23 de enero de 2013
Español
Original: inglés

Grupo de expertos encargado de realizar un estudio exhaustivo del delito cibernético
Viena, 25 a 28 de febrero de 2013

Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno

Resumen

I. Introducción

1. En su resolución 65/230 la Asamblea General solicitó a la Comisión de Prevención del Delito y Justicia Penal que, 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, estableciera un grupo intergubernamental de expertos de composición abierta para realizar un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, 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[1]. Además, en su resolución 67/189 la Asamblea General observó con aprecio la labor del grupo intergubernamental de expertos de composición abierta para realizar un estudio exhaustivo del problema del delito cibernético y lo alentó a intensificar sus esfuerzos para concluir su labor y presentar los resultados del estudio a la Comisión de Prevención del Delito y Justicia Penal oportunamente.

2. La primera reunión del grupo de expertos se celebró en Viena del 17 al 21 de enero de 2011. En ella el grupo de expertos examinó y aprobó un conjunto de temas y una metodología del estudio[2]. La metodología del estudio contemplaba la

[1] Anexo de la resolución 65/230 de la Asamblea General.
[2] E/CN.15/2011/19.

V.13-80342 (S) 220213 220213

distribución de un cuestionario a los Estados Miembros, organizaciones intergubernamentales, y representantes del sector privado e instituciones académicas. De conformidad con la metodología acordada, la Oficina de las Naciones Unidas contra la Droga y el Delito recopiló información durante el período de febrero a julio de 2012[3]. El presente informe contiene un resumen del proyecto de estudio exhaustivo preparado por la Secretaría basándose en la información recopilada, para que sea examinado en la segunda reunión del grupo intergubernamental de expertos en delito cibernético.

II. La conectividad mundial y el delito cibernético

3. En 2011 al menos 2.300 millones de personas, equivalente a más de un tercio de la población total del mundo, tuvo acceso a Internet. Más del 60% de todos los usuarios están en los países en desarrollo y el 45% de todos los usuarios de Internet tienen menos de 25 años. Se estima que para 2017 las suscripciones a la banda ancha móvil llegarán, aproximadamente, al 70% de la población mundial. Para 2020 el número de dispositivos interconectados por la red ("Internet de las cosas") será seis veces mayor al número de personas, lo que transformará la concepción actual de Internet. En el mundo hiperconectado del futuro será difícil imaginar un "delito informático", o quizás ningún delito, que no implique pruebas electrónicas relacionadas con la conectividad del protocolo Internet.

4. Las "definiciones" del delito cibernético dependen, en gran medida, de la intención con que se emplee esa expresión. Un número limitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos se hallan en la base del delito cibernético. Sin embargo, los actos relacionados con la informática realizados en provecho propio, o para obtener beneficios económicos o perjudicar a otros, por ejemplo los delitos relacionados con la identidad y los actos que guardan relación con contenidos informáticos (los cuales quedan comprendidos todos en el significado más amplio de la expresión "delito cibernético") impiden llegar fácilmente a definiciones jurídicas de esa expresión en un sentido general. Es preciso llegar a determinadas definiciones respecto de los actos que se hallan en la base del delito cibernético. No obstante, la "definición" de ese delito no reviste tanta importancia a otros fines, como por ejemplo para definir el alcance de las facultades especializadas de investigación y de cooperación internacional, ya que en este caso es preferible centrarse en las pruebas electrónicas de cualquier delito más que en un concepto amplio y artificial del "delito cibernético".

III. Panorama mundial del delito cibernético

5. Para muchos países, el aumento vertiginoso de la conectividad mundial ha llegado en medio de cambios económicos y demográficos, con crecientes disparidades en los ingresos, ajustes en los gastos del sector privado y menos

[3] Se recibió información de 69 Estados Miembros con la siguiente distribución regional: África (11), América (13), Asia (19), Europa (24) y Oceanía (2). Se recibió información de 40 organizaciones del sector privado, 17 organizaciones académicas y 11 organizaciones intergubernamentales. La Secretaría también examinó 500 documentos de fuentes públicas.

liquidez financiera. Los funcionarios encargados de hacer cumplir la ley que respondieron al estudio consideraron que a nivel mundial habían aumentado los actos de delito cibernético a medida que tanto personas como los grupos delictivos organizados buscaban nuevas posibilidades ilícitas para obtener ganancias y beneficios personales. Se estima que más del 80% de esos actos tienen su origen en alguna forma de actividad organizada, con mercados negros cibernéticos establecidos en un círculo de creación de programas informáticos maliciosos, infección informática, gestión de redes zombi o "botnet", recolección de datos personales y financieros, venta de datos y obtención de dinero a cambio de información financiera. Los delincuentes cibernéticos ya no necesitan pericias ni habilidades técnicas complejas. Especialmente en el contexto de los países en desarrollo han aparecido subculturas de jóvenes dedicados al fraude financiero relacionado con la informática, muchos de los cuales comenzaron a participar en dicho delito en sus últimos años de adolescencia.

6. Los actos delictivos cibernéticos son muy diversos a nivel mundial, desde actos motivados por intereses financieros y actos relacionados con el contenido informático hasta actos que atentan contra la confidencialidad, la integridad y la accesibilidad de los sistemas informáticos. Sin embargo, los gobiernos y las empresas del sector privado perciben la amenaza y el riesgo relativos de manera diferente. En la actualidad las estadísticas de delitos registrados por la policía no son una base sólida para hacer comparaciones entre países, aunque estas estadísticas suelen servir para formular políticas a nivel nacional. Dos tercios de los países consideran que su sistema de estadísticas policiales es insuficiente para registrar los delitos cibernéticos. Las tasas de delitos cibernéticos registrados por la policía se corresponden con los niveles de desarrollo del país y con la capacidad policial especializada más que con las tasas de delincuencia existentes.

7. Las encuestas de victimización son una base más sólida de comparación. Estas demuestran que en el caso de los delitos cibernéticos la victimización individual es considerablemente superior a la que corresponde a las formas de delitos convencionales. Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a una tentativa de "pesca de datos" o "phishing", o sufrir el acceso no autorizado al correo electrónico varían entre el 1% y el 17% de la población con acceso a Internet de 21 países de todo el mundo, mientras que las tasas de delitos típicos, como robo, hurto y robo de coches, son en esos mismos países inferiores al 5%. Las tasas de victimización en el caso de delitos cibernéticos son más altas en los países con menores niveles de desarrollo, lo que indica la necesidad de aumentar las medidas de prevención en esos países.

