientes enseñanzas, así como sensibilizar a la comunidad encargada de hacer cumplir la ley acerca de lo que el sector privado podía y no podía hacer. Los expertos dijeron que era posible y deseable cooperar en un amplio conjunto de ámbitos específicos, como la prevención, la cooperación en las investigaciones, la reunión de información de carácter más general sobre la evolución de la delincuencia y sus tendencias y la formación de investigadores y expertos forenses en las nuevas tecnologías a medida que se creaban y comercializaban. Una cuestión concreta que se mencionó con respecto a la cooperación entre los sectores público y privado en las investigaciones era la medida en que se aplicaban las salvaguardias jurídicas cuando las empresas privadas realizaban actividades de investigación. Otras cuestiones conexas eran la aplicación de la supervisión judicial y las salvaguardias de los derechos humanos, la protección de la soberanía nacional cuando se trataba de empresas o actividades transnacionales y la admisibilidad como prueba de la información obtenida.

31. Algunos expertos destacaron la importancia de la asistencia técnica y el intercambio de información, tanto bajo los auspicios de un instrumento jurídico internacional amplio como teniendo en cuenta las necesidades más inmediatas y los medios para atenderlas. Se señaló que en la Declaración de Salvador se había determinado que esa misma cuestión era una prioridad independiente y específica, y varios expertos hicieron hincapié en que se necesitaba urgentemente asistencia técnica y que no podía aplazarse ni retrasarse hasta que concluyera el estudio en curso. También se señaló que la naturaleza del problema requería que esos intercambios de información fueran recíprocos. Algunos expertos indicaron que la asistencia técnica relacionada con la ciberdelincuencia también estaba vinculada a cuestiones más amplias, como las estrategias de desarrollo y un conjunto de iniciativas o proyectos concretos. La Secretaría señaló que la UNODC tenía mandatos para desarrollar y prestar asistencia técnica y que solo necesitaba los recursos extrapresupuestarios necesarios para comenzar a trabajar. Los expertos que representaban a otras organizaciones intergubernamentales presentes expresaron su disposición a cooperar en las labores de asistencia técnica.

32. El alcance del estudio y la labor futura sobre el delito cibernético y su relación con cuestiones más amplias de ciberseguridad y terrorismo se plantearon en varias

ocasiones durante la reunión. Con respecto a las cuestiones relacionadas con el terrorismo, finalmente se llegó a un consenso de que en el estudio se deberían evitar las investigaciones amplias o abiertas sobre el terrorismo. En la medida en que se planteara, la atención debía centrarse en el delito cibernético propiamente dicho en el contexto del terrorismo (véase E/CN.15/2011/19, párrafo 3). Varios expertos señalaron de manera más general que tanto la evolución de la ciberseguridad como la del terrorismo plantearían retos y crearían oportunidades para posibles sinergias con respecto a cualquier actividad futura que pudiera resultar del mandato actual del Grupo de Expertos y del propio estudio. Se observó que, si bien los Estados Miembros podrían considerar algunas de las amenazas más graves como materia de ciberseguridad a efectos de políticas, la mayor parte de las actividades en cuestión estarían comprendidas en el ámbito de los delitos específicos o generales existentes, o bien en la posible labor futura sobre el delito cibernético. Se formularon observaciones similares con respecto al ciberterrorismo. Se señaló que el significado del término "ciberterrorismo" no estaba muy claro y que tampoco había consenso internacional sobre el alcance del término "terrorismo". Sin embargo, ese hecho no excluía necesariamente que se realizaran progresos hacia la consecución y aplicación de un consenso sobre problemas o actividades concretos. También se señaló que muchas actividades en línea realizadas en apoyo de grupos terroristas estarían previstas en el marco de delitos de carácter más general.

C. Estudio exhaustivo del delito cibernético (tema 5 del programa)

33. El acuerdo alcanzado por el Grupo de Expertos en su primera sesión figura en los anexos de su informe de procedimiento a la Comisión de Prevención del Delito y Justicia Penal (véanse los documentos UNODC/CCPCJ/EG.4/2011/3 y E/CN.15/2011/19). Al examinar las opciones para el estudio, se expusieron diversas cuestiones y enfoques. La Secretaría proporcionó estimaciones de los costos de producción de un documento de estudio de 150 a 200 páginas y de la celebración de nuevas sesiones del Grupo de expertos. También observó que, si bien los costos de la primera sesión habían sido absorbidos por el presupuesto ordinario, la labor posterior del Grupo de Expertos y en el seno de la UNODC dependería de la aportación de contribuciones extrapresupuestarias. Se debatieron otras opciones, como la utilización de subgrupos más pequeños y menos costosos, pero se llegó a un acuerdo general en el sentido de que el estudio debía quedar bajo el control del propio Grupo de Expertos a fin de garantizar que la supervisión de la labor y los resultados siguieran siendo abiertos a la participación general y de carácter intergubernamental. La mayoría de los expertos destacaron que las cuestiones debían examinarse a nivel gubernamental y que el proceso debía permanecer abierto a todos los Estados Miembros. No obstante, se convino que cada grupo regional podría designar hasta seis expertos gubernamentales a los que la Secretaría podría consultar sobre cuestiones concretas. Se expresó confianza en la neutralidad de la Secretaría como órgano principal encargado de realizar la investigación e informar sobre ella, y se hizo hincapié en que los resultados finales serían objeto de examen por el Grupo Intergubernamental de Expertos de Composición Abierta antes de que se trasladaran a la Comisión de Prevención del Delito y Justicia Penal.

D. Conclusiones y recomendaciones, aprobación del informe y clausura de la reunión (temas 6 a 8 del programa)

34. Como se señaló anteriormente, el Grupo de Expertos aprobó un informe breve de procedimiento preparado por la Secretaría, además del conjunto de temas sustantivos que englobaría el estudio y la metodología del estudio, tal como se habían examinado y modificado durante la reunión. Aparte de eso, no se propusieron ni consideraron conclusiones o recomendaciones específicas[3]. Se acordó que se prepararían los

[3] Puede obtenerse más información sobre los temas 6 a 8 del programa en el informe de la reunión del Grupo Intergubernamental de Expertos de Composición Abierta encargado de realizar un

informes sobre los resultados de las reuniones de la Mesa del Grupo de Expertos y se distribuirían por conducto de los grupos regionales. El Relator indicó que, además de los textos sustantivos y metodológicos aprobados, se prepararía un informe con un resumen de las deliberaciones del Grupo de Expertos y se distribuiría para su aprobación tan pronto como estuviera elaborado y distribuido en los seis idiomas oficiales[4].

Estudio Exhaustivo del Problema del Delito Cibernético, celebrada en Viena del 17 al 21 de enero de 2011 (E/CN.15/2011/19).

[4] Como se señaló en el párrafo 2, esto no se hizo después de las sesiones primera (2011) y segunda (2013) debido a la falta de recursos.