8. Las empresas del sector privado en Europa informa de tasas similares de victimización, entre el 2% y el 16%, en relación con actos como la violación de datos por intrusión o "phishing". Los mecanismos ilegales elegidos para cometer esos delitos, como por ejemplo las redes zombi o "botnet", tienen un alcance mundial. En 2011 había más de un millón de direcciones únicas del protocolo Internet en todo el mundo que funcionaban como servidores de mando y control de redes zombi o "botnet". El contenido de Internet también planteaba una importante preocupación a los gobiernos. Entre el material que se eliminaba estaban no solo la pornografía infantil y los discursos de incitación al odio, sino también el contenido relacionado con la difamación y las críticas al gobierno, lo que en algunos casos despertaba inquietudes respecto de los derechos humanos. Se estima que casi

el 24% del tráfico total de Internet a nivel mundial infringe los derechos de propiedad intelectual, con bajadas de material entre pares (P2P) especialmente numerosas en países de África, América del Sur y Asia Occidental y Meridional.

IV. Legislación relativa al delito cibernético

9. Las medidas legales desempeñan un papel fundamental en la prevención del delito cibernético y en la lucha contra él. Son necesarias en todas las esferas, incluida la tipificación como delito, la competencia procesal, la jurisdicción, la cooperación internacional y la responsabilidad de los proveedores de servicios de Internet. A nivel nacional la legislación vigente y la legislación nueva (o prevista) sobre los delitos cibernéticos suelen comprender su tipificación como delito, centrándose predominantemente en establecer figuras delictivas específicas de los principales actos que constituyen delitos cibernéticos. Pero los países cada vez reconocen más la necesidad de contar con legislación en otras esferas. En comparación con la legislación vigente la legislación nueva o prevista en esta materia trata principalmente de las medidas de investigación, la jurisdicción, las pruebas electrónicas y la cooperación internacional. A nivel mundial menos de la mitad de los países que respondieron consideran que su ordenamiento jurídico en materia penal y procesal es suficiente, aunque esto oculte grandes diferencias regionales. Si bien más de los dos tercios de los países de Europa comunicaron legislación suficiente la situación se revierte en África, América, Asia y Oceanía, donde más de los dos tercios de los países consideran que la legislación es parcialmente suficiente o no lo es en absoluto. Solo la mitad de los países, que comunicaron que su legislación era insuficiente, también señalaron legislación nueva o prevista, destacando así la urgente necesidad de consolidar las disposiciones legislativas en esas regiones.

10. En el último decenio se han producido grandes avances en la promulgación de instrumentos internacionales y regionales destinados a hacer frente al delito cibernético. Esos instrumentos pueden ser obligatorios o no. Se pueden definir cinco grupos, que consisten en instrumentos elaborados o inspirados por: i) el Consejo de Europa o la Unión Europea, ii) la Comunidad de Estados Independientes, la Organización de Cooperación de Shanghái, iii) organizaciones intergubernamentales africanas, iv) la Liga de los Estados Árabes y v) las Naciones Unidas. Existe una considerable interdependencia entre todos los instrumentos, en especial conceptos y enfoques elaborados en el marco del Convenio sobre el delito cibernético, del Consejo de Europa. Del análisis de las disposiciones de 19 instrumentos multilaterales pertinentes al delito cibernético se desprende la existencia de disposiciones fundamentales comunes, pero también de considerables diferencias en las esferas sustantivas que tratan.

11. A nivel mundial 82 países han firmado y/o ratificado un instrumento obligatorio sobre el delito cibernético[4]. Además de contar con miembros oficiales que los aplican directamente, los instrumentos multilaterales han influido indirectamente en las legislaciones nacionales en forma indirecta, al ser adoptados como modelo por países que no son parte en ellos, o las legislaciones de los Estados Partes han influido en otros países. La adhesión a un instrumento multilateral sobre el delito cibernético coincide con la percepción de una mayor suficiencia de las leyes nacionales penales y procesales, lo que indica que, generalmente, las disposiciones multilaterales vigentes en la materia se consideran eficaces. En opinión de los más de 40 países que suministraron información, el Convenio sobre el delito cibernético, del Consejo de Europa, es el instrumento multilateral más utilizado para elaborar legislación sobre este tema. En total los instrumentos multilaterales de otros "grupos" se utilizaban en la mitad de ese número de países.

12. En general un tercio de los países que respondieron comunicaron que su legislación armonizaba en gran medida con la de los países considerados importantes a los fines de la cooperación internacional. Pero esto varía según la región, con mayores grados de armonización dentro de América y Europa. Esto puede deberse al uso, en algunas regiones, de instrumentos multilaterales, inherentemente designados para desempeñar un papel en la armonización. La fragmentación a nivel internacional y la diversidad de las leyes nacionales, por lo que respecta a la tipificación de los delitos cibernéticos, las formas de atribución de la jurisdicción y los mecanismos de cooperación, puede coincidir con la existencia de múltiples instrumentos que regulen los delitos cibernéticos con diferente alcance temático y distinto ámbito de aplicación geográfico. Tanto los instrumentos como las regiones presentan en la actualidad divergencias derivadas de diferencias jurídicas y constitucionales subyacentes, como por ejemplo diferentes conceptos de los derechos y de la privacidad.

V. Tipificación del delito

13. La información sobre las normas penales relativas a los delitos cibernéticos se reunió mediante el cuestionario del estudio y mediante fuentes primarias por el análisis de la legislación disponible recopilada por la Secretaría[5]. El cuestionario del estudio menciona 14 actos comúnmente incluidos en el concepto de delito cibernético[6]. Los países que respondieron mostraron una tipificación generalizada

---

[4] Uno o más de los siguientes instrumentos: el Convenio sobre el delito cibernético, del Consejo de Europa; la Convention on Combating Information Technology Offences, de la Liga de Estados Árabes; el Acuerdo sobre la Cooperación entre los países de la CEI para luchar contra el delito en la esfera de la información computadorizada; o el Agreement in the Field of International Information Security, de la Organización de Cooperación de Shanghái.

[5] Como fuente primaria se analizó la legislación correspondiente a 97 Estados Miembros, incluidos 56 que respondieron al cuestionario, con la siguiente distribución regional: África (15), América (22), Asia (24), Europa (30) y Oceanía (6).

[6] Acceso ilegal a un sistema informático; acceso, interceptación o adquisición ilícitas de datos informáticos; interferencia ilícita de datos o de sistemas; producción, distribución o posesión de dispositivos informáticos de uso indebido; violación de la privacidad o de las medidas de protección de los datos; fraude o falsificación relacionados con la informática; delitos contra la identidad relacionados con la informática; delitos contra la propiedad intelectual o las marcas de fábrica relacionados con la informática; actos relacionados con la informática que causen daños

de estos 14 actos, con excepción, principalmente, de los delitos relativos al correo basura y, en menor medida, los delitos relativos al uso indebido de dispositivos, el racismo y la xenofobia, y la incitación a la prostitución o "grooming" de menores en línea. Esto refleja un cierto consenso básico sobre lo que constituye una conducta culpable en la esfera de la informática. Los países comunicaron pocos delitos que no estuvieran mencionados en el cuestionario. Estos se referían principalmente al contenido informático, incluida la tipificación de material obsceno, el juego en línea y los mercados ilícitos en línea, como por ejemplo el mercado de drogas y de personas. Para los 14 actos los países comunicaron la existencia de delitos cibernéticos específicos para los principales actos contra la confidencialidad, la integridad y la accesibilidad de los sistemas informáticos. Para otras formas de delitos cibernéticos se aplicaban con más frecuencia figuras delictivas generales (no específicamente cibernéticas). Sin embargo se comunicó que en el caso de los actos relacionados con la informática que implicaban una violación de la privacidad, un fraude o falsificación o un delito contra la identidad se aplicaban ambos criterios.

14. Si bien existe un consenso de alto nivel con respecto a amplias esferas de la tipificación, un análisis detallado de las disposiciones de las legislaciones nacionales muestran distintos criterios. Los delitos que implican un acceso ilícito a los sistemas y los datos informáticos difieren con respecto al objeto del delito (datos, sistema o información) y respecto a la tipificación del "mero" acceso o el requisito adicional de la intención, como por ejemplo la intención de causar una pérdida o daño. El requisito de la intención para la existencia del delito también difiere en los criterios de tipificación de la interferencia de datos o sistemas informáticos. La mayoría de los países requieren que la interferencia sea intencional, mientras que otros incluyen la interferencia temeraria. En el caso de la interferencia de datos informáticos la figura delictiva va de dañar o borrar hasta alterar, suprimir, agregar o transmitir datos. La figura de la interceptación ilícita difiere según esté limitada o no a las transmisiones de datos no públicos y a que la figura esté limitada o no a la interceptación "por medios técnicos". No todos los países tipifican como delito los dispositivos informáticos de uso indebido. Entre los que sí lo hacen, las diferencias estriban en que la figura abarque la posesión, difusión o uso de software (por ejemplo el malware) y/o los códigos de acceso informático (por ejemplo la contraseña de la víctima). Desde la perspectiva de la cooperación internacional estas diferencias pueden tener consecuencias para el caso de que se dictamine la doble incriminación entre países.

15. Varios países han incorporado figuras delictivas cibernéticas específicas para el fraude, la falsificación y los delitos contra la identidad relacionados con la informática. Otros han extendido las disposiciones generales sobre fraude o robo, o recurrido a delitos que abarcan los elementos constitutivos –como por ejemplo el acceso ilícito, la interferencia y la falsificación de datos, en el caso de los delitos contra la identidad. Varias figuras delictivas relacionadas con el contenido, especialmente las relativas a la pornografía infantil, muestran una generalizada tipificación como delitos. Sin embargo, aparecen diferencias con respecto a la definición de "menor", las limitaciones en relación con el material "visual" o la

---

personales; actos relacionados con la informática que impliquen racismo o xenofobia; producción, distribución o posesión relacionados con la informática de pornografía infantil; incitación a la prostitución o "grooming" de menores relacionada con la informática; y actos relacionados con la informática en favor del terrorismo.

exclusión del material simulado, como así también respecto a los actos abarcados. En el caso de la pornografía infantil, por ejemplo, si bien la gran mayoría de los países incluyen su producción y distribución, existe una mayor variación con respecto a la tipificación como delito de la posesión y el acceso. Por lo que se refiere a los delitos relacionados con la informática en violación de los derechos intelectuales o las marcas de fábrica los países comunicaron, en general, la aplicación de los delitos generales para los actos cometidos con dolo y a escala comercial.

16. El creciente uso del contenido de los medios sociales y de Internet generada por los usuarios ha resultado en respuestas normativas de los gobiernos, incluso la aplicación del derecho penal, y requiere el respeto de la libertad de expresión. Los países que contestaron señalan una diversidad en la amplitud del derecho de expresión, incluso con respecto a la difamación, el desacato, las amenazas, la incitación al odio, el insulto a las creencias religiosas, el material obsceno y la subversión del Estado. El elemento sociocultural de algunas limitaciones se refleja no solo en la legislación nacional sino también en los instrumentos multilaterales. Algunos instrumentos regionales sobre el delito cibernético, por ejemplo, contienen figuras delictivas amplias con respecto al atentado contra la moral pública, el material pornográfico y los principios o valores familiares o religiosos.

17. La legislación internacional en materia de derechos humanos actúa como una espada y como un escudo al requerir la tipificación como delito de (ciertas) formas extremas de expresión, mientras que protege otras formas. Por lo tanto, los Estados que son parte en los instrumentos internacionales de derechos humanos pertinentes deben aplicar algunas limitaciones a la libertad de expresión, como por ejemplo la incitación al genocidio, la manifestación de odio que constituye una incitación a la discriminación, la hostilidad o la violencia, la incitación al terrorismo y la propaganda de guerra. Para otros países, el “margen de apreciación” les permite una cierta libertad para determinar límites a la libertad de expresión que sean aceptables para sus propias culturas y tradiciones jurídicas. De todas formas la legislación internacional de derechos humanos intervendrá en determinado punto. Por ejemplo, las leyes penales sobre difamación, desacato a la autoridad e insulto, por ejemplo, que se aplican a las expresiones en línea tendrán un alto umbral para demostrar que las medidas son proporcionadas, apropiadas y lo menos invasivas posibles. Cuando el contenido sea ilegal en un país pero legal de producir y difundir en otro los Estados necesitarán concentrar las respuestas de la justicia penal en las personas que tienen acceso al contenido dentro de la jurisdicción nacional y no en el contenido producido fuera del país.

VI. Aplicación de la ley e investigaciones

18. Más del 90% de los países que respondieron señalan que los actos delictivos cibernéticos más frecuentes atraen la atención de las autoridades encargadas de aplicar la ley por denuncias de víctimas individuales o de empresas. Los países que respondieron estiman que la proporción de la actual tasa de victimización denunciada a la policía por delitos cibernéticos es superior al 1%. En una encuesta mundial del sector privado se sugiere que el 80% de las víctimas individuales de los principales delitos cibernéticos no denuncian el hecho a la policía. La escasez de denuncias se debe a una falta de reconocimiento de la victimización y de los

mecanismos de denuncia, a la vergüenza y el bochorno de la víctima, y a los posibles riesgos para la reputación de las empresas. Las autoridades de todas las regiones del mundo destacaron las iniciativas para favorecer las denuncias, entre ellas los sistemas de denuncias en línea y líneas telefónicas directas, las campañas de sensibilización pública, los enlaces del sector privado y una mayor divulgación e intercambio de información de la policía. Pero la respuesta a los delitos cibernéticos en caso de denuncia de un incidente debe estar acompañada por investigaciones tácticas a mediano y largo plazo que se concentren en el mercado del delito y en los arquitectos de los planes delictivos. En los países desarrollados las fuerzas del orden realizan estas tareas, incluso mediante brigadas de agentes secretos que buscan delincuentes en los sitios de las redes sociales, las salas de charla y los servicios de mensajería instantánea y P2P. Los problemas en la investigación de los delitos cibernéticos nacen de las novedades delictivas de los delincuentes, de las dificultades en acceder a las pruebas electrónicas y de las limitaciones en materia de recursos internos, capacidad y logística. Los sospechosos suelen utilizar tecnologías de anonimato y de confusión, y nuevas técnicas se difunden rápidamente a una amplia audiencia criminal mediante los mercados del delito en línea.

19. Las investigaciones que realizan las fuerzas del orden requieren una mezcla de técnicas policiales tradicionales y nuevas. Mientras que algunas diligencias investigativas se pueden realizar con las facultades tradicionales muchas disposiciones procesales no se traducen bien de un enfoque espacial y orientado al objeto a uno que implica el almacenamiento de datos electrónicos y flujos de datos en tiempo real. El cuestionario del estudio remite a diez diligencias investigativas de los delitos cibernéticos, que van de la inspección e incautación genéricas a las facultades especializadas, como por ejemplo la conservación de datos informáticos[7]. Con mayor frecuencia los países comunicaron la existencia de facultades generales (no específicas de la cibernética) para todas las diligencias investigativas. Varios países también comunicaron legislación específica de la cibernética, especialmente para garantizar la conservación rápida de datos informáticos y para obtener datos almacenados por un suscriptor. Muchos países comunicaron una falta de competencia jurídica para las diligencias novedosas, como por ejemplo los instrumentos remotos para los estudios forenses. Mientras que las competencias procesales tradicionales pueden aplicarse a situaciones en la esfera de la cibernética, en muchos casos este criterio también puede llevar a una incertidumbre jurídica y a problemas con respecto a la licitud en la obtención de las pruebas y, por lo tanto, a su inadmisibilidad. En general los criterios nacionales con relación a las facultades investigativas en el caso de los delitos cibernéticos muestran menos puntos fundamentales en común que la tipificación como delito de muchos actos cibernéticos.

20. Independientemente de la forma legal que tengan las facultades investigativas todas las autoridades que respondieron emplean la inspección e incautación para la apropiación física del equipo de computación y para la captura de los datos

[7] Inspección de hardware o datos; incautación de hardware o datos informáticos; requerimiento de información del suscriptor; requerimiento de los datos almacenados relativos al tráfico; requerimiento de los datos almacenados relativos al contenido; recopilación en tiempo real de datos relativos al tráfico; recopilación en tiempo real de los datos sobre el contenido; conservación rápida de datos informáticos almacenados; empleo de instrumentos remotos en los estudios forenses; y acceso transfronterizo a un sistema o datos informáticos.

informáticos. La mayoría de los países también emplean requerimientos para obtener de los proveedores de servicios de Internet los datos informáticos almacenados. Pero fuera de Europa aproximadamente un tercio de los países señalan problemas para obligar a los terceros en una investigación a facilitar la información. Aproximadamente las tres cuartas partes de los países recurren a diligencias investigativas especializadas, como por ejemplo la obtención en tiempo real de datos o la conservación rápida de datos. El empleo de diligencias investigativas requiere generalmente un mínimo de pruebas iniciales o la denuncia de un hecho delictivo cibernético. Las diligencias más invasivas, como por ejemplo las que implican la obtención en tiempo real de datos o el acceso al contenido de los datos, suelen exigir mayores requisitos, como por ejemplo aportar pruebas de la comisión de un hecho grave o demostrar la existencia de causa probable o motivos fundados.

21. La relación entre las fuerzas del orden y los proveedores de servicios de Internet es especialmente compleja. Los proveedores de servicios tienen información de los suscriptores, facturas, algunos registros de conexión, información sobre la ubicación (como por ejemplo datos de las torres de celulares para los proveedores de telefonía móvil) y el contenido de las comunicaciones, todo lo cual puede representar una prueba electrónica fundamental de un delito. Las obligaciones jurídicas nacionales y las políticas de retención y divulgación de datos del sector privado varían enormemente según el país, la industria y el tipo de dato. En general los países comunicaron el empleo de una orden judicial para obtener pruebas de los proveedores de servicios. Sin embargo en algunos casos las fuerzas del orden pueden obtener directamente datos almacenados del suscriptor, datos sobre el tráfico e incluso datos sobre el contenido. A este respecto organizaciones del sector privado comunicaron con frecuencia tanto una política primaria de exigir el debido proceso legal para divulgar la información, como también el cumplimiento voluntario de las solicitudes directas de las fuerzas del orden en determinadas circunstancias. La relación oficiosa entre las fuerzas del orden y los proveedores de servicio, que existe en más de la mitad de los países que respondieron, facilita el proceso de intercambio de información y fomento de la confianza. Las respuestas indicaron la necesidad de equilibrar la privacidad y el debido proceso, con la divulgación de las pruebas en forma oportuna a fin de garantizar que el sector privado no se convierta en un cuello de botella de las investigaciones.

22. La investigación de los delitos cibernéticos implica invariablemente cuestiones de privacidad en el marco de la normativa internacional de derechos humanos. Estas normas de derechos humanos estipulan que las leyes deben ser suficientemente claras para dar una indicación adecuada de las circunstancias en que las autoridades están facultadas para realizar una diligencia investigativa, y especifican que deben existir garantías suficientes y eficaces contra el abuso. Los países comunicaron que protegían el derecho a la privacidad en la legislación nacional, como así también que existía una variedad de límites y de salvaguardias para las investigaciones. Pero cuando las investigaciones son transnacionales los distintos niveles de protección tornan imprevisible el acceso de las fuerzas del orden extranjeras a los datos y dan lugar a posibles lagunas jurisdiccionales en los regímenes de protección de la privacidad.

23. Más del 90% de los países que respondieron al cuestionario han comenzado a establecer estructuras especializadas para la investigación de los delitos cibernéticos

y de los delitos que requieren pruebas electrónicas. Pero en los países en desarrollo estas estructuras no cuentan con los recursos suficientes y padecen de una escasez de capacidad. Los países con un menor nivel de desarrollo cuentan con mucha menos policía especializada, aproximadamente 0,2 por cada 100.000 usuarios nacionales de Internet. Este porcentaje es de dos a cinco veces mayor en países más desarrollados. Se ha comunicado que en los países menos desarrollados el 70% de los agentes del orden especializados adolece de idoneidad informática y carece de equipos, y solamente la mitad recibe capacitación más de una vez por año. Más de la mitad de los países de África que respondieron y un tercio de los países de América comunicaron que los recursos de las fuerzas del orden para investigar los delitos cibernéticos eran insuficientes. Es posible que globalmente el panorama sea peor. El estudio recibió respuestas, por ejemplo, de solo el 20% de los 50 países menos adelantados del mundo. Todos los países de África que respondieron y más del 80% de los países de América y de Asia y Oceanía comunicaron que necesitaban asistencia técnica. El sector que se citaba con más frecuencia como necesitado de asistencia técnica era el de técnicas generales de investigación de delitos cibernéticos. El 60% de los países que necesitaban asistencia señalaron que la necesitaban los organismos encargados de aplicar la ley.

VII. Pruebas electrónicas y respuesta de la justicia penal

24. La prueba es el medio de constatar los hechos que hacen a la culpabilidad o inocencia de una persona en juicio. La prueba electrónica es todo ese tipo de material que existe en forma electrónica o digital. Puede estar almacenado o ser transitorio. Puede existir en forma de archivos informáticos, transmisiones, registros, metadatos o datos de la red. La ciencia forense digital se ocupa de recuperar información -frecuentemente volátil y fácilmente contaminada- que pueda tener valor probatorio. Entre las técnicas forenses se encuentran la creación de copias exactas (bit por bit) de la información almacenada y borrada, el bloqueo de escritura para asegurarse de que la información original no sea cambiada y el resumen criptográfico del archivo (hashes) o firmas digitales que pueda mostrar los cambios en la información. Casi todos los países comunicaron algún tipo de capacidad en ciencias forenses digitales. Muchos países que respondieron, de todas las regiones, señalaron que tenían un número insuficiente de técnicos forenses, diferencias entre la capacidad a nivel federal y estatal, falta de instrumentos forenses y atrasos debidos a la abrumadora cantidad de datos para analizar. La mitad de los países comunicaron que los sospechosos empleaban claves secretas, con lo cual el acceso a este tipo de pruebas es difícil y muy lento cuando no se conoce la clave. En la mayoría de los países la tarea de analizar las pruebas electrónicas corresponde a los organismos policiales. Pero los fiscales deben ver y comprender las pruebas electrónicas para poder presentar la acusación. Todos los países de África y un tercio de los países de otras regiones comunicaron que los recursos que tenían eran insuficientes para que los fiscales pudieran hacerlo. Los conocimientos informáticos de los fiscales generalmente son inferiores a los que tienen los investigadores. Alrededor del 65% de los países de todo el mundo que respondieron comunicaron alguna forma de especialización de los fiscales en delitos cibernéticos. Solamente el 10% de los países comunicaron que contaban con servicios judiciales especializados. La vasta mayoría de los casos de delitos cibernéticos está en manos de jueces no especializados que en el 40% de los países que respondieron no reciben

ninguna forma de capacitación relacionada con los delitos cibernéticos. La capacitación judicial en derecho cibernético, recopilación de pruebas y conocimientos informáticos básicos y avanzados constituye una prioridad especial.

25. Más de 60% de los países que respondieron no hacen una distinción jurídica entre prueba electrónica y prueba física. Si bien los criterios son variados, muchos países consideran que esta es una buena práctica, ya que garantiza una admisibilidad equitativa junto a los otros tipos de pruebas. Varios países fuera de Europa no admiten las pruebas electrónicas en absoluto, con lo que resulta imposible el procesamiento en caso de un delito cibernético o de cualquier otro delito que se deba probar con información electrónica. Si bien los países no cuentan, en general, con normas propias para las pruebas electrónicas, una serie de países se remiten a principios tales como: la norma de la mejor prueba, la pertinencia de la prueba, la norma de la prueba indirecta, la autenticidad y la integridad, todo lo cual puede aplicarse especialmente a la prueba electrónica. Muchos países destacaron los problemas de atribuir un hecho a determinada persona y observaron que esto solía depender de pruebas circunstanciales.

26. Los problemas que encuentran tanto los investigadores de las fuerzas del orden como los fiscales se traducen en que las tasas de enjuiciamiento son bajas en el caso de los delincuentes cibernéticos. Los sospechosos identificados por el registro policial del delito de pornografía infantil son comparables a los registrados por otros delitos sexuales. Sin embargo, los sospechosos registrados por delitos tales como el acceso ilegal y el fraude o la falsificación relacionada con la informática solo son aproximadamente de 25 por cada 100 delitos. Muy pocos países pudieron facilitar datos sobre las personas encausadas o condenadas. Sin embargo, los cálculos correspondientes a los delitos cibernéticos en un país muestran que el porcentaje de personas condenadas en relación con los delitos registrados es considerablemente menor al porcentaje de otros delitos “convencionales”.

VIII. Cooperación internacional

27. Los países que respondieron al cuestionario del estudio señalan que entre el 30% y el 70% de los delitos cibernéticos tienen una dimensión transnacional, con lo cual se plantean cuestiones de investigaciones transnacionales, soberanía, jurisdicción, pruebas extraterritoriales y requerimientos de cooperación internacional. La dimensión transnacional de un delito cibernético se presenta cuando un elemento o un efecto considerable del delito se dan en otro territorio, o cuando parte del *modus operandi* está en otro territorio. El derecho internacional establece distintas bases de atribución de la jurisdicción aplicable a estos actos, como la jurisdicción según el territorio y la jurisdicción según la nacionalidad. Algunas de estas normas también figuran en instrumentos multilaterales sobre el delito cibernético. Mientras que todos los países de Europa consideran que el derecho nacional brinda un marco suficiente para la tipificación del delito cibernético y para el enjuiciamiento en caso de actos extraterritoriales, entre un tercio y más de la mitad de los países en otras regiones del mundo señalan marcos jurídicos insuficientes. En muchos países las disposiciones reflejan la idea de que no hace falta que “todo” el acto delictivo se realice dentro de un país para afirmar la jurisdicción territorial. Se pueden establecer vínculos territoriales con respecto a los elementos o efectos del acto, o a la ubicación de los sistemas o datos informáticos

empleados en la comisión del delito. Cuando se plantea un conflicto jurisdiccional, generalmente se resuelve con consultas oficiales u oficiosas entre los países. Las respuestas de los países no muestran, en la actualidad, ninguna necesidad de contar con formas adicionales de jurisdicción sobre una presunta dimensión de "ciberespacio". Más bien las formas de jurisdicción según la territorialidad o según la nacionalidad casi siempre permiten establecer una relación suficiente entre los actos delictivos cibernéticos y al menos un Estado.

28. Las formas de cooperación internacional incluyen la extradición, la asistencia jurídica recíproca, el reconocimiento recíproco de la sentencia extranjera y la cooperación oficiosa entre policía y policía. Debido al carácter volátil de la prueba electrónica la cooperación internacional en asuntos penales en la esfera de los delitos cibernéticos requiere una respuesta pronta y la habilidad de solicitar diligencias investigativas especializadas, como por ejemplo la conservación de los datos informáticos. El recurso a formas tradicionales de cooperación es lo más usual para obtener pruebas extraterritoriales en los casos de delincuencia cibernética, ya que más del 70% de los países señalan para este fin el empleo de solicitudes oficiales de asistencia jurídica recíproca. Dentro de este tipo de cooperación oficial casi el 60% de las solicitudes se fundan en instrumentos bilaterales. Los instrumentos multilaterales sirven de fundamento en el 20% de los casos. Se comunicó que el tiempo de respuesta en el caso de los mecanismos oficiales era de meses, tanto para la extradición como para la solicitud de asistencia jurídica recíproca, un plazo que presenta un problema para la recopilación de pruebas electrónicas volátiles. El 60% de los países de África, América y Europa, y el 20% de Asia y Oceanía, comunicaron canales para solicitudes urgentes. Sin embargo, no está claro qué consecuencias tiene esto para el plazo de respuesta. Aproximadamente los dos tercios de los países que respondieron admiten modos oficiosos de cooperación, aunque pocos países tienen una política para el empleo de estos mecanismos. Las iniciativas para una cooperación oficiosa y para facilitar la cooperación oficial, como por ejemplo redes 24/7, presentan grandes posibilidades de lograr respuestas más rápidas. Sin embargo, se utilizan muy poco, ya que se recurre a ellos en el 3% del total de casos de delitos cibernéticos en manos de las fuerzas del orden del grupo de países que contestaron.

29. Se han previsto modos oficiales y oficiosos de cooperación que guían el procedimiento de lograr el consentimiento de un Estado para que fuerzas del orden extranjeras realicen investigaciones que afectan su soberanía. Pero cada vez más los investigadores, a sabiendas o no, acceden a datos extraterritoriales en ocasión de reunir pruebas, sin el consentimiento del Estado donde están físicamente situadas. Una de las razones de que se presente esta situación es la informática en la nube, que implica el almacenamiento de los datos en múltiples centros de datos situados en diferentes ubicaciones geográficas. La "ubicación" de los datos, si bien es técnicamente posible de conocer, es cada vez más artificial, al grado de que las solicitudes tradicionales de asistencia jurídica recíproca suelen dirigirse al país sede del proveedor del servicio más que al país donde el centro de datos está físicamente ubicado. El acceso directo de fuerzas del orden extranjero a datos extraterritoriales puede ocurrir cuando los investigadores aprovechan una conexión activa desde un dispositivo del sospechoso, o cuando emplean credenciales de acceso a los datos obtenidas legalmente. Los investigadores pueden, ocasionalmente, obtener datos de los proveedores de servicios extraterritoriales presentando una solicitud directa oficiosa, aunque los proveedores de servicios suelen requerir el debido proceso

legal. Las disposiciones vigentes relativas al acceso “transfronterizo” contenidas en el Convenio sobre el delito cibernético, del Consejo de Europa, y la Convention on Information Technology Offences, de la Liga de Estados Árabes, no regulan debidamente estas situaciones porque destacan el “consentimiento” de la persona legalmente autorizada para divulgar los datos y presuponen el conocimiento de la ubicación de los datos al momento de acceso o recepción.

30. El actual panorama de cooperación internacional corre el peligro de que aparezcan grupos nacionales que tengan las facultades y los procedimientos necesarios para cooperar entre ellos pero que con respecto a los demás países están restringidos a emplear modos “tradicionales” de cooperación internacional que no toman en cuenta la especificidad de las pruebas electrónicas ni el carácter mundial de la delincuencia cibernética. Esto ocurre especialmente en el caso de la cooperación en las diligencias investigativas. La falta de un criterio común, incluso en los instrumentos multilaterales vigentes sobre el delito cibernético, significa que la solicitud de acción, como por ejemplo la rápida conservación de los datos, será difícil de cumplir fuera de los países que tienen obligaciones internacionales de garantizar este servicio y de brindarlo cuando se solicite. La inclusión de esta facultad en el proyecto de convenio sobre la seguridad cibernética de la Unión Africana sería un adelanto en el camino de cubrir esta laguna. A nivel mundial las divergencias en el alcance de las disposiciones sobre cooperación contenidas en los instrumentos multilaterales y bilaterales, la falta de obligación en el cumplimiento de los plazos, la falta de acuerdo sobre el acceso directo a los datos extraterritoriales, múltiples redes oficiosas de cumplimiento de la ley y diversidad en las garantías de cooperación representan grandes obstáculos para lograr una cooperación internacional eficaz con respecto a la prueba electrónica en asuntos penales.

IX. Prevención del delito cibernético

31. La prevención del delito comprende estrategias y medidas tendientes a reducir el riesgo de comisión de delitos y mitigar las posibles consecuencias perjudiciales para las personas y la sociedad. Casi el 40% de los países que respondieron dijeron que contaban con leyes o políticas nacionales para prevenir el delito cibernético. Otro 20% de los países se encuentra en el proceso de preparación de iniciativas en ese sentido. Los países destacan que entre las buenas prácticas de prevención del delito cibernético figuran la promulgación de leyes, una dirección eficaz, desarrollo de una justicia penal y de una capacidad de mantener el orden, la educación y la sensibilización, el desarrollo de una base firme de conocimientos y la cooperación a nivel de gobierno, comunidades, sector privado e internacional. Más de la mitad de los países comunicaron la existencia de estrategias en materia de delito cibernético. En muchos casos esas estrategias están estrechamente integradas en las estrategias de la seguridad cibernética. Aproximadamente 70% de todas las estrategias nacionales comunicadas incluían componentes de sensibilización, cooperación internacional y capacidad de mantenimiento del orden. A los fines de la coordinación, los organismos que se señalaron con más frecuencia como las principales instituciones en materia de delitos cibernéticos fueron las fuerzas del orden y el ministerio público.

32. Las encuestas, incluidas las realizadas en países en desarrollo, demuestran que hoy en día la mayoría de los usuarios de Internet adoptan medidas básicas de seguridad. Los gobiernos, las entidades del sector privado y las instituciones académicas que respondieron a dichas encuestas destacaron la importancia de las campañas de sensibilización pública, en particular las relativas a las nuevas amenazas y las dirigidas a destinatarios específicos, como los menores. La educación del usuario resulta extremadamente eficaz cuando se combina con sistemas que los ayudan a alcanzar sus objetivos de manera segura. Si el costo para el usuario es superior a su beneficio directo las personas tienen pocos incentivos para adoptar medidas de seguridad. Las entidades del sector privado también comunicaron que la sensibilización del usuario y del empleado debe integrarse en un criterio holístico de la seguridad. Los principios fundamentales y las buenas prácticas mencionadas incluyen la responsabilidad por adoptar medidas sobre la sensibilización, políticas y prácticas de gestión de riesgo, liderazgo a nivel de directorio y capacitación del personal. Los dos tercios de quienes contestaron por el sector privado habían realizado una evaluación de riesgos en materia de delitos cibernéticos y la mayoría comunicaron el uso de tecnologías de seguridad tales como cortafuegos, conservación de las pruebas digitales, identificación del contenido, detección de la intrusión y sistemas de supervisión y vigilancia. Sin embargo, se expresó la preocupación de que las empresas pequeñas y medianas no adoptaban suficientes medidas para proteger los sistemas o tuvieran la impresión errónea de que no se convertirían en blanco de tales delitos.

33. Los marcos regulatorios tienen una importante función que desempeñar en la prevención del delito cibernético, tanto con respecto al sector privado en general como a los proveedores de servicio en particular. Casi la mitad de los países han dictado normas de protección de los datos, con requisitos específicos para la protección y el uso de los datos personales. Algunos de estos regímenes incluyen requisitos específicos para los proveedores de servicios de Internet y demás proveedores de comunicaciones electrónicas. Si bien las normas de protección de los datos requieren que los datos personales se borren cuando ya no sean necesarios, algunos países han establecido excepciones a los fines de la investigación penal, exigiendo que los prestadores de servicios de Internet almacenen tipos específicos de datos por un plazo determinado. Muchos países desarrollados también tienen normas que exigen a las organizaciones notificar las violaciones de datos a los particulares y a quienes dictan las normas. Los proveedores de servicios de Internet tienen generalmente una responsabilidad limitada como “meros conductores” de datos. La modificación del contenido trasmitido aumenta la responsabilidad, al igual que el conocimiento real o constructivo de una actividad ilegal. La acción rápida después de la notificación, por otra parte, reduce la responsabilidad. Si bien existen posibilidades técnicas de que los proveedores de servicios filtren el contenido de Internet las restricciones al acceso a Internet quedan sujetas a requisitos de previsibilidad y proporcionalidad en el marco de las normas internacionales de derechos humanos que protegen el derecho a buscar, recibir y dar información.

34. La alianza entre los sectores público y privad es fundamental para la prevención del delito cibernético. Más de la mitad de los países señalan la existencia de alianzas. Estas se crean en igual número por acuerdos oficiosos y por normas legales. Las entidades del sector privado son las que más participan, seguidas por las instituciones académicas y por organizaciones internacionales o regionales. Las alianzas generalmente sirven para facilitar el intercambio de información sobre

amenazas y tendencias, pero también para desarrollar actividades y medidas de prevención en casos específicos. En el contexto de algunas alianzas entre los sectores público y privado, entidades del sector privado han adoptado un criterio proactivo para investigar operaciones de la delincuencia cibernética e interponer acciones judiciales. Esas acciones complementan las de las fuerzas del orden y pueden ayudar a mitigar los daños ocasionados a las víctimas. Las instituciones académicas desempeñan diversos papeles en la prevención del delito cibernético, por ejemplo con la instrucción y capacitación de profesionales, la elaboración de normas y la formulación de políticas, así como su labor en la elaboración de normas técnicas y formulación de soluciones Las universidades reúnen y favorecen a expertos en delitos cibernéticos, a algunos equipos informáticos de respuestas de emergencia (CERT) y a centros de investigación especializada.

X. Principales conclusiones y opciones

35. Las principales conclusiones del estudio amplio sobre el delito cibernético son las siguientes:

a) la fragmentación a nivel internacional y la diversidad en las leyes nacionales sobre delitos cibernéticos puede tener relación con la existencia de múltiples instrumentos de diferente alcance temático y geográfico. Si bien es legítimo que los instrumentos reflejen diferencias socioculturales y regionales las discrepancias en la extensión de la competencia procesal y de las disposiciones internacionales de cooperación pueden llevar a la aparición en los países de "grupos" de cooperación que no siempre son convenientes para el carácter mundial del delito cibernético;

b) la dependencia de formas tradicionales oficiales de cooperación internacional en cuestiones de delito cibernético no puede ofrecer actualmente la respuesta oportuna necesaria para obtener las pruebas electrónicas volátiles. Como un creciente número de delitos implican pruebas electrónicas repartidas por el mundo, esto será un problema no solo para el delito cibernético sino para todos los delitos en general;

c) en un mundo de computación en la nube y de centros de datos habrá que replantearse el papel de la "ubicación" de las pruebas, incluida la posibilidad de obtener consenso sobre cuestiones relativas al acceso directo de las fuerzas del orden a los datos extraterritoriales;

d) el análisis de los marcos jurídicos nacionales disponibles señala una armonización insuficiente de los delitos cibernéticos "primordiales", de las facultades investigativas y de la admisibilidad de la evidencia electrónica. La legislación internacional en materia de derechos humanos representa un importante punto de referencia externa para la tipificación como delito y para las disposiciones procesales;

e) las fuerzas del orden, los fiscales y los jueces de los países en desarrollo necesitan ayuda y asistencia técnicas de largo plazo, sostenible y amplia, para investigar y luchar contra el delito cibernético;

f) las actividades de prevención del delito cibernético en todos los países deben consolidarse con un enfoque global que implique una mayor sensibilización, alianzas entre los sectores público y privado y la integración de las estrategias del delito cibernético con una perspectiva más amplia de la seguridad cibernética.

36. Entre las 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, figuran una o más de las siguientes:

a) la elaboración de disposiciones internacionales modelo sobre la tipificación como delito de los actos cibernéticos primordiales a fin de ayudar a los Estados a eliminar los refugios seguros mediante la adopción de elementos de los delitos comunes:

i) las disposiciones podrían mantener el criterio de los instrumentos vigentes sobre los delitos contra la confidencialidad, la integridad y la accesibilidad de los sistemas y datos informáticos;

ii) las disposiciones podrían también abarcar los delitos "convencionales" cometidos o facilitados por el uso de sistemas informáticos solo cuando los criterios vigentes para la tipificación se consideraran insuficientes;

iii) las disposiciones podrían abarcar esferas no comprendidas en los instrumentos vigentes, como por ejemplo la tipificación como delito del correo basura;

iv) las disposiciones podrían elaborarse conforme a las últimas normas internacionales de derechos humanos sobre la tipificación de delitos, especialmente la protección a la libertad de expresión sobre la base de tratados;

v) la aplicación por el Estado de estas disposiciones reduciría el problema de la doble incriminación en la cooperación internacional;

b) la elaboración de disposiciones internacionales modelo sobre las facultades para investigar las pruebas electrónicas y ayudar a los Estados a establecer los mecanismos procesales necesarios para investigar delitos que impliquen pruebas electrónicas:

i) las disposiciones podrían aprovechar el criterio de los instrumentos vigentes, incluidos los requerimientos de rápida conservación de los datos y requerimientos para obtener datos almacenados y datos en tiempo real;

ii) las disposiciones podrían ofrecer directrices sobre la posibilidad de extender a las pruebas electrónicas las facultades tradicionales, como la inspección e incautación;

iii) las disposiciones podrían ofrecer directrices sobre la aplicación de salvaguardias adecuadas a las técnicas intrusivas de investigación, basadas en la legislación internacional sobre derechos humanos, incluida la protección del derecho a la privacidad basada en los tratados;

c) la elaboración de disposiciones modelo sobre jurisdicción a fin de establecer al respecto bases comunes efectivas en asuntos penales relacionadas con el delito cibernético:

i) las disposiciones podrían incluir bases tales como las derivadas del principio de la territorialidad objetiva y la doctrina de efectos sustanciales;

ii) las disposiciones podrían incluir directrices para tratar de resolver los problemas de concurrencia de jurisdicciones;

d) la elaboración de disposiciones modelo sobre cooperación internacional en el caso de las pruebas electrónicas para incluir en instrumentos bilaterales o multilaterales, como por ejemplo en un texto revisado del Tratado modelo de asistencia recíproca en asuntos penales, de las Naciones Unidas, en concordancia con las sugerencias contenidas en la Guía para las Deliberaciones del 13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal:

i) las disposiciones se centrarían en mecanismos prácticos de cooperación que pudieran incluirse en los instrumentos vigentes para la conservación oportuna y el aporte de pruebas electrónicas en los asuntos penales;

ii) las disposiciones podrían incluir la obligación de crear centros de coordinación para respuestas rápidas en materia de pruebas electrónicas y acordar plazos de ejecución;

e) la elaboración de un instrumento multilateral sobre la cooperación internacional respecto de las pruebas electrónicas en los asuntos penales, a fin de contar con un mecanismo internacional de cooperación para la conservación y obtención de pruebas electrónicas:

i) como un complemento de los tratados vigentes de cooperación internacional un instrumento de este tipo podría centrarse fundamentalmente en un mecanismo para solicitar la rápida conservación de los datos por un plazo determinado;

ii) el instrumento también podría incluir disposiciones específicas de cooperación para otras medidas investigativas, como el suministro de datos almacenados y la recopilación de datos en tiempo real;

iii) habría que definir el ámbito de aplicación, pero no debería quedar limitado al “delito cibernético” o a los delitos “relacionados con la informática”;

iv) el instrumento podría requerir respuestas dentro de un plazo específico y establecer canales de comunicación claros de un centro de coordinación a otro, ampliando más que duplicando las actuales iniciativas 24/7;

v) el instrumento podría incluir las salvaguardias tradicionales en materia de cooperación internacional, así como las debidas exclusiones en materia de derechos humanos;

f) la elaboración de un instrumento multilateral amplio sobre el delito cibernético con el objeto de fijar un criterio internacional en materia de tipificación, competencia procesal, jurisdicción y cooperación internacional:

i) el instrumento podría incluir elementos de todas las opciones mencionadas en una forma vinculante y multilateral;

ii) el instrumento podría basarse en elementos básicos comunes en la actual gama de instrumentos internacionales y regionales tanto de carácter vinculante como no vinculante;

g) la consolidación de las alianzas internacionales, regionales y nacionales, incluidas las alianzas con el sector privado y con instituciones académicas, a fin prestar una mejor asistencia técnica para la prevención y represión del delito cibernético en los países en desarrollo:

i) la asistencia técnica podría prestarse basándose en normas elaboradas según las disposiciones modelo expuestas en las opciones *supra*;

ii) la prestación de la asistencia técnica podría orientarse a una prestación por múltiples interesados, entre ellos representantes del sector privado y del académico